Network Working Group B. Fraser
Request for Comments: 2196 Editor
FYI: 8 SEI/CMU
Obsoletes: 1244 September 1997
Category: Informational

Руководство по безопасности сайтов

Site Security Handbook

Статус документа

Этот документ содержит информацию для сообщества Internet. Документ не задает каких-либо стандартов Internet и может распространяться свободно.

Тезисы

Этот документ является руководством по разработке политики компьютерной безопасности для сайтов, подключенных к сети Internet. Руководство содержит практические рекомендации для администраторов, пытающихся обеспечить безопасность информации и сетевых служб. Тематика документа включает разработку политики безопасности, вопросы сетевой безопасности и расследования инцидентов.

Оглавление

1. Введение

Этот документ является руководством для системных и сетевых администраторов по вопросам обеспечения безопасности при работе в Internet. Документ основан на информации, представленной в RFC 1244, и является результатом коллективной работы многих людей. В число авторов входят: Jules P. Aronson (aronson@nlm.nih.gov), Nevil Brownlee (n.brownlee@auckland.ac.nz), Frank Byrum (byrum@norfolk.infi.net), Joao Nuno Ferreira (ferreira@rccn.net), Barbara Fraser (byf@cert.org), Steve Glass (glass@ftp.com), Erik Guttman (erik.guttman@eng.sun.com), Tom Killalea (tomk@nwnet.net), Klaus-Peter Kossakowski (kossakowski@cert.dfn.de), Lorna Leone (lorna@staff.singnet.com.sg), Edward.P.Lewis (Edward.P.Lewis.1@gsfc.nasa.gov), Gary Malkin (gmalkin@xylogics.com), Russ Mundy (mundy@tis.com), Philip J. Nesser (pjnesser@martigny.ai.mit.edu), Michael S. Ramsey (msr@interpath.net).

В дополнение к перечисленным авторам значительный вклад в работу внесли рецензенты, комментарии которых были весьма существенны. К числу таких рецензентов относятся: Eric Luiijf (luiijf@fel.tno.nl), Marijke Kaat (marijke.kaat@sec.nl), Ray Plzak (plzak@nic.mil) и Han Pronk (h.m.pronk@vka.nl).

Joyce Reynolds (ISI) и Paul Holbrook (CICnet) заслуживают особой благодарности за их работу по созданию первой версии этого руководства. Рабочая группа, подготовившая новую версию, искренне надеется, что этот документ будет столь же полезен, как и его предшественник.

1.1 Цель

Этот документ является руководством по установке правил и процедур защиты для компьютеров и сайтов, подключенных к сети Internet (приведенная здесь информация будет полезна и для сайтов, которые еще не связаны с Internet). В документе рассматриваются различные вопросы, связанные с обеспечением безопасности, приведено множество рекомендаций и обсуждаются различные вопросы, связанные с безопасностью.

Документ является лишь основой для разработки и реализации политики безопасности и процедур защиты. Для создания эффективной системы защиты потребуется реализация комплекса мер.

1.2 Аудитория

Документ адресован системным и сетевым администраторам, а также принимающим решения менеджерам сайтов. Для краткости будем использовать термин «администратор» для обозначения системных и сетевых администраторов.

Данный документ не предназначен для программистов и тех, кто пытается создавать защищенные программы или системы. Документ посвящен в основном политике и процедурам, требуемым для обеспечения технических аспектов безопасности, которые могут быть реализованы на сайте.

Рассматриваемые в этом документе вопросы относятся в основном к сайтам, являющимся членами сообщества Internet. Однако документ будет полезен для любых сайтов, которые соединены с другими сайтами. Как общее руководство по вопросам безопасности этот документ может быть полезен даже для изолированных сайтов.

1.3 Определения

Термином «сайт» в этом документе обозначается любая организация, имеющая свои компьютерные или сетевые ресурсы. К таким ресурсам могут относиться хост-системы, маршрутизаторы, терминальные серверы, ПК и другие устройства, которые могут иметь доступ в Internet. Сайт может быть конечным пользователем сервиса Internet или предоставлять в сеть свои услуги. Большая часть этого документа посвящена пользовательским сайтам. Предполагается, что сайт имеет возможность выбрать для себя правила (политику) и процедуры обеспечения безопасности по согласованию и при поддержке владельцев соответствующих ресурсов. Предполагается также, что сайты, являющиеся частью более крупной организации, знают с кем им нужно консультироваться, сотрудничать или получать рекомендации в родительской компании.

Термин «Internet» используется для обозначения множества сетей, соединенных между собой на базе общего набора технических протоколов, позволяющего пользователям любой из сетей обмениваться данными с пользователями других сетей или использовать ресурсы, расположенные в других сетях (FYI4, RFC 1594).

Термин «администратор» используется для обеспечения тех, кто отвечает за повседневную работу систем или сетей. Администраторами могут быть как отдельные люди, так и целые организации.

Термин «администратор безопасности» используется применительно к людям, которые отвечают за безопасность информации и информационных технологий. На некоторых сайтах администраторами безопасности являются специальные сотрудники, а на других эти функции могут возлагаться на системных или сетевых администраторов.

Термин «лицо, принимающее решения» используется применительно к тем людям на сайте, которые устанавливают или одобряют (разрешают использовать) политику. Достаточно часто (но не всегда) решения принимаются владельцами ресурсов.

1.4 Связанные работы

Группа Site Security Handbook работает над «Руководством пользователя по вопросам безопасности Internet». Этот документ будет служить практическим руководством для конечных пользователей, предназначенным для оказания помощи в вопросах защиты информации и используемых ресурсов.

1.5 Базовая модель

Этот документ написан, как базовое руководство для разработки плана защиты вашего сайта. Одним из наиболее распространенных путей является использование предложений Файтса (Fites) и др., описанных в работе [Fites 1989]:

(1) Идентификация защищаемых компонент.

(2) Что и от кого будем пытаться защитить.

(3) Определение наиболее вероятных угроз.

(4) Реализация мер, которые будут будут защищать ваши активы с достаточной экономической эффективностью.

(5) Постоянный присмотр и внесение улучшений в систему защиты при обнаружении слабых мест.

Большая часть этого документа посвящена п. (4), но остальные этапы также не могут быть пропущены, если вы избрали эффективный план защиты своего сайта. Одной из прописных истин защиты является допущение о том, что расходы на обеспечение безопасности от угрозы должны быть ниже стоимости восстановления при реализации угрозы. Следует помнить, что в данном случае стоимость включает реальные деньги, репутацию, ущерб от потери доверия и др. Без разумного подхода к выбору того, что следует защищать и от каких угроз, следовать приведенному выше правилу будет затруднительно.

1.6 Оценка риска

1.6.1 Общие вопросы

Одной из наиболее важных причин разработки политики компьютерной безопасности является необходимость обеспечения экономической эффективности системы защиты. Меры защиты могут казаться очевидными, однако достаточно просто ошибиться в выборе точек концентрации усилий. В качестве примера укажем на факт наличия достаточно большого числа публикаций о вторжениях в компьютерные системы, хотя опросы показывают, что многие организации гораздо больше теряют в результате действий своих сотрудников[1].

Анализ рисков включает определение компонент, требующих защиты, и угроз, от которых следует защищаться, а также способов защиты. Сначала нужно оценить все возможные риски, а потом ранжировать их по уровню значимости. Это процесс включает принятие экономически обоснованного решения вопроса о выборе защищаемых компонент. Как было отмечено выше, нет смысла тратить на защиту больше средств, нежели может потребоваться на восстановление или компенсацию ущерба.

Полное рассмотрение вопросов анализа рисков выходит за пределы этого документа. В работах [Fites 1989] и [Pfleeger 1989] даются вводные рекомендации по вопросам оценки рисков. Однако анализ рисков включает два элемента, которые будут кратко рассмотрены в двух следующих параграфах:

(1) идентификация активов;

[1]Их часто называют «инсайдерами» от английского insider. *Прим. перев.*

(2) идентификация угроз.

Для каждого актива основной целью защиты является обеспечение доступности, конфиденциальности и целостности. Каждую угрозу следует оценивать с учетом ее влияния на эти параметры.

1.6.2 Идентификация активов

Первым шагом анализа рисков является идентификация всего, что следует защитить. Некоторые из защищаемых компонент очевидны (важная корпоративная информация, интеллектуальная собственность, компоненты оборудования), а другие могут остаться незамеченными (например, люди, реально использующие систему). Существенной частью этого этапа является создание полного списка того, что может быть связано с вопросами безопасности.

Один из подобных списков предложен Пфлигером в работе [Pfleeger 1989]. Ниже приведен адаптированный вариант этого списка:

(1) **Оборудование**: процессорные модули, платы, клавиатуры, терминалы, рабочие станции, ПК, принтеры, дисковые накопители, коммуникационные линии, терминальные серверы, маршрутизаторы.

(2) **Программы**: исходные коды, объектные модули, утилиты, диагностические программы, ОС, коммуникационные программы.

(3) **Данные**: рабочие копии, сохраненные копии, архивные копии, резервные копии, журналы аудита, базы данных, информация, передаваемая через коммуникационные каналы.

(4) **Люди**: пользователи, администраторы, ремонтники.

(5) **Документация**: на программы, оборудование, систему, процедуры локального администрирования.

(6) **Расходные материалы**: бумага, формы (бланки), ленты, магнитные носители.

1.6.3 Идентификация угроз

После того, как определены требующие защиты активы, необходимо идентифицировать угрозы для этих активов. Угрозы можно также проверить в целях определения возможного ущерба. Это поможет определить, от каких угроз требуется защитить ваши активы. Ниже приведен список различных классов угроз, которые следует принимать во внимание. В зависимости от специфики вашего сайта могут существовать и другие типы угроз, которые также следует учитывать.

(1) Несанкционированный доступ к ресурсам и информации.

(2) Непреднамеренное и/или несанкционированное разглашение информации.

(3) Атака на службы.

2. Политика безопасности

В этом документе будет регулярно упоминаться политика безопасности. Обычно такие упоминания будут включать конкретные рекомендации. Рекомендации по созданию и распространению политики безопасности не будут повторяться и читателю следует применять приведенные в этой главе сведения при разработке той или иной политики, рекомендованной в других главах документа.

2.1 Что такое политика безопасности и зачем она нужна?

Связанные с обеспечением безопасности решения, которые вы принимаете (или не принимаете), как администратор, в значительной мере определяют уровень безопасности вашей сети и удобство пользователей при работе с сетью. Однако невозможно принять хорошее решение в части безопасности без определения на первом этапе целей. Пока вы не определите свои цели в части безопасности, вы не сможете эффективно использовать средства защиты, поскольку вы просто не будете знать, что следует проверять или ограничивать.

Например, ваши цели могут весьма существенно расходиться с целями производителей используемого вами оборудования. Производители пытаются максимально упростить настройку и обслуживание своего оборудования и в результате установленная по умолчанию конфигурация зачастую является слишком открытой (т. е., небезопасной). Такой подход упрощает начальную настройку оборудования, но оставляет возможность доступа к этой системе (и через нее к другим системам) для всех желающих.

Ваши цели станут более определенными после учета перечисленных ниже аспектов:

(1) Поддерживаемые службы и безопасность

Каждый тип сервиса, предоставляемого пользователям, связан с потенциальной опасностью. Для некоторых служб риск может превышать преимущества, обеспечиваемые этой службой, и администратор может просто отказаться от поддержки этого сервиса вместо попыток обезопасить его.

(2) Простота использования и безопасность

Самая простая в использовании система позволяет любому пользователю выполнять какие ему угодно действия и не требует от пользователя пароля - здесь просто речи нет о какой-либо безопасности. Запрос пароля делает систему менее удобной, но более безопасной. Использование генерируемых аппаратными средствами одноразовых паролей усложняет работу с системой, но обеспечивает существенное повышение уровня безопасности.

(3) Расходы на защиту и возможные потери

Обеспечение безопасности связано с множеством издержек - прямые финансовые затраты (стоимость оборудования и программ типа межсетевых экранов и генераторов одноразовых паролей), необходимость повышения производительности (затраты ресурсов на шифрование и дешифровку), усложнение работы

пользователей (см. выше). Существует также много уровней риска - утечка информации (несанкционированный доступ к данным), потеря данных (порча или уничтожение информации), осложнение работы служб (расход пространства в устройствах хранения, использование системных ресурсов, атаки на сетевые службы). Следует учесть все типы расходов и сравнить с возможными потерями.

Политика безопасности должна быть доведена до всех пользователей, технического персонала и менеджеров в виде набора правил. В этом документе используется термин «политика безопасности», а не «политика компьютерной безопасности» по той причине, что данный документ посвящен безопасности всех типов информационных технологий и данных, которые обрабатываются или хранятся с помощью таких технологий.

2.1.1 Определение политики безопасности

Политика безопасности представляет собой формализованный набор правил, которым должны следовать пользователи, имеющие доступ к технологическим и информационным активам.

2.1.2 Цели политики безопасности

Основной целью политики безопасности является информирование пользователей, персонала и менеджеров об обязательных требованиях, связанных с защитой технологических и информационных активов. Эти правила должны описывать механизмы выполнения предъявляемых требований. Другой целью политики безопасности является обоснование стратегии и тактики приобретения, настройки конфигурации и аудита компьютерных систем и сетей в соответствии с заданной политикой. Следовательно, попытка использования набора средств обеспечения безопасности при отсутствии хотя бы подразумеваемой политики безопасности просто не имеет смысла.

Правила допустимого использования (AUP[1]) могут быть включены как часть политики безопасности. Эти правила должны содержать список того, что пользователям разрешено и запрещено делать по отношению к различным компонентам системы, включая описание типов трафика, разрешенного в сети. Правила AUP следует делать максимально явными и однозначными во избежание их непонимания и ложных толкований. Например, AUP может содержать список запрещенных конференций USENET.

2.1.3 Кто должен участвовать в формировании политики?

Для того, чтобы политика безопасности была эффективной и удобной, она должна учитывать потребности всех уровней сотрудников организации. Особенно важно, чтобы руководство компании полностью поддерживало политику безопасности, поскольку в противном случае вероятность реализации этой политики становится сомнительной. Ниже приведен список людей, которых следует привлечь к процессу разработки и утверждения документов, связанных с политикой безопасности.

(1) администратор безопасности сайта;

(2) технический персонал ИТ (например, сотрудники компьютерного центра);

(3) администраторы больших групп пользователей (например, подразделений компании, факультетов учебного заведения и т. п.);

(4) команда по расследованию инцидентов;

(5) представители групп пользователей, на которые оказывает влияние политика безопасности;

(6) руководство компании;

(7) юристы (если это приемлемо).

Приведенный выше список подходит для большинства организаций, но он не является всеобъемлющим. Идея заключается в том, чтобы в разработке политики безопасности принимали участие представители основных групп пользователей, руководители, решающие вопросы финансирования и утверждающие политику, технический персонал, который знает, что можно и что нельзя сделать, а также юристы, которые могут подтвердить законность требований политики. В некоторых организациях целесообразно также привлекать специалистов по аудиту электронной обработки данных (EDP[2]). Включение этой группы достаточно важно, если требуется обеспечить одобрение политики максимально широким кругом пользователей. Отметим также, что привлечение юристов к разработке политики безопасности может быть связано с законодательством вашей страны.

2.2 Что хорошо для политики безопасности?

Ниже приведены отличительные черты хорошей политики.

(1) Политика должна быть реализуемой путем процедур системного администрирования, публикации правил допустимого использования и других подходящих методов.

(2) Политика должна быть выполняемой с помощью средств защиты, когда это приемлемо, и путем применения санкций в тех случаях, когда технические меры неприменимы.

(3) Политика должна четко и ясно определять сферы ответственности для пользователей, администраторов и руководства.

Хорошая политика безопасности включает:

(1) Рекомендации по приобретению оборудования, указывающие требуемые или предпочтительные функции защиты. Эти рекомендации следует делать дополнением к существующим правилам и рекомендациям по приобретению оборудования.

(2) Правила конфиденциальности, которые определяют разумные ожидания пользователей в сфере сохранения конфиденциальности, включая мониторинг электронной почты, запись информации о нажатии клавиш и доступ к файлам пользователей.

[1]Appropriate Use Policy или Acceptable Use Policy.
[2]Electronic data processing. *Прим. перев.*

(3) Правила доступа, которые определяют права доступа и привилегии для защиты активов от потери или разглашения путем указания допустимых действий для пользователей, технического персонала и руководства. Эти правила должны включать рекомендации по организации внешних соединений, обмену данными, подключению устройств к сети, установке программ. Следует также описать все требуемые уведомления (например, при подключении следует выдавать сообщение о правилах доступа и мониторинге линии, а не просто сообщение «Добро пожаловать»).

(4) Меры ответственности, которые определяют обязанности пользователей, технического персонала и руководства. В этих правилах должна указываться возможность аудита и приводиться руководство по расследованию инцидентов (например, что следует делать и к кому обращаться при обнаружении возможного вторжения в систему).

(5) Правила идентификации, которые позволяют предоставлять доверенным пользователям доступ на основе паролей, а также рекомендации по идентификации удаленных пользователей и применения специальных устройств (например, средств генерации одноразовых паролей).

(6) Условия доступа, включающие информацию для пользователей о доступности ресурсов, вопросы резервирования и восстановления, а также часы работы и периоды остановки для обслуживания. Здесь же следует указать контактную информацию для обращения в случаях отказов.

(7) Правила обслуживания систем и сети, в которых описываются вопросы обслуживания систем и сети внутренним и внешним техническим персоналом. Важно указать здесь возможность удаленного обслуживания и способы контроля доступа при таком обслуживании. Следует также описать здесь возможность и условия аутсорсинга при обслуживании.

(8) Правила информирования о нарушениях, в которых описано, о каких типах нарушений (например, конфиденциальность и безопасность, внутренние или внешние) и кому следует сообщать. Возможность анонимно сообщать о нарушениях и понимание того, что информатору ничего не грозит, будет повышать вероятность того, что пользователи будут сообщать о замеченных нарушениях.

(9) Информация о поддержке с контактной информацией для всех типов нарушений, рекомендации по обработке внешних запросов по поводу связанных с безопасностью инцидентов, список информации, которая может рассматриваться как конфиденциальная, ссылки на связанную с обеспечением безопасности информацию (политика компании, законодательные акты и т. п.).

Могут существовать требования законодательства, которые оказывают влияние на те или иные аспекты вашей политики безопасности (например, мониторинг линий). Разработчикам политики следует проконсультироваться с юристами и, как минимум, показать политику юрисконсульту предприятия.

После создания политики безопасности ее нужно довести до сведения пользователей, технического персонала и руководства. Сбор подписей всего персонала об ознакомлении, понимании и согласии с политикой безопасности является важным этапом. В дальнейшем политику следует регулярно просматривать для того, чтобы понять насколько она соответствует требованиям безопасности.

2.3 Обеспечение гибкой политики

Для того, чтобы политику безопасности можно было использовать в течение долгого срока, эта политика должна обеспечивать достаточную гибкость, основанную на использовании концепций архитектуры безопасности. Политику безопасности следует делать (в значительной мере) независимой от программных и аппаратных компонент (та или иная компонента может быть заменена или перемещена в любой момент). Механизмы обновления политики должны быть понятными. Следует включать в описание процессы обновления, людей которые участвуют в этих процессах, а также тех, кто подписывает обновленную политику.

Важно также понимать, что для каждого правила существуют определенные ожидания. По возможности такие ожидания следует включать в политику. Например, следует указывать, при каких условиях системному администратору разрешено просматривать пользовательские файлы. Также следует оговорить возможность работы в системе множества пользователей с одним именем. Например, имя root может использоваться группой администраторов, которым известен пароль учетной записи root.

Следует также принять во внимание Garbage Truck Syndrome[1]. Это относится к ситуациям, когда кто-то из ключевых фигур сайта неожиданно становится недоступным на своей работе (например, внезапно заболеет или уволится из компании). Хотя лучшим способом обеспечения безопасности информации является ее нераспространение, однако риск потери критически важной информации возрастает, если эта информация известна лишь одному лицу. Вам нужно найти для своего сайта разумный компромисс.

3. Архитектура

3.1 Задачи

3.1.1 Детальное планирование защиты

Для всех сайтов следует создавать детальный план обеспечения безопасности. Этот план должен иметь более высокий уровень, нежели политика безопасности, которая обсуждалась в главе 2, и служить руководством при создании политики безопасности.

Важно обеспечить согласованность этого плана в виде реализованной в его рамках политики безопасности с общей архитектурой защиты сайта. Например, при использовании жестких ограничений для доступа в Internet в сочетании с либеральностью по отношению к использованию модемов, возникает отчетливая несогласованность.

В план обеспечения безопасности следует включать общий список всех поддерживаемых сетевых служб, подразделения, которые будут поддерживать эти службы, доступ конкретных пользователей к службам, способы обеспечения доступа, список администраторов служб и т. п.

[1]Синдром мусорной тележки.

В плане также следует описать процедуры расследования инцидентов. В главе 5 этот вопрос рассматривается подробно, но важно сейчас подчеркнуть, что для каждого сайта должны быть определены классы инцидентов и соответствующая реакция на них. Например, сайтам с межсетевыми экранами следует устанавливать пороговое значение для числа попыток, отражаемых межсетевым экраном, после которого будут приниматься соответствующие меры. Уровни эскалации следует определять, как для атак, так и для реакции на них. Для сайтов без межсетевого экрана следует определить, является ли единственная попытка подключения к хосту инцидентом, требующим реакции. Следует также определить свое отношение к систематическому сканированию систем.

Для сайтов, подключенных к Internet, решение вопросов связанных с инцидентами в результате атак из Internet, может (потенциально) отвлечь внимание от многих серьезных внутренних проблем защиты. Для сайтов, которые ранее не были подключены к Internet и имеют мощную, хорошо определенную внутреннюю политику безопасности, подключение к Internet может потребовать существенного пересмотра политики безопасности.

3.1.2 Разделение служб

Существует множество служб, которые сайт может поддерживать для своих пользователей; некоторые из служб могут быть доступны извне. Существует множество причин локализации служб на специально выделенных для этого хостах. Во многих случаях такая локализация связана также с вопросами производительности, но этот вопрос выходит за рамки документа.

Службы, которые может поддерживать сайт, в большинстве случаев существенно различаются по уровню требуемого доступа и моделям поддержки доверия. Службы, которые имеют важное значение для безопасности и нормальной работы сайта, лучше разместить на выделенной машине с более ограниченным доступом к ней (см. модель «запретить все» в параграфе 3.1.3), нежели на машине, которая обеспечивает службы, являющиеся менее защищенными или требующими более высокого уровня доступа для пользователей, которые могут неумышленно нарушать требования безопасности.

Важно также разделять хосты, которые используют различные модели доверия (например, хосты, защищенные межсетевым экраном, и хосты, непосредственно доступные извне).

Некоторые службы, которые следует отделять одну от другой, рассматриваются кратко в параграфе 3.2.3. Важно помнить о том, что уровень безопасности определяется наиболее слабым звеном в цепочке. Несколько наиболее известных вторжений последних лет было осуществлено путем использования уязвимостей в системах электронной почты. Злоумышленники не пытались красть электронную почту, а использовали уязвимости этого сервиса для получения доступа к другим системам.

По возможности каждую службу хорошо организовать на отдельной машине, которая используется только для поддержки этой службы. Такое разделение позволит изолировать попытки вторжения и ограничить потенциальный ущерб.

3.1.3 Разрешить/запретить все

Существуют две диаметрально противоположные базовые модели, которые могут быть адаптированы при определении политики безопасности. Оба варианта подходят для адаптации и выбор той или иной модели зависит от сайта и его потребностей в защите.

В первой модели отключаются все службы и после этого некоторые службы включаются по мере возникновения необходимости в них. Такая модель может быть реализована на уровне хостов или сети. Эта модель, которую далее будем называть deny all[1], в общем случае обеспечивает более высокий уровень защиты, нежели вторая модель, описанная ниже. Модель достаточно трудоемка в реализации и требует глубокого понимания механизмов работы служб. Дозволение использования только известных служб упрощает анализ отдельных служб/протоколов и разработку механизмов защиты на уровне сайта в целом.

Другая модель, которую мы будем называть allow all[2], проще в реализации, но в общем случае обеспечивает более низкий уровень защиты, нежели модель deny all. В этой модели просто включаются все службы (обычно на уровне хостов) и разрешается поддержка в сети всех протоколов (обычно на уровне маршрутизаторов). По мере обнаружения прорех в защите они ограничиваются или прикрываются «заплатами» на уровне хостов или сети.

Для той или иной части сайта может применяться любая из этих моделей в зависимости от функциональных требований, административного контроля, политики сайта и т. д. Например, политика может использовать модель allow all для рабочих станций общего назначения и модель deny all для информационных серверов типа сервера электронной почты. Подобно этому, политика allow all может использоваться для трафика между локальными сетями сайта, а для передачи данных между сайтом и Internet – политика deny all.

При использовании обоих вариантов политики следует соблюдать осторожность. Многие сайты выбирают жесткую политику для периметра и мягкую внутреннюю политику. Они вправе использовать дорогостоящие системы обеспечения безопасности и строгие меры для внешнего трафика, но не могут или не хотят реализовать подобную защиту внутри. Если защиту периметра (межсетевой экран) удастся преодолеть, то при использовании такой модели проникновение во внутреннюю сеть становится тривиальной задачей.

3.1.4 Определение реальных потребностей в службах

Существует широкий спектр сетевых служб, как реализованных внутри сайта, так и тех, к которым пользователи обращаются через Internet. Обеспечение безопасности во многих случаях связано с управлением доступом к службам внутри сайта, а также с управлением доступом внутренних пользователей к информации на удаленных сайтах.

Создание новых типов сервиса волнами проходит через Internet. За долгие годы на многих сайтах создавались серверы FTP с анонимным доступом, серверы gopher, wais, WWW и т. п., по мере роста популярности того или иного типа сервиса, но не все эти службы нужны на каждом сайте. Оценка новых типов сетевого сервиса с долей здорового скептицизма помогает понять, действительно ли эта служба является достаточно нужной или это очередная смена моды в Internet.

[1]Запретить все.
[2]Разрешить все.

Помните, что сложность системы защиты экспоненциально растет с увеличением числа поддерживаемых служб. Для поддержки новых протоколов требуется обновлять фильтры маршрутизаторов. Некоторые протоколы весьма сложны в точки зрения фильтрации (например, службы RPC и UDP) и использование таких протоколов делает сеть более открытой. Службы, организованные на одной машине, могут взаимодействовать между собой самыми причудливыми (и катастрофическими) способами. Например, организация сервера FTP с анонимным доступом на одной машине с сервером WWW может привести к тому, что атакующий разместит файлы в области диска, доступной анонимным пользователям FTP и с помощью сервера HTTP инициирует исполнение содержащихся в файлах программ.

3.2 Настройка сети и служб

3.2.1 Защита инфраструктуры

Многие администраторы затрачивают значительные усилия на защиту хостов своей сети и лишь немногочисленные защищают саму сеть. В этом есть рациональное зерно. Например, защитить хост гораздо проще, нежели сеть. Весьма вероятно также, что атакующих интересует прежде всего доступ к данным на хосте и нарушение работы сети не способствует решению их задач. Тем не менее существуют причины, по которым следует защищать саму сеть. Например, атакующий может изменить маршрут передачи трафика, направив его через внешний хост, на котором данные будут просматриваться (например, в поисках паролей). Сетевая инфраструктура включает множество сетей и соединяющих эти сети маршрутизаторов. Кроме того, сетевая инфраструктура включает системы сетевого управления (например, SNMP), различные службы (типа DNS, NFS, NTP, WWW) и средства обеспечения безопасности (механизмы аутентификации пользователей и ограничения доступа).

Инфраструктура также требует защиты от ошибок, присущих людям. Когда администратор некорректно настроит конфигурацию хоста, производительность служб на таком хосте может сильно снизиться. Это оказывает влияние лишь на тех пользователей, которым нужны соответствующие службы, и число таких пользователей будет ограничено. Если же ошибки будут в конфигурации маршрутизатора, они окажут влияние на всех пользователей, которым нужна сеть. Обычно число пользователей сети существенно выше числа пользователей служб того или иного хоста.

3.2.2 Защита сети

Существует несколько проблем, которые делают сети уязвимыми. Классической проблемой являются атаки, направленные на отказ служб - DoS[1]. Эти атаки вынуждают сеть перейти в такое состояние, в котором она уже не способна передавать данные легитимных пользователей. Существует два наиболее распространенных варианта достижения такой цели – атака на маршрутизаторы и организация лавины дополнительного трафика (flooding). Отметим, что термин «маршрутизатор» в данном случае обозначает широкий класс активных компонент организации межсетевых соединений, который может включать такие узлы, как межсетевые экраны, прокси-серверы и т. п.

Атаки на маршрутизаторы предпринимаются с целью остановки пересылки пакетов между сетями или искажения картины пересылки. Второй вариант может быть связан с изменением конфигурации, вставкой поддельных маршрутных обновлений или лавинной атакой («бомбардировкой» маршрутизатора немаршрутизируемыми пакетами, приводящей к затрате значительных ресурсов и снижению производительности). Лавинная атака на сеть похожа на такую же атаку на маршрутизатор, но обычно использует для «бомбардировки» широковещательные пакеты. Идеальной лавинной атакой явилась бы генерация и вставка единственного пакета, который, используя тот или иной известный дефект в узле сети, заставит последний повторить передачу этого пакета или начать генерацию ошибочных пакетов, каждый из которых будет принят и заново передан в сеть другим хостом. Грамотно подготовленный стартовый пакет может даже спровоцировать экспоненциальный рост числа повторов передачи.

Другой классической проблемой является подмена адресов - spoofing. В этом случае подложные обновления маршрутов передаются одному или нескольким маршрутизаторам, вынуждая их пересылать пакеты по неправильным маршрутам. Такая атака отличается от атаки на службы по своим целям. В атаках на отказ служб задачей является утрата маршрутизатором работоспособности, а это состояние достаточно легко обнаруживается пользователями сети. При использовании спуфинга подмена маршрутов будет приводить к изменению путей доставки пакетов, что позволяет атакующему направить их на специальный хост, способный обеспечить возможность мониторинга данных в пакетах. После просмотра пакеты могут быть возвращены на путь к исходному адресату. Отметим, что атакующий также имеет возможность изменения перехватываемых пакетов.

Решение большинства таких проблем заключается в защите пакетов с обновлениями маршрутов, передаваемых протоколами маршрутизации (например, RIP-2, OSPF). Существует три вида защиты - незашифрованные пароли, криптографические контрольные суммы и шифрование. Пароли зачастую обеспечивают наименьший уровень защиты, который может помочь, если атакующий не имеет прямого доступа к физической сети. Использование паролей также обеспечивает некоторый уровень защиты от маршрутизаторов с некорректной конфигурацией. Преимуществом парольной защиты является незначительная дополнительная нагрузка на систему (малый расход полосы и процессорного времени). Контрольные суммы защищают от вставки подложных пакетов даже при наличии у атакующего физического доступа в сеть. В комбинации с порядковыми номерами или иными уникальными идентификаторами, контрольные суммы могут также обеспечивать защиту от replay-атак, при которых атакующим или некорректно настроенным маршрутизатором заново передается старое, но еще корректное обновление маршрутов. Максимальную защиту обеспечивает полное шифрование упорядоченных или имеющих уникальные идентификаторы обновлений маршрутизации. Такой вариант не позволяет атакующему определить топологию сети. Недостатком шифрования является значительное увеличение нагрузки на процессор при обработке маршрутных обновлений.

Протоколы RIP-2 (RFC 1723) и OSPF (RFC 1583) поддерживают нешифрованные пароли. Кроме того, эти протоколы поддерживают расширения, которые позволяют использовать шифрование (хэширование) MD5.

К сожалению не существует адекватной защиты от лавинных атак и некорректного поведения хостов или маршрутизаторов, поддерживающих лавинную пересылку пакетов. К счастью такие атаки достаточно просто обнаружить и блокировать.

[1] Denial of service.

3.2.3 Защита служб

Существует множество разнотипных служб и каждая из них предъявляет свои требования в части безопасности. Зачастую такие требования основаны на специфике использования той или иной службы. Например, сервис, который должен быть доступен только в пределах сайта (скажем, NFS), может требовать полной блокировки доступа извне. Однако сервер WWW, предназначенный для просмотра через Internet, также требует защиты (т. е., требуется система предотвращения несанкционированного доступа и изменения содержимого документов).

Внутренние (т. е., предназначенные для использования только внутри сайта) и внешние (с определенными предосторожностями открытые для доступа извне) службы будут, в общем случае, предъявлять разные требования в части защиты, как было сказано выше. Из этого следует, что разумно разделить хосты, на которых будут поддерживаться внутренние и внешние службы. Т. е., внутренние и внешние службы не следует совмещать на одном хосте. На практике достаточно часто поступают именно так и используют один набор подсетей (или даже различные сети) для предоставления доступа извне и другой набор адресов, доступ к которым открыт только в пределах данного сайта. Естественно, что между этими частями устанавливается межсетевой экран. Следует принять меры предосторожности для обеспечения корректной работы такого экрана и эффективного выполнения функций фильтрации.

Возрастает интерес к использованию технологий intranet для соединения различных частей организации (например, подразделений компании). Данный документ в общем случае различает внутренние и внешние (приватные и публичные) службы и сайтам, использующим технологии intranet, следует осознать необходимость рассмотрения вопроса о разделении таких служб во всей инфраструктуре и принять соответствующие меры при разработке и развертывании служб. Сервис, предлагаемый в intranet, не может быть отнесен ни к внутренним, ни к внешним. Следовательно, такой сервис должен быть отделен как от внутренних, так и от внешних служб и сетей.

Одна из форм внешнего доступа заслуживает специального рассмотрения. Это анонимный или гостевой доступ. Примерами такого сервиса являются FTP с анонимным доступом или гостевая регистрация в системе (login) без идентификации пользователя. Очень важно обеспечить изоляцию серверов FTP с анонимным доступом и хостов с гостевым входом в систему от остальных хостов и файловых систем. Другим важным аспектом анонимного доступа является возможность записи на диск. Сайт может нести юридическую ответственность за содержимое доступных публично документов и файлов, поэтому рекомендуется обеспечивать мониторинг информации, сохраненной анонимными пользователями.

Далее мы рассмотрим некоторые службы из числа наиболее важных - серверы имен, серверы паролей/ключей, серверы идентификации, электронная почта, WWW, файловые серверы и NFS. Поскольку эти службы наиболее распространены, они являются частыми объектами атак. Кроме того, успешная атака на одну из таких служб может оказать существенное влияние на работу других служб.

3.2.3.1 Серверы имен (DNS и NIS(+))

В сети Internet используется система доменных имен DNS[1] для преобразования имен хостов в адреса IP и обратно. Службы NIS[2] и NIS+ не столь широко распространены в Internet, однако подвержены такому же риску, как и серверы DNS. Преобразование имен в адреса играет важнейшую роль в обеспечении безопасности работы любой сети. Атакующий, которому удалось захватить управление сервером DNS, сможет перенаправить трафик и обойти систему защиты. Например, обычный трафик может быть направлен на контролируемую атакующим систему мониторинга или пользователей можно направить на подставной сервер аутентификации для перехвата паролей. Организации следует создать хорошо известные и надежно защищенные сайты, которые будут функционировать как вторичные серверы имен и защищать основные серверы DNS от DoS-атак с использованием фильтров на маршрутизаторах.

В общем случае DNS не имеет встроенных систем защиты. В частности, информация, возвращаемая по запросу, не может быть проверена на предмет искажения, а также не поддерживается возможность проверки получения отклика именно от того сервера, которому был направлен запрос. Ведутся работы по встраиванию в протокол цифровых подписей, которые позволяли бы проверять целостность информации (см. RFC 2065).

3.2.3.2 Серверы паролей/ключей (NIS(+) и KDC)

Серверы паролей и ключей в общем случае применяются для защиты жизненно важной информации (т. е., паролей и ключей) с использованием алгоритмов шифрования. Однако даже шифрованные пароли можно определить с помощью атак по словарю (когда слова общего назначения шифруются и сравниваются с хранящимся в системе зашифрованным паролем). Следовательно, для таких серверов нужно предотвратить возможность доступа с хостов, которые не планирует использовать эти серверы для поддержки своей работы, и даже для хостов, которым доступ разрешен, этот доступ должен быть ограничен только соответствующими службами (например, службы общего назначения, Telnet и FTP на таких серверах не следует делать доступными для кого-либо за исключением администраторов).

3.2.3.3 Серверы аутентификации и прокси-серверы (SOCKS, FWTK)

Прокси-серверы[3] обеспечивают множество механизмов защиты. Такие серверы позволяют организовать доступ к службам через специальный хост, который позволяет осуществлять мониторинг, скрывает внутреннюю структуру и т. д. В силу этого прокси-серверы являются заманчивой целью для атак. Тип защиты, требуемой для прокси-сервера в значительной степени определяется используемым протоколом и набором служб, для которых обеспечиваются посреднические функции. Общее правило ограничения доступа состоит в том, что доступ следует предоставлять только к тем хостам, на которых реализованы соответствующие службы, и доступ этот следует ограничивать лишь разрешенными службами. Это правило будет хорошей стартовой точкой.

3.2.3.4 Электронная почта

Системы электронной почты достаточно давно являются мишенью для атак, поскольку протоколы обмена почтовыми сообщениями являются одними из старейших и наиболее распространенных сетевых протоколов. Кроме того, по своей природе сервер электронной почты должен обеспечивать доступ из внешних сетей и многие серверы обеспечивают

[1]Domain Name System.
[2]Network Information Service – сетевая информационная служба.
[3]Proxy - посредник.

доступ с любого хоста. В общем случае сервер электронной почты состоит из 2 частей - агента приема-передачи и агента обработки сообщений. Поскольку электронная почта доставляется всем пользователям и обычно является приватной, агент обработки должен работать с правами system (root) для того, чтобы обеспечить доставку сообщений пользователям. Многие реализации систем электронной почты выполняют обе функции и это означает, что принимающий сообщения агент также имеет системные привилегии. При таком подходе в системе возникает несколько уязвимых мест, которые в данном документе не рассматриваются. Существуют реализации систем электронной почты, позволяющие разделить оба агента. Такие реализации в общем случае являются более безопасными, но и они требуют осторожной инсталляции чтобы избежать проблем с безопасностью.

3.2.3.5 WWW

Популярность Web растет экспоненциально, благодаря простоте использования и развитым возможностям концентрации информационных услуг. Большинство серверов WWW[2] воспринимают от своих пользователей некоторые типы директив и действий. Наиболее типичным примером может служить получение запроса от удаленного пользователя и передача предоставленной информации некой программе, работающей на сервере, для обработки запроса. Некоторые программы-обработчики не обеспечивают должной защиты и создают бреши в системе обеспечения безопасности («дыры в защите»). Если Web-сервер доступен сообществу Internet, особенно важно избегать хранения на одном хосте с сервером конфиденциальной информации. Фактически, рекомендуется выделять для сервера отдельный хост и не рассматривать его, как доверенный для других внутренних хостов.

Многие сайты желают совмещать на одном хосте серверы FTP и WWW. Однако это следует делать только для серверов FTP с анонимным доступом, которые позволяют лишь загружать файлы с сервера (ftp-get). Операции записи на анонимный сервер FTP, совмещенный с сервером WWW, могут вызывать опасность (например, возможность изменения содержимого Web-сервера), а требования по защите для каждой службы различаются.

3.2.3.6 Файловые серверы (FTP, TFTP)

FTP и TFTP обеспечивают пользователям возможность получения и передачи файлов в режиме «точка-точка». Однако FTP требует идентификации пользователя, а TFTP всегда позволяет действовать анонимно. По этой причине серверы TFTP не следует использовать без необходимости.

Некорректно настроенные серверы FTP могут позволить нарушителю копирование, замену и удаление файлов по его усмотрению, независимо от их размещения на сервере, поэтому корректная настройка конфигурации сервера очень важна. Доступ к зашифрованным паролям или приватной информации, а также внедрение троянских программ являются примерами потенциальных дыр в защите, которые могут возникать при некорректной настройке серверов. Серверы FTP следует размещать на выделенных хостах. На некоторых сайтах серверы FTP и Web размещают на одном хосте, поскольку два протокола используют общий подход к защите. Однако на практике совместное размещение серверов не рекомендуется, особенно в тех случаях, когда FTP позволяет размещать файлы на сервере (см. параграф WWW выше). Как было отмечено в начале параграфа 3.2.3, службы, предлагаемые внутри сайта не следует размещать вместе со службами, доступными извне. Каждой следует выделять отдельный хост.

TFTP не поддерживает полной функциональности FTP и не обеспечивает какой-либо защиты. Этот сервис следует применять лишь для внутреннего доступа и настраивать так, чтобы ограничивать доступ лишь конкртеным набором предопределенных файлов (взамен доступа ко всем открытым на чтение файлам в системе). Возможно наиболее распространенным применением протокола TFTP является загрузка параметров конфигурации в маршрутизаторы[3]. TFTP следует размещать на отдельном хосте и не следует устанавливать на хостах, обеспечивающих доступ извне к службам FTP или Web.

3.2.3.7 NFS

NFS[4] позволяет хостам совместно использовать диски. NFS часто применяется на бездисковых хостах, которые для всех своих задач пользуются дисками серверов. К сожалению NFS не имеет встроенных средств защиты. Следовательно, требуется обеспечить, чтобы доступ к серверу NFS могли получить только те хосты, которым этот сервис необходим. Это достигается путем указания хостов, которым экспортируется файловая система и режим доступа (например, read-only - только чтение, read-write - чтение и запись и т. п.). Файловые системы не следует экспортировать каким-либо хостам за пределами локальной сети, поскольку это потребует открыть внешний доступ к сервису NFS. В идеале внешний доступ к сервису NFS следует закрывать на межсетевом экране.

3.2.4 Защита средств защиты

Поразительно, как часто сайты, уделяющие пристальное внимание своей безопасности, оставляют средства защиты открытыми для атак. Основываясь на приведенном выше обсуждении, следует прояснить этот вопрос. Серверы защиты не следует делать доступными извне, а также следует предоставлять внутренним пользователям минимальный уровень доступа к таким серверам за исключением доступа к функциям идентификации. Кроме того, серверы защиты не следует совмещать на одном хосте с любыми другими серверами. Более того, весь доступ к узлу, включая доступ к самому сервису, следует протоколировать в журнальном файле для обеспечения возможности анализа инцидентов.

3.3 Межсетевые экраны

Одним из наиболее широко распространенных и рекламируемых средств защиты в Internet является межсетевой экран (МСЭ, брандмауэр, firewall). Межсетевые экраны считаются панацеей от многих, если не всех, сетевых угроз в Internet. Это ошибочная точка зрения. Межсетевые экраны являются лишь одним из средств защиты. Они обеспечивают некий уровень защиты и средства реализации политики безопасности на уровне сети. Уровень защиты, обеспечивемый межсетевым экраном, может меняться в широких пределах, как и уровень защиты на конкретной машине. Здесь присутствуют обычные компромиссы между защитой, простотой использования, ценой сложностью и т. п.

---

[2] World Wide Web - «всемирная паутина».

[3] В настоящее время этот протокол достаточно широко используется для загрузки образов программного кода в различные устройства (маршрутизаторы, коммутаторы и пр.). *Прим. ред.*

[4] Network File Service - сетевая файловая служба (система).

Межсетевой экран представляет собой один из нескольких механизмов, используемых для контроля и присмотра за доступом в сеть и доступом наружу из сети с целью защиты сети. Межсетевой экран действует, как шлюз, через который проходит весь трафик в защищаемую сеть (систему) и/или из нее. Межсетевые экраны помогают наложить ограничения на объем и тип взаимодействия между защищаемой сетью и другими сетями (например, Internet или сетью другого сайта).

Межсетевой экран в общем случае обеспечивает способ построения «стены» между разными частями сети (например, сетями подразделений компании). Уникальным свойством такой стены является то, что она «прозрачна» для некого трафика с заданными характеристиками, оставаясь преградой для прочего трафика. Сложной задачей является формулировка критериев, по которым пакетам разрешается или запрещается проходить через межсетевой экран. Книги, посвященные межсетевым экранам, используют разную терминологию для описания различных видов брандмауэров. Это может вводить в заблуждение администраторов, недостаточно хорошо знакомых с межсетевыми экранами. Важно отметить отсутствие общепринятой терминологии описания межсетевых экранов[1].

Типичный межсетевой экран представляет собой отдельную машину, хотя это не всегда так. В отдельных случаях МСЭ образуется из комбинации маршрутизаторов, сетевых сегментов и хост-компьютеров. Следовательно, в контексте этого документа термин МСЭ может подразумевать наличие множества физических устройств. Обычно МСЭ создаются с использованием двух разных компонент — фильтрующих маршрутизаторов и прокси-серверов.

Фильтрующие маршрутизаторы являются простейшими компонентами в концепции межсетевого экранирования. Маршрутизаторы перемещают данные туда и обратно между двумя (или несколькими) сетями. «Обычный» маршрутизатор берет маршрутизатор из сети A и направляет его в другую сеть B. Фильтрующий маршрутизатор делает то же самое, но принимает решение не только о выборе сети для отправки пакета, но и о целесообразности маршрутизации конкретного пакета. Это выполняется за счет организации цепочек фильтров в соответствии с которыми маршрутизатор решает судьбу каждого пакета данных.

Обсуждение возможностей конкретных моделей маршрутизаторов с определенными версиями программ выходит за рамки этого документа. Однако при оценке маршрутизатора, который будет служить для фильтрации пакетов, следует принимать во внимание возможности фильтрации по следующим критериям: IP-адреса отправителя и получателя, номера портов TCP у отправителя и получателя, состояние флага ack для TCP, номера портов UDP у отправителя и получателя, направление потока пакетов (A->B или B->A). Другим важным при создании надежной системы фильтрации пакетов аспектом является возможность изменения маршрутизатором порядка применения фильтров (обычно это делается в целях оптимизации, но иногда может привести к существенному изменению политики фильтрации и предоставлению нежелательного доступа), а также применение фильтров к входящим и исходящим пакетам на каждом интерфейсе (если маршрутизатор фильтрует только исходящие пакеты, тогда он сам окажется за пределами действия фильтров и может стать объектом атаки). Кроме защиты самого маршрутизатора отдельные фильтры для входящих и исходящих пакетов имеют большое значение для маршрутизаторов с числом интерфейсов больше 2. Другим важным аспектом является возможность создания фильтров на основе опций заголовка IP и состояния фрагментации. Создание хорошей системы фильтрации может оказаться сложной задачей, требующей глубокого понимания разных типов услуг (протоколов) для которых организуются фильтры.

Для обеспечения защиты фильтры обычно ограничивают возможности прямого взаимодействия между соединенными сетями, разрешая доступ в обе сети только одному хосту (бастиону). Любое взаимодействие между разными сетями осуществляется только через бастион. Это ведет к тому, что только этот хост остается в качестве возможной цели для атаки из другой сети. Обеспечить высокий уровень защиты для одного хоста существенно проще, нежели сделать это для каждого хоста сети. Для обеспечения доступа легитимных пользователей к сетевым ресурсам через МСЭ соответствующие запросы пересылаются хосту-бастиону. Некоторые службы имеют встроенные возможности пересылки запросов (например, серверы DNS или SMTP), а для остальных (например, Telnet, FTP и т. п.) приходиться использовать специальные серверы-посредники (proxy — прокси) для безопасного доступа к сетевым ресурсам через МСЭ.

Прокси-сервер обеспечивает способ концентрации прикладных служб на одной машине. Обычно такой сервер является одной машиной (бастион), которая служит посредником для разных протоколов (Telnet, SMTP, FTP, HTTP и т. п.), но возможно использование отдельного компьютера для каждого сервиса. Вместо подключения к внешним серверам напрямую клиенты соединяются с сервером-посредником, который, в свою очередь, инициирует соединение с нужным клиенту внешним сервером. В зависимости от типа используемого прокси-сервера можно настроить на внутренних клиентах автоматическое перенаправление этому серверу запросов к соответствующим службам. Для некоторых серверов требуется явно организовать соединение с прокси и только после этого инициировать соединение с использованием заданного формата.

Использование прокси-серверов может существенно повышать уровень безопасности. Можно добавить списки управления доступом для отдельных протоколов, что будет требовать от пользователей того или иного уровня представления себя (аутентификации) перед получением прав доступа. Более эффективные серверы-посредники, которые называют иногда шлюзами прикладного уровня (ALG[2]), могут быть созданы на основе понимания конкретных протоколов и будут допускать блокировку некоторых аспектов работы протокола. Например, ALG для протокола FTP может различать команды put и get, если организация решит позволить своим сотрудникам загружать файлы (get) из Internet, но при этом будет блокировать передачу своих файлов на удаленные серверы (put). Фильтрующий маршрутизатор такой фильтрации обеспечить не сможет — он будет пропускать или блокировать весь трафик протокола FTP, но не отдельные его подмножества.

Серверы-посредники можно также настроить для шифрования потоков данных в зависимости от набора параметров. Организация может использовать такую возможность для организации шифрованного канала связи между двумя точками, соединенными между собой через сеть Internet.

Межсетевые экраны обычно рассматривают как средство предотвращения в сеть внешних злоумышленников. Однако МСЭ можно применять и для организации доступа в сеть извне для легитимных пользователей. Существует множество ситуаций, когда удаленным пользователям требуется регулярный доступ в сеть организации. Доступ в Internet у находящегося в командировке сотрудника обычно имеется, но он осуществляется через сети, которые не могут

[1]Несмотря на много лет, прошедших с момента выхода этого документа, и разработку множества стандартов для межсетевых экранов, различия в терминологии сохраняются до сих пор. *Прим. перев.*
[2]Application Layer Gateway/

считаться доверенными. Корректно настроенный прокси-сервер может обеспечить доступ в сеть легитимных пользователей, предотвращая одновременно проникновение злоумышленников.

Опыт показывает, что наилучших результатов в части межсетевого экранирования можно достигнуть при использовании пары экранирующих маршрутизаторов и одного или нескольких серверов-посредников, установленных в сегменте сети между этими двумя маршрутизаторами. Такое решение позволяет на внешнем маршрутизаторе блокировать любые попытки использования уровня IP (обманные адреса IP, заданная отправителем маршрутизация, фрагменты) для преодоления защиты и предотвратить за счет прокси-сервера попытки использования потенциальных уязвимостей вышележащих уровней. Внутренний маршрутизатор будет просто блокировать весь трафик через границу сети за исключением трафика сервера-посредника. При корректной реализации такой схемы можно обеспечить высокий уровень защиты.

Многие МСЭ обеспечивают протоколирование своих действий, которое при правильной настройке может существенно упростить работу администраторов безопасности. Протоколирование может быть централизованным и систему можно настроить на передачу сигналов о возникновении аномалий. Важно регулярно просматривать и анализировать системные журналы для своевременного обнаружения попыток вторжения или иных непредусмотренных действий. Поскольку некоторые злоумышленники попытаются для сокрытия своих следов почистить журнальные файлы, желательно обеспечить для таких файлов защиту. Существует множество методов решения этой задачи, включая использование устройств WORM[1], вывод информации на бумагу, централизованное протоколирование с использованием утилиты syslog. Другим методом может служит организация подставного «последовательного принтера», вместо которого которого к порту подключен изолированный компьютер, на котором сохраняются файлы системных журналов.

МСЭ значительно отличаются по качеству и возможностям. Цены на коммерческие устройства начинаются приблизительно с $10000 и могут превышать $250000. Самодельный МСЭ может быть построен за гораздо меньшие деньги. Следует помнить, что для корректной установки и настройки МСЭ (как покупного, так и самодельного) потребуются глубокие знания протоколов стека TCP/IP. МСЭ требуют регулярного обслуживания, установки программных обновлений и постоянного мониторинга. При оценке расходов на организацию МСЭ эти вопросы не следует оставлять без внимания.

Как было отмечено, построение «самодельного» МСЭ требует глубоких знаний TCP/IP. Следует также подчеркнуть, что ложное ощущение безопасности при ненадежной защите в долгосрочной перспективе оказывается хуже, нежели просто отсутствие защиты. Как и для других защитных мер, важно идентифицировать угрозы, оценить защищаемые активы и сравнить их стоимость с расходами на защиту.

В заключение разговора о МСЭ отметим, что экраны могут существенно повысить уровень безопасности, защищая сеть от множества разных атак. Но важно понимать, что это лишь часть решения задачи и никакой МСЭ не сможет уберечь от всех типов атак.

4. Элементы и процедуры системы защиты

В этом разделе рассматривается множество вопросов, которые должны быть решены при организации защиты сайта. В каждом параграфе рассматривается сервис или свойство, которые могут потребоваться для защиты информации и систем, входящих в состав сайта. Порядок рассмотрения вопросов обеспечивает сначала знакомство читателя с концепциями.

В этом разделе значительное внимание уделяется вопросам криптографии. Детальное рассмотрение криптографической тематики выходит за рамки данного документа, но интересующиеся читатели могут сами получить нужную информацию из книг и статей, приведенных в списке литературы.

4.1 Идентификация

В течение многих лет для идентификации пользователей предписывалось применение обычных паролей многократного использования (условно постоянных). Изначально такие пароли применялись пользователями терминалов для представления себя центральному компьютеру. В те времена практически не было сетей (внутренних или внешних), поэтому риск раскрытия текстовых паролей был минимальным. Современные системы соединены между собой через локальные сети, а те, в свою очередь, подключены через распределенные (глобальные) сети к Internet. Пользователи могут входить в систему из любого места, поэтому передача паролей в открытом виде через сети создает большой риск утечки (перехвата). И действительно, координационный центр CERT и другие организации отмечают значительное число инцидентов, связанных с перехватом передаваемых в открытом виде паролей.

С появлением новых методов аутентификации типа одноразовых паролей (например, S/Key), PGP и маркеров доступа (token) началось использование подобных паролям текстовых строк в качестве секретных маркеров персональных или идентификаторов. При необдуманном выборе такого маркера или идентификатора схему аутентификации можно легко обойти.

4.1.1 Одноразовые пароли

Как было отмечено выше, в современных сетевых средах сайтам, заботящимся о безопасности и целостности своих систем и сетей, следует уходить от практики применения обычных паролей многократного использования. Известно о множестве инцидентов с использованием троянских сетевых программ (например, telnet и rlogin), а также средств перехвата пакетов в сети. Такие программы позволяют получать информацию о передаваемых в открытом виде именах хостов и пользователей, а также паролях. Эта информация может потом использоваться злоумышленниками для входа в систему с перехваченными учетными данными. Причин тут две: 1) один и тот же пароль используется много раз, 2) пароль передается через сеть в открытом виде.

Для решения указанной проблемы было разработано несколько методов аутентификации. Среди них следует упомянуть технологию challenge-response (вызов-отклик), позволяющую использовать пароль только один раз (однократный пароль). Существует множество решений, основанных на таких технологиях. Выбор конкретной продукции определяется задачами организации.

[1]Write once, read many — однократная запись, множественное считывание.

4.1.2 Kerberos

Kerberos представляет собой распределенную систему сетевой защиты, которая обеспечивает аутентификацию через незащищенные сети. При необходимости система может также обеспечивать для приложений услуги шифрования и защиты целостности. Первый вариант Kerberos был разработан в Массачусетском технологическом институте (MIT[1]) в середине 1980-х годов. Две основных версии Kerberos (4 и 5), получивших распространение, несовместимы между собой.

Система Kerberos основана на использовании базы данных о симметричных ключах с центром распространения ключей (KDC[2]), совместно называемых сервером Kerberos. Пользователям и службам (доверитель - principal) предоставляются электронные квитанции (tickets) после успешного соединения с KDC. Эти квитанции используются для взаимной аутентификации доверителей. Все квитанции включают временные метки, ограничивающие срок действия квитанции. Следовательно, для работы клиентов и сервера Kerberos требуется защищенный эталон часов, обеспечивающий достаточную точность синхронизации.

На практике Kerberos интегрируется с приложениями. Типовыми примерами могут служить FTP, telnet, POP, NFS с поддержкой функций Kerberos. Имеется множество реализаций с различными уровнями интеграции. Дополнительную информацию можно найти в документе Kerberos FAQ, доступном на сайте http://www.ov.com/misc/krb-faq.html.

4.1.3 Выбор и защита маркеров безопасности и PIN

При выборе маркеров защиты (парольных фраз) следует быть осторожным. Как при выборе паролей следует обращать внимание на устойчивость к атакам методом подбора (brute force). Т. е., в качестве маркеров не следует выбирать слова какого-либо языка, общеизвестные сокращения и т. п. Лучше выбирать длинные последовательности, нежели короткие, и включать в них строчные и прописные буквы, цифры и специальные символы.

После выбора маркера безопасности важно обеспечить его защиту. Некоторые парольные фразы служат для доступа к устройствам (типа карт доступа) и их не следует записывать или помещать в одно место с устройством, для которого они предназначены. Другие (например, PGP[3]) следует защищать от несанкционированного доступа.

В заключение темы отметим, что при использовании криптографических систем типа PGP, следует с осторожностью отнестись к выбору размера ключей и обеспечить обучение и тренировку всех пользователей. По мере совершенствования технологий размеры ключей будут увеличиваться. Для обеспечения эффективной криптографической защиты следует использовать наиболее современные технологии.

4.1.4 Надежность паролей

Хотя необходимость отказа от стандартных многоразовых паролей достаточно ясна, во многих организациях продолжают ими пользоваться. При сохранении рекомендации перехода на более эффективные технологии мы хотим помочь таким организациям в решении вопросов выбора и поддержки традиционных паролей. При этом не следует забывать, что ни одна из перечисленных здесь мер не обеспечит защиты от раскрытия паролей путем перехвата данных в сети.

(1) Надежность паролей. Во многих (если не в большинстве) случаях проникновения в системы нарушитель получал доступ через имеющуюся в системе учетную запись пользователя. Одним из распространенных вариантов такого проникновения является угадывание пароля. Зачастую для выяснения паролей используют специальные программы, которые анализируют парольные файлы с применением очень больших словарей. Единственным способом предотвращения таких нарушений является внимательный выбор пароля, который не может быть просто подобран с помощью программ (пароль, содержащий комбинацию букв, цифр и знаков препинания). Пароли должны быть достаточно длинными с учетом ограничений системы и возможности пользователей запомнить пароль.

(2) Смена установленных по умолчанию паролей. Во многих операционных системах и прикладных программах применяются принятые по умолчанию имена пользователей и пароли, которые задаются при установке. Такие пароли следует незамедлительно менять с целью предотвращения несанкционированного доступа в систему.

(3) Ограничение доступа к парольному файлу. В частности, хочется сохранить часть файла с зашифрованными паролями от общего доступа и возможности подбора паролей по хэш-значениям. Эффективным методом является использование теневого файла, когда поле пароля в обычном файле содержит пустую или ложную запись, а файл с реальными паролями хранится где-то в защищенном месте системы.

(4) Смена паролей. Вопрос сроков действия и механизмов смены паролей постоянно обсуждается в сообществе информационной безопасности. Принято считать, что неиспользуемые пароли не нуждаются в поддержке, однако не прекращаются дискуссии о целесообразности принуждения пользователей к замене используемых ими качественных паролей. Сторонники смены паролей обосновывают свою точку зрения необходимостью предотвращения продолжающегося использования «взломанных» учетных записей. Противники регулярной замены утверждают, что такая замена вынуждает пользователей записывать свои пароли (на приклеенных к монитору листочках) или выбирать простые для запоминания пароли, которые легко угадать. Они также заявляют, что нарушитель скорее будет применять перехваченные или подобранные пароли, нежели старые.

Несмотря на то, что определенного ответа на отмеченный выше вопрос не найдено, политика в отношении паролей должна в явном виде решать вопрос замены паролей и давать четкие рекомендации по частоте смены пароля пользователем. Для большинства пользователей смена пароля не вызывает затруднений и следует предусматривать такую замену. Рекомендуется менять пароли в случаях компрометации привилегированных учетных записей, смене критически важного персонала (особенно администраторов) или компрометации их учетных записей. Кроме того, в случае компрометации привилегированных учетных записей следует менять все пароли в системе.

(5) Блокировка учетных записей/паролей. Некоторые сайты считают полезной блокировку учетных записей после нескольких неудачных попыток аутентификации. При намерении реализовать такой механизм рекомендуется

[1]Massachusetts Institute of Technology.
[2]Key distribution center.
[3]Pretty Good Privacy.

сделать так, чтобы он не «анонсировал» себя. После блокировки учетной записи даже в случае ввода корректного пароля пользователю следует выдавать такое же сообщение, как при неудачной попытке входа в систему. Реализация такого механизма будет требовать от легитимных пользователей обращения к своему системному администратору в случае блокирования учетной записи.

(6) О демоне finger. По умолчанию демон finger выводит важную информацию о системе и пользователе. Например, он может показать список всех пользователей, работающих в данный момент в системе или полное содержимое пользовательского файла .plan. Такая информация может быть использована злоумышленниками для идентификации пользователей и угадывания их паролей. Рекомендуется изменить поведение демона finger с целью ограничения набора отображаемой информации.

4.2 Защита конфиденциальности

Ваш сайт наверняка захочет защитить часть своих ресурсов от раскрытия данных не имеющим полномочий лицам. Операционные системы часто имеют встроенные механизмы защиты, которые позволяют администратору управлять правами доступа (просмотра) к файлам в системе. Мощным средством защиты конфиденциальности данных является шифрование. Извлечение информации из зашифрованного файла потребует колоссальных затрат ресурсов и времени от любого лица, за исключением уполномоченных. Владелец информации и уполномоченные лица могут легко расшифровать данные с помощью соответствующего ключа. Рекомендуется применять шифрование для обеспечения конфиденциальности и защиты важной информации.

Применение шифрования в некоторых случаях регулируется государством или правилами сайта, поэтому мы рекомендуем администраторам ознакомиться с соответствующими документами до начала использования шифрования. Обсуждение алгоритмов и программ шифрования выходит за рамки данного документа, но мы хотим предостеречь от использования утилиты UNIX crypt, которая не обеспечивает надежной защиты. Рекомендуется также найти время на изучение вопросов шифрования и ознакомиться с конкретным алгоритмом или программой, которые планируется использовать для защиты. Многие популярные программы достаточно хорошо описаны в литературе, поэтому с их изучением не должно возникать сложностей.

4.3 Защита целостности

Администратору нужно обеспечить для информации (например, файлов операционной системы, корпоративных данных и т. п.) защиту от несанкционированного изменения. Это означает необходимость обеспечения гарантий целостности информации в системе. Одним из способов защиты целостности является создание контрольных сумм, хранящихся отдельно от данных, и периодическая (или по обстоятельствам) проверка совпадения текущих контрольных сумм с сохраненными значениями. Расхождения в контрольных суммах будут говорить об изменении информации.

В некоторых операционных системах имеются утилиты для подсчета контрольных сумм (например, sum в UNIX). Однако не все такие программы обеспечивают требуемый уровень защиты. Файлы можно изменить так, что программа UNIX sum не заметит этого! Следовательно, нужно использовать более сильные (криптографически) алгоритмы подсчета контрольных сумм типа MD5 [ref], позволяющие обеспечить эффективный контроль целостности.

Для некоторых приложений (например, электронной почты) требуется обеспечить контроль целостности при передаче информации. Имеются программы, способные обеспечить такой контроль. Для выбора конкретных решений нужно сначала определиться с потребностями, а потом выбрать технологии, способные реализовать требуемую защиту.

4.4 Предоставление полномочий (авторизация)

Авторизацией называют процесс предоставления полномочий (системным) процессам и, в конечном итоге, пользователям. Это отличается от идентификации (authentication) тем, что во втором случае процесс используется лишь для идентификации пользователя. После (надежной) идентификации привилегии, права, владение и набор доступных действий определяются авторизацией.

Явное перечисление всех разрешенных действий для каждого пользователя (и пользовательского процесса) не представляется возможным по отношению ко всем ресурсам (объектам) системы. В реальных условиях используются те или иные методы упрощения предоставления и проверки полномочий.

Одним из решений, продвигаемым в системах UNIX, является связывание с каждым объектом трех классов доступа — для владельца (owner), группы-владельца (group) и всех прочих пользователей (world). Владельцем объекта считается его создатель или пользователь, которому права владения предоставлены администратором (super-user). Полные права доступа (обычно, read - чтение, write - запись и execute - запуск на исполнение) принадлежать только владельцу. Группа представляет собой множество пользователей с одинаковыми правами доступа к объекту. Права группы предоставляются всем членам группы, но владелец может иметь дополнительные права. Права доступа для всех прочих (world) предоставляются любому пользователю, получившему доступ в систему. Права группы и владельца могут быть иными (расширенными).

Другим решением является связывание с объектом списка, в котором явно указываются все имеющие доступ пользователи (группы). Это называется списком управления доступом (ACL[1]). Преимуществом ACL является простота их поддержки (один список на объект) и визуальной проверки имеющих права доступа. Недостатком решения является необходимость выделения дополнительных ресурсов для хранения списков, а также огромное число таких списков в больших системах.

4.5 Доступ

4.5.1 Физический доступ

Следует ограничивать физический доступ к хостам, предоставляя его только уполномоченному персоналу. Под хостами в данном случае понимаются «доверенные» терминалы (т. е. терминалы без идентификации пользователей — системные консоли, терминалы операторов и спецтерминалы), а также отдельные микрокомпьютеры и рабочие станции (особенно, подключенные к сети). Рабочие зоны, в которых размещается такое оборудование следует

[1]Access Control List.

оснащать средствами контроля доступа, поскольку без этого контроль физического доступа к хостам просто не возможен.

Храните рабочие и резервные копии данных и программ в защищенных местах. Помимо обеспечения надежности в плане резервирования, необходимо также защищать данные и программы от краж. Важно хранить оригиналы и резервные копии в разных местах, что повышает уровень их защиты как от повреждения, так и от краж.

Переносные хосты создают особый риск. Следует обеспечить защиту от краж портативных компьютеров сотрудников организации. Подготовьте рекомендации с перечнями данных, которые допускается хранить на переносных компьютерах, а также данных, требующих защиты (например, шифрования) при их размещении на переносных компьютерах.

К зонам, требующим ограничения физического доступа, относятся также кроссовые помещения и важные элементы сети (файловые серверы, серверы DNS, маршрутизаторы.

4.5.2 Свободные сетевые порты

Свободные сетевые порты предназначены для удобства подключения переносных хостов пользователей к сети.

Рассмотрим вопрос организации таких портов с учетом того, что он позволяют пользователям подключить к сети произвольный (непроверенный) хост. Это повышает риск атак, связанных с подменой адресов IP (spoofing), перехватом пакетов и т. п. Пользователи и руководство сайта должны принимать во внимание это обстоятельство. Если вы решили организовать в своей сети свободные порты, следует внимательно отнестись к планированию размещения таких портов для предотвращения несанкционированного доступа в сеть.

Для подключаемых к таким портам хостов следует организовать проверку полномочий до предоставления им реального доступа к сетевым ресурсам. Как вариант, можно организовать контроль физического доступа. Например, если такие порты предоставляются студентам, можно установить розетки только в студенческих аудиториях.

Если свободные порты предоставляются посетителям для получения ими доступа в свои сети (например, для просмотра почты) из вашей сети, имеет смысл организовать для таких пользователей отдельную подсеть.

Обращайте внимание на такие места, которые могут обеспечить бесконтрольный доступ в сеть (например, порт уволившегося сотрудника). Зачастую разумно отключать такие порты на уровне кроссов или использовать в сети устройства, позволяющие организовать мониторинг сетевых портов в плане несанкционированных подключений.

4.5.3 Прочие сетевые технологии

Рассматриваемые здесь технологии включают X.25, ISDN, SMDS, DDS и Frame Relay. Все эти сети основаны на физических соединениях через телефонные станции, что позволяет организовать перехват данных. Взломщики, безусловно, заинтересованы в телефонных коммутаторах и сетях передачи данных!

При работе с коммутируемыми соединениями по возможности следует применять постоянные виртуальные соединения (PVC[2]) или закрытые группы пользователей (CUG[3]). Технологии, позволяющие обеспечить идентификацию и/или шифрование (такие, как IPv6) развиваются достаточно быстро. Если безопасность важна для вас, следует обратить внимание на такие технологии.

4.5.4 Модемы

4.5.4.1 Модемные линии должны быть управляемыми

Модемы обеспечивают удобный доступ к сайту для его пользователей, но они же могут служить средством обхода межсетевых экранов. По этой причине важно контролировать использование модемов.

Не следует разрешать пользователям организацию несанкционированных модемных соединений. Это относится и к временным соединениям, когда модем подключается вместо телефонного или факсимильного аппарата.

Регистрируйте все установленные в сети модемы и поддерживайте актуальность этих данных. Регулярно (в идеале, автоматически) проверяйте наличие в сети несанкционированных модемных соединений.

4.5.4.2 Пользователи модемов должны идентифицироваться

Доступ пользователей в сеть во всех случаях следует предоставлять лишь после ввода пользователем своего имени и пароля. Требования к организации парольной защиты рассмотрены в параграфе 4.1.1.

Помните, что телефонные линии могут «прослушиваться» и достаточно просто организовать перехват информации в сетях сотовой связи. Современные высокоскоростные модемы используют изощренные методы модуляции, которые усложняют перехват, но разумно предполагать, что злоумышленники умеют это делать. По этой причине следует по возможности пользоваться одноразовыми паролями.

Полезно организовать одну точку входа из телефонных сетей (например, большой модемный пул), чтобы для всех пользователей применялись общие механизмы идентификации.

Пользователи иногда забывают свои пароли. В связи с этим целесообразно задать небольшую (например, 2 секунды) задержку после первого и второго ввода неверного пароля, а после третьей ошибки разрывать соединение. Это позволит существенно замедлить и осложнить организацию атак с автоматическим подбором пароля. Не следует сообщать пользователю, где он допустил ошибку (имя, пароль или оба).

4.5.4.3 «Обратные вызовы»

Некоторые серверы доступа предлагают услуги обратного вызова (т. е., пользователь набирает номер модема и проходит процедуру идентификации, после чего сервер разрывает соединение и организует его заново, набирая известный номер пользователя). Такая функция позволяет предотвратить несанкционированное подключение к сети в случае правильного подбора имени пользователя и пароля, поскольку сервер будет набирать известный ему номер

[2]Permanent Virtual Circuit.
[3]Closed User Group.

легитимного пользователя, а не взломщика. Однако это ведет к тому, что пользователи могут подключаться к сети только при звонках с определенного номера (заданного в параметрах сервера). Кроме того, это может вызывать дополнительные расходы, связанные с организацией телефонного соединения сервером.

Использовать данную функцию следует с осторожностью, поскольку ее можно обойти достаточно простым путем. По крайней мере следует настроить сервер так, чтобы исходящее соединение с пользователем во всех случаях организовывалось не с того модема, который принял вызов пользователя. В целом функция обратных звонков повышает уровень защиты модемного доступа в сеть, но следует использовать ее в комбинации с другими методами.

4.5.4.4 Все входы в систему должны фиксироваться

Все случаи входа пользователей в систему (успешные и неудачные) должны регистрироваться в журнальном файле. Однако хранить пользовательские пароли в этом файле не следует. Достаточно просто зафиксировать факт входа в систему. Поскольку большинство случаев ввода ошибочных паролей связано с опечатками пользователей разница между правильным и ошибочным паролем может заключаться в одном-двух символах. Следовательно, если системный журнал не имеет достаточно хорошей защиты, некорректно введенные пароли также не следует сохранять.

При доступности услуг CLI[1], имеет смысл записывать номера телефонов, с которых осуществлялись попытки входа в систему. Однако в этом случае следует соблюдать требования по защите приватности. Важно также понимать, что CLI не обеспечивает полной достоверности определения номера (например, нарушители могут взломать телефонный коммутатор и пользоваться подставными номерами), поэтому номера можно использовать только для получения информации, но не для идентификации пользователей.

4.5.4.5 Выбор системного приветствия

На многих сайтах в качестве приветствия при входе в систему (opening banner) используется так называемое «сообщение дня». К сожалению в таких сообщениях зачастую содержится информация об операционной системе и оборудовании хоста. Эти данные могут оказать помощь злоумышленнику. Рекомендуется отказаться от вывода сообщения дня, создав свой вариант приветствия при входе в систему с минимальным набором информации.

Выводите короткое сообщение, а не «зазывающее» имя (например, University of XYZ, Student Records System). Просто выведите на экран краткое название сайта, предупреждение о мониторинге сеансов работы и предложение ввода имени/пароля. Представьте текст сообщения юристам для проверки во избежание возникновения правовых проблем.

Для приложений с высоким уровнем защиты следует использовать ввода пароля «вслепую» (без отображения на экране звездочек или иных символов). Это будет похоже на имитацию «умершего» модема.

4.5.4.6 Идентификация при коммутируемом доступе

Для пользователей, подключающихся к сети по коммутируемым линиям, также следует идентификацию (особенно в тех случаях, когда организация оплачивает телефонные звонки).

Никогда не позволяйте организовывать исходящие соединения по телефонным линиям для неидентифицированных входящих телефонных подключений и создайте правила для организации исходящих вызовов идентифицированных пользователей. Это позволит предотвратить использование вашего модемного пула для организации цепочки вызовов с регистрацией (login) в нескольких системах. Такие цепочки регистраций сложно обнаружить особенно в случаях использования хакерами пути через несколько хостов вашего сайта.

В любом случае не позволяйте использовать одни и те же модемы и телефонные линии для приема входящих соединений и организации исходящих. Реализовать это можно путем организации двух раздельных модемных пулов.

4.5.4.7 Максимальная защита модемов

Убедитесь, что ваши модемы не были перепрограммированы, если вы сдаете их на обслуживание. По крайней убедитесь, что команда +++ не переводит модемы на входящих линиях в командный режим!

Запрограммируйте свои модемы на сброс в стандартную конфигурацию при старте каждого нового соединения. Если это невозможно, выполняйте сброс модема по завершении каждого соединения. Такой подход обеспечит защиту от случайного перепрограммирования модемов. Сброс параметров модема в начале и по завершении каждого вызова обеспечить гарантию того, что при следующем вызове не будут наследоваться параметры предыдущей сессии.

Проверьте свои модемы на корректность завершения соединений. При отключении пользователя от сервера доступа линия должна освобождаться. Не менее важно обеспечить завершение пользовательских сеансов в случае разрыва телефонного соединения со стороны пользователя.

4.6 Аудит

В это разделе рассматриваются процедуры сбора данных о сетевой активности, которые могут быть полезны для анализа защищенности сети и расследования инцидентов.

4.6.1 Что собирать

В данные аудита следует включать любые попытки изменения уровня защиты и эскалации привилегий со стороны процессов и пользователей, а также иных элементов сети. К таким действиям относятся процедуры регистрации в системе и выхода из нее (login и logout), доступ с правами суперпользователя (root в UNIX или его эквивалент в других PC), генерация квитанций (например, для Kerberos), а также все прочие изменения прав или состояний. Особенно важно фиксировать доступ пользователей anonymous и guest к публичным службам.

Реально собираемые данные зависят от сайта и типов используемого на нем доступа. В общем случае собираемая информация должна включать: имена пользователей и хостов для процедур входа и выхода из системы, предшествующие и новые права доступа при попытках их изменения. Для всех событий следует сохранять временные метки. Естественно, в своей системе вы найдете гораздо более широкий круг информации для аудита. Но не следует забывать об объеме, который эта информация потребует для своего хранения.

[1]Calling Line Identification — идентификация вызывающей линии (АОН).

Важно предостеречь от сохранения паролей. В этом случае возникает серьезная угроза безопасности всего сайте в случае получения злоумышленником доступа к данным аудита. Не следует записывать даже некорректные пароли при неудачных попытках входа, поскольку в большинстве случаев эти пароли будут отличаться от корректных лишь одним или парой символов.

4.6.2 Процесс сбора

В процесс сбора данных следует включать хосты и ресурсы, к которым осуществляется доступ. В зависимости от важности данных и потребности в наличии локальной копии при недоступности сервиса данные можно сохранять локально на связанном с ними ресурсе до возникновения потребности в них или передавать в специальное хранилище после каждого события.

Существует три основных способа хранения записей аудита: в файле с правами чтения и записи на хосте, на устройстве с однократной записью и многократным считыванием (например, CD-R или специально настроенное устройство записи на ленту) или на устройстве, позволяющем только запись (например, вывод на печать). Каждому из методов присущи свои преимущества и недостатки.

Запись в обычный файл обеспечивает наименее ресурсоемкий и простой в настройке вариант хранения. В этом случае возможен постоянный доступ к файлу данных для анализа записей, что может быть важно при работе с данными во время атаки. Однако этот способ отличается наименьшей надежностью. Если хост, используемый для хранения будет скомпрометирован, злоумышленник получит доступ к данным аудита и сможет изменить или уничтожить их.

Хранение данных аудита на устройствах с однократной записью несколько сложнее в настройке, но обеспечивает существенные преимущества в плане безопасности за счет того, что нарушитель не может изменить или удалить записанную информацию. Недостатком этого метода является необходимость поддержки устройства со сменными носителями, а также стоимость носителей для записи данных[1]. Кроме того, не может быть обеспечено постоянного доступа к данным.

Вывод системного журнала на принтер полезен в системах, где требуется постоянный и незамедлительный доступ к данным протоколирования. Примером могут служить системы, работающие в реальном масштабе времени, где требуется точно фиксировать момент отказа или атаки. Лазерный принтер или иное устройство буферизации (например, сервер печати) могут не обеспечивать сохранность данных в критических случаях. Недостатками этого метода являются необходимость хранения больших объемов бумажных лет и невозможность автоматизированного поиска данных в журнале.

Для каждого из описанных выше методов возникает вопрос защиты пути между устройством, генерирующим данные аудита и устройством записи этих данных (файловый сервер, стример, устройство CD-R, принтер). При компрометации этого пути данные могут быть удалены или подменены. В идеале устройство хранения/вывода должно подключаться простым кабелем непосредственно к устройству сбора (генерации) данных. Однако на практике данные могут проходить через сети и маршрутизаторы. Можно предотвратить подмену данных даже при «захвате» пути их доставки путем использования контрольных сумм для данных аудита (шифровать сами данные большого смысла не имеет, поскольку они обычно не содержат критичной информации).

4.6.3 Хранение данных аудита

Для хранения данных аудита может потребоваться значительное пространство на устройствах хранения и этот вопрос следует обдумать заранее. Существует несколько способов снижения размера требуемого пространства. Данные можно сжимать, используя один из имеющихся методов компрессии, или можно сократить срок хранения собранных данных, оставляя на долгосрочное хранение лишь результаты предварительной обработки. Одним из основных недостатков второго варианта является ограничение возможностей по расследованию инцидентов. Зачастую инцидент не удается заметить сразу и к моменту начала его расследования первичные данные могут оказаться уже недоступными, а результатов предварительной обработки может оказаться не достаточно для полного расследования.

4.6.4 Обработка и хранение данных аудита

Данные аудита следует бережно сохранять на сайте и в форме резервных копий. Если нарушитель получит доступ к этим данным, возникнет риск не только для самих данных, но и для системы в целом.

Данные аудита весьма важны для расследования, задержания и судебного преследователя виновных в инциденте. По этой причине рекомендуется заранее проконсультироваться с юристами по вопросам толкования данных аудита. Это следует сделать, не дожидаясь возникновения инцидента.

Если план обработки данных не был адекватно определен до инцидента, при возникновении такового имеющихся данных может оказаться не достаточно или они не будут иметь юридической силы.

4.6.5 Правовые вопросы

В силу самой природы данных аудита с ними связано множество юридических вопрос. Если вы собираете и храните данные аудита, нужно быть готовым к последствиям, связанным как с наличием, так и с содержимым этих данных.

Один из вопросов связан с правами личности. В некоторых случаях данные аудита могут включать персональную информацию. Поиск в таких данных даже с помощью программ системной защиты может быть связан с нарушением прав личности.

Второй вопрос связан с информацией о деструктивных действиях с вашего сайта. Если организация хранит данные аудита, должна ли она отвечать за идентификацию инцидентов, которые можно обнаружить в этих данных? Если хост сайта используется для атаки на другую организацию, может эта организация воспользоваться вашими данными аудита для проведения расследования?

Приведенные примеры достаточно абстрактны, но они должны послужить стимулом для рассмотрения юридических вопросов, связанных с данными аудита.

---

[1]Стоимость носителей для однократной записи в настоящее время весьма низка, однако важно отметить, что срок хранения такой информации сравнительно невелик. *Прим. перев.*

4.7 Защита резервных копий

Процедура создания резервных копий является классической часть операционной системы компьютера. В контексте этого документа резервные копии рассматриваются как часть общего плана защиты сайта. В этом смысле важно принимать во внимание перечисленные ниже аспекты резервного копирования.

(1) Убедитесь, что на сайте создаются резервные копии.

(2) Убедитесь, что для резервных копий используются внешние хранилища. Следует выбирать место хранения резервных копий с учетом его защищенности и доступности.

(3) При хранении резервных копий за пределами сайта рассмотрите вопрос шифрования информации. Следует помнить, что при использовании шифрования потребуется хорошая схема управления ключами, чтобы вы смогли восстановить зашифрованные данные в любой момент. Следует также удостовериться в гарантированном доступе к программам, которые могут потребоваться для восстановления зашифрованных данных.

(4) Не следует предполагать, что резервные копии гарантированно будут хорошими. Возникало множество компьютерных инцидентов, которые обнаруживались далеко не сразу. В таких случаях резервные копии вовлеченных в инцидент систем уже могли быть искаженными.

(5) Периодически проверяйте корректность и полноту резервных копий.

5. Расследование инцидентов

В этой главе приводятся рекомендации по действиям до, во время и после связанных с компьютерной безопасностью инцидентов на хосте, в сети, на сайте или в среде множества сайтов. Во время связанных с нарушениями системы защиты инцидентов следует действовать по плану. Такой подход является правильным независимо от природы инцидента, будь это атака извне, неумышленное повреждение при тестировании студентом нового эксплойта для использования программной уязвимости или действия обиженного сотрудника. Для каждого из возможных типов событий (таких, как перечислены в примере) следует заранее подготовить план адекватного реагирования.

В традиционной компьютерной безопасности основное внимание уделяется общему плану защиты сайта, но вопросы отражения атак обычно рассматриваются недостаточно. Это приводит к тому, что в случае реальной атаки многие решения вынужденно принимаются в спешке и могут в процессе действий по восстановлению работоспособности и защите важных данных приводить к уничтожению или повреждению информации, нужной для отслеживания источника атаки и сбора доказательств.

Одним из наиболее важных, но часто упускаемым из виду вопросом обработки инцидентов является экономический аспект. Технические и административные меры при обработке инцидентов могут требовать значительных ресурсов. Если персонал проходит заблаговременно соответствующее обучение, при возникновении атак он будет работать быстрее и эффективней.

Распространение сети в мировом масштабе привело к тому, что большинство инцидентов не ограничивается одним сайтом. Уязвимости операционных систем применимы (в некоторых случаях) к миллионам систем, и в самих сетях также имеется множество уязвимостей. Следовательно, своевременное информирование всех вовлеченных в инцидент сторон является жизненно важным.

Другое преимущество относится к распространению информации об инцидентах. Новости об инцидентах в сфере компьютерной безопасности негативно влияют на репутацию компании среди потенциальных клиентов. Эффективная реакция на инциденты минимизирует потенциальный ущерб репутации.

Основное преимущество эффективной реакции на инциденты связано с юридическими аспектами. Не исключено, что вслед а инцидентом организация может быть привлечена к ответственности по причине того, что компоненты ее сети оказались вовлеченными в организацию сетевой атаки. Аналогично этому разработчики «заплаток» (patch) или временных решений могут быть привлечены к ответственности в случае компрометации систем или их повреждения по причине недостаточной эффективности разработанных ими мер. Информация об уязвимостях операционных систем и картин атак в комбинации с правильными мерами по снижению потенциальных угроз имеют очень важное значение в плане возможных юридических последствий инцидентов.

В последующих параграфах этого раздела описана схема и начальные этапы организации политики безопасности сайта в части реакции на инциденты:

(1) подготовка и планирование (цели и задачи при обработке инцидентов);

(2) уведомления (с кем следует контактировать при возникновении инцидента);

- местный персонал и управляющие,
- службы правопорядка и детективные агентства,
- команда по реагированию на инциденты в сфере компьютерной безопасности,
- вовлеченные в инцидент сайты и сайты, на которые инцидент может оказать воздействие,
- службы внутренних коммуникаций,
- службы по связям с общественностью;

(3) идентификация инцидентов (является ли это инцидентом и насколько он серьезен);

(4) обработка (что делать при возникновении инцидента);

- уведомления (кому следует сообщить об инциденте),
- защита улик и системных журналов (какие записи следует сохранять до, во время и после инцидента),
- сдерживание (как ограничить воздействие инцидента),

- искоренение (как устранить породившие инцидент причины),
- восстановление (как возобновить работу системы и служб),
- последствия (какие действия следует предпринять после инцидента);

(5) последствия (каковы последствия прошлых инцидентов);

(6) административная реакция на инцидент.

Далее в этом разделе подробно рассматриваются вопросы, связанные с перечисленными выше темами, и даются рекомендации по разработке политики сайта в части обработки инцидентов.

5.1 Подготовка и планирование расследований инцидентов

Частью обработки инцидента является подготовка к реагированию на него еще до первого случая возникновения инцидента. Это включает организацию соответствующего уровня защиты, как было описано выше. Такие действия должны защитить сайт от возникновения инцидентов, а также ограничить возможные негативные последствия при возникновении инцидента. Защита включает также подготовку рекомендаций по обработке инцидентов, как часть плана действий при возникновении непредвиденных ситуаций в организации или на сайте. Наличие написанного плана позволяет избавиться от значительной части неопределенностей, возникающих во время инцидента, и позволит более адекватно реагировать на инциденты. Очень важно проверить предложенный план до возникновения инцидента (в «лабораторных» условиях). Для таких тренировок можно даже привлекать специальную команду «злоумышленников», которая будет работать одновременно с командой защиты (в команду «злоумышленников» следует включать специалистов, которые будут пытаться преодолеть защиту системы).

Обучение реагированию на инциденты важно для решения целого ряда задач:

(1) защита активов, которые могут быть подвергнуты опасности;

(2) защита активов, которые могли бы использоваться более эффективно, если бы инцидент не потребовал их применения;

(3) соответствие требованиям регуляторов (государственных и иных);

(4) предотвращение использования вашей системы для атак на другие системы (может иметь юридические последствия)

(5) минимизация негативных последствий инцидента.

Как в любом наборе заранее планируемых процедур особое внимание должно быть уделено целям действий по обработке инцидента. Уровни приоритета для таких целей могут меняться от сайта к сайту. Ниже приведен конкретный набор задач, которые можно выделить при реагировании на инциденты.

(1) выяснение картины происходящего;

(2) определение путей предотвращения дальнейшего использования той же уязвимости;

(3) предотвращение эскалации инцидента и возникновения новых;

(4) определение активов, на которые оказал воздействие инцидент;

(5) восстановление после инцидента;

(6) обновление правил и процедур после инцидента;

(7) поиск участников инцидента (если это возможно).

По самой природе инцидента может возникать противоречие между обнаружением источника проблем и восстановлением работоспособности систем и служб. Более важные задачи (типа обеспечения целостности критичных систем) могут послужить причиной отказа от анализа инцидента. Естественно, что такое решение должен принимать персонал управляющих, однако все вовлеченные в инцидент стороны должны осознавать, что без анализа причин такой же инцидент может повториться.

Важно расставить приоритеты действий как во время инцидента, так и опережающих. Иногда инцидент может оказаться столь сложным, что не будет возможности применить все меры для отклика на него — в этом случае правильная расстановка приоритетов становится особенно важной. Хотя расстановка приоритетов может сильно меняться от сайта к сайту, приведенный ниже список мер может послужить отправной точкой.

(1) Приоритет 1 (высший) — защита человеческих жизней и безопасность людей; жизнь человека всегда имеет более высокий приоритет.

(2) Приоритет 2 — защита секретных и/или конфиденциальных данных. Предотвращение раскрытия секретных и/или конфиденциальных систем, сетей или сайтов. Информирование о затронутых инцидентом секретных и/или конфиденциальных системах, сетях и сайтах, на которые удалось проникнуть злоумышленникам (будьте в курсе требований своего сайта и регуляторов).

(3) Приоритет 3 — защита остальных данных, включая патентованные (proprietary), научные, данные управления, поскольку потеря данных влечет за собой реальные издержки. Предотвращение использования злоумышленниками систем, сетей и сайтов, а также информирование о системах, сетях и сайтах, на которые злоумышленники уже проникли.

(4) Приоритет 4 — предотвращение повреждения систем (например, потеря или изменение системных фалов, повреждение дисков и т. п.). Системные повреждения влекут за собой финансовые и временные издержки.

(5) Приоритет 5 — минимизация повреждений компьютерных ресурсов (включая процессы). Лучше выключить систему или отсоединить ее от сети, чем рисковать потерей данных или системы. Сайты могут оценить потери в случае выключения и сравнить их с риском утраты или повреждения. Могут существовать сервисные соглашения,

требующие сохранения работающих систем даже с риском их повреждения. Однако повреждения и сфера влияния инцидента могут оказаться столь велики, что оказание услуг придется вынужденно прервать.

После того, как приоритетные вопросы, связанные с защитой человеческих жизней и обеспечением национальной безопасности, решены, следует решать вопросы сохранения данных, что обычно более важно по сравнению с сохранностью программ и оборудования. Потери и повреждения при любом инциденте нежелательны, однако почти любую систему можно заменить. Потеря же или повреждение данных (особенно секретных или уникальных фирменных[1]) обычно неприемлемы ни при каких обстоятельствах.

Другим важным аспектом является влияние на системы и сети, не затронутые инцидентом напрямую. Затрагиваемые инцидентом стороны следует информировать как можно скорее с учетом требований регуляторов. С учетом возможных правовых последствий этот вопрос следует включить в плановые процедуры, чтобы избежать дальнейших задержек и неопределенности для администраторов.

При любом планировании действий для инцидентов следует руководствоваться местными правилами и требованиями регуляторов. Для государственных и частных сайтов, имеющих дело с конфиденциальными материалами должны выполняться специальные правила.

Правила, выбранные для вашего сайта в плане реагирования на инциденты, будут определять отклик на инцидент. Например, может не уделяться значительного внимания вопросам мониторинга и отслеживания злоумышленников, если ваша организация не планирует действий по их преследованию. У других организаций могут существовать планы, которые будут оказывать воздействие на ваши планы. Телефонные компании обычно передают сведения о трассировке звонков только в правоохранительные органы.

Отклик на инцидент может оказаться утомительным и включать множество рутинных операций, которые должны выполнять службы поддержки. Для освобождения технических специалистов может оказаться полезным заранее определить сотрудников служб поддержки для помощи (например, копировщиков, телефонных операторов и т. п.).

5.2 Уведомление об инциденте

Важно организовать контакты с персоналом до возникновения инцидента. Зачастую реальные инциденты не создают чрезвычайных ситуаций. На деле они просто могут хорошей тренировкой. Однако достаточно часто в обработку инцидента нужно включать сотрудников других подразделений. К числу таких людей относятся местные управляющие и системные администраторы, администраторы других сайтов Internet, детективные агентства. Организация контактов с такими людьми до возникновения инцидента может существенно повысить эффективность обработки инцидента.

Для каждого типа контактов следует определить «точки входа» (POC[2]). Они могут быть техническими или административными, а также могут включать следственные органы, сервис-провайдеров и производителей. При организации таких контактов важно определить объем информации, которая может быть представлена для каждого класса контактов. Особенно важно заранее определить, какая информация может быть доступна для пользователей сайта, других сайтов и какую информацию можно сделать общедоступной (СМИ).

Решение этих вопросов имеет особую важность для лиц, ответственных за обработку инцидентов, поскольку именно они отвечают за уведомление других сторон. Список контактов каждой категории обеспечит существенную экономию времени в процессе обработки инцидента. Во время инцидента поиск того или иного человека на фоне множества важных и срочных дел может вызывать сложности. Настоятельно рекомендуется включать в политику безопасности сайта все имеющие отношение к делу телефонные номера (а также адреса электронной почты и номера для факсимильной связи). Имена и контактную информацию людей, которые могут быть непосредственно вовлечены в обработку инцидента, следует размещать в начале списка контактов.

5.2.1 Местный персонал и управляющие

Во время инцидента одним из важнейших вопросов является координация действий многочисленных участников процесса. Одной из основных ошибок при этом является организация множества независимых групп без координации их действий. Обычно это дополнительно усложняет ситуацию и может существенно снижать эффективность действий.

Единой «точной контактов» (POC) может быть человек, отвечающий за обработку инцидента. Роли ответственного и контактного лиц при обработке инцидентов различаются. Отвечающий за обработку инцидента будет принимать решения в части интерпретации правил, применимых к данному событию. Человек, играющий роль POC, должен координировать работу всех участников процесса обработки инцидента.

Роль POC должен играть человек с техническим опытом, которого достаточно для координации действий системных менеджеров и пользователей, вовлеченных в мониторинг и действия по реагированию на инцидент. К выбору человека на эту роль следует подходить аккуратно. Это не обязательно должен быть человек, являющийся администратором «взломанной» системы, поскольку такие администраторы зачастую могут лишь обеспечивать повседневную работу компьютеров и не имеют требуемого технического уровня.

Другой важной функцией является поддержка взаимодействия с правоохранительными органами и другими внешними организациями для обеспечения межведомственного взаимодействия. Уровень вовлеченности внешних организаций определяется решением руководства и требованиями законодательства.

Человек, исполняющий функции POC, должен также единолично отвечать за сбор доказательств, поскольку, как правило, увеличение числа людей, имеющих отношение к возможным уликам, ведет к снижению вероятности того, что их показания будут приняты судом. Для обеспечения гарантий восприятия свидетельских показаний (улик) следует выполнять требования и процедуры, обусловленные местным законодательством и регулирующими документами.

Одной из наиболее важных задач POC является координация всех имеющих отношение к инциденту процессов. Обязанности могут быть распределены по всему сайту с подключением множества независимых подразделений и групп. Это потребует координации их усилий для достижения успеха. Ситуация усложняется при вовлечении в инцидент нескольких сайтов. В таких случаях POC одного из сайтов вряд ли сможет адекватно координировать все

[1] В оригинале - proprietary. *Прим. перев.*
[2] Point of Contact — контактная точка.

действия по обработке инцидента. Вместо этого следует подобрать и подключить к процессу команду по реагированию на инциденты.

В процесс обработки инцидентов следует включать те или иные механизмы повышения уровня. Для определения такого механизма сайтам потребуется создать для инцидентов внутреннюю схему классификации. Для каждого уровня инцидентов будут выбраны соответствующие POC и процедуры. При повышении уровня инцидента может меняться POC в соответствии со сменой уровня и внутренней классификацией. При смене POC человеку, выполнявшему функции POC до смены, следует передать новому POC всю информацию об инциденте.

Пользователи должны знать, как сообщить о произошедшем инциденте. На сайтах следует поддерживать процедуры информирования как для рабочих часов, так и для неурочного времени. Для приема такой информации обычно используются службы поддержки в часы работы и пейджеры или телефоны в остальное время.

5.2.2 Правоохранители и следователи

Если инцидент может иметь юридические последствия, важно связаться со следственными органами (например, ФБР или Secret Service в США) как можно скорее. По возможности следует также уведомить местные правоохранительные органы, службы безопасности и полицию. В этом параграфе рассматривается множество вопросов, которые могут возникнуть, но следует иметь в виду, что каждая организация будет связана местными и правительственными требованиями и законодательством, которые будут играть важную роль при взаимодействии с правоохранителями и следователями. Важно подчеркнуть необходимость работы в этом направлении для каждого сайта.

Основной причиной необходимости заблаговременного определения точки контакта при инцидентах является нехватка времени на такое определение при возникновении инцидента. Другая важная причина обусловлена необходимостью налаживания тесных контактов и эффективного взаимодействия с упомянутыми выше службами. Знание рабочих процедур и известные контакты существенно упрощают взаимодействие во время инцидентов. Например, важно собрать доказательства, которые будут приняты в последующих юридических процедурах, а для этого нужно понимать, как такие доказательства могут быть собраны. Последней причиной упреждающего налаживания контактов является то, что заранее не известно, какая конкретная организация будет отвечать за расследование конкретного инцидента. Наличие контактов и установившихся каналов взаимодействия позволят более эффективно организовать работу в случае возникновения инцидента.

Если в вашей организации или на сайте имеется юридическая служба, ее следует уведомить сразу же после появления ясности в части возникновения инцидента. Юристов следует привлечь по крайней мере к защите правовых и финансовых интересов вашего сайта или организации. Это включает множество правовых и практических вопросов, часть из них перечислена ниже:

(1) Готова ли ваша организация или сайт рисковать своей общественной репутацией, а также раскрывать информацию для взаимодействия с правоохранительными органами.

(2) Отложенная ответственность — если вы оставите поврежденную систему, как есть, ее можно будет отследить и использовать для повреждения других систем, поэтому ваш сайт или организация может понести ответственность за такие повреждения.

(3) Распространение информации — если ваш сайт или организация распространит сведения об атаке, в которую может быть вовлечен другой сайт или организация, а также сообщить об уязвимости продукции, которая может повлиять на продажу этой продукции, ваш сайт или организация могут понести ответственность за ущерб (в том числе, за ущерб репутации).

(4) Ответственность за мониторинг — ваш сайт или организация могут понести ответственность, если пользователи вашего сайта или других сайтов обнаружат, что ваш сайт занимается мониторингом операций по счетам (account activity) без информирования пользователей об этом.

К сожалению нет четких прецедентов в части обязательств или ответственности организаций, вовлеченных в инциденты безопасности, а также в части возможности привлечения к расследованию инцидентов. Следователи часто призывают организации помогать им в отслеживании и мониторинге нарушителей. На практике же большинство следователей не может организовать преследование злоумышленников без поддержки вовлеченных в инцидент организаций. Однако следователи не могут обеспечить защиту от претензий на возмещение ущерба, разбор которых может затянуться на многие месяцы и потребовать значительных усилий.

С другой стороны, юридические службы могут посоветовать из осторожности прекратить отслеживание нарушителя и тот сможет спокойно выйти из системы. Это не обеспечит защиты от ответственности и может помешать следователям в поиске нарушителя.

Сбалансировать интересы следствия и защиты от ответственности достаточно сложно. Нужно принимать во внимание рекомендации юристов и возможный ущерб от действий нарушителя, принимая решение о действиях во время конкретного инцидента.

Юридические службы следует привлекать к любым решениям относительно контактов со следствием при возникновении инцидента на вашем сайте. Решение о координации работы со следствием является разумным для вашего сайта или организации. Привлечение к этому процессу юристов будет способствовать многоуровневой координации между вашим сайтом и сотрудниками следственного органа, что обеспечить более эффективное распределение работы. Другим результатом такого вовлечения будет получение рекомендаций, которые помогут впредь избегать юридических ошибок.

И, наконец, юристам следует оценить документы, описывающие процедуры при обработке инцидентов на вашем сайте. Важно получить одобрение этих процедур от юристов до того, как процедуры начнут реально применяться.

При взаимодействии со следствием очень важно убедиться, что задающее вопросы лицо является законным представителем следственного органа. К сожалению достаточно часто возникают утечки конфиденциальной информации об инцидентах за счет того, что информация предоставляется лицам, маскирующимся под представителей государственных служб (Отметим, что это применимо не только к следователям).

Аналогичные вопросы возникают и в плане защиты коммуникаций. Поскольку многие из атакующих способны перемаршрутизировать сообщения электронной почты, следует избегать такого способа обмена информацией с

другими организациями (а также со всеми вовлеченными в работу по данному инциденту). Незащищенные телефонные линии (те, что используются для обычных целей) тоже часто становятся средством перехвата информации, поэтому будьте осторожны!

Не существует единого набора правил реагирования на инцидент при вовлечении местных государственных органов. Обычно (в США) никому не разрешается без ордера осуществлять операции по мониторингу, отключение от сети, воспрепятствование телефонным контактам с предполагаемыми атакующими и т. п. Для каждой организации имеется свой набор местных и государственных законов и требований, которые должны соблюдаться при обработке инцидента. Рекомендуется знать эти законы и требования, а также заранее найти и получить контактную информацию органов, в чьи функции входит расследование инцидентов.

5.2.3 Команды по реагированию на компьютерные инциденты

Существует множество групп реагирования на инциденты (CSIRT[1]) типа координационного центра CERT, немецкой DFN-CERT и других в разных странах. Подобные группы имеются во многих государственных организациях и крупных корпорациях. При доступности подобной группы уведомление ее о произошедшем на начальной стадии инцидента является первоочередной задачей. Такие группы отвечают за координацию действий во время инцидентов со множеством сайтов и более крупных объектов. Даже для инцидентов, ограничивающихся одним сайтом, доступная таким группам информация может помочь в преодолении инцидента.

Если известно, что инцидент связан с аппаратными или программными ошибками в системе, следует как можно скорее уведомить об этом производителя (или поставщика) и команду по обработке компьютерных инцидентов (Computer Security Incident Handling team). Это важно по той причине, что другие похожие системы остаются уязвимыми и производители вместе с группами реагирования на инциденты могут своевременно оказать им помощь.

При разработке политики обработки инцидентов желательно организовать группу, похожую на упомянутые выше, которая будет отвечать за обработку компьютерных инцидентов на сайте (в организации). Если такая команда была создана, важно поддерживать ее связь с другими группами реагирования. При возникновении инцидента заниматься налаживанием контактов с другими группами будет существенно сложнее, если не сделать этого заранее.

5.2.4 Вовлеченные и пострадавшие сайты

Если инцидент затрагивает другие сайты, хорошим тоном будет проинформировать их. Понимание того, что инцидент не ограничивается вашим сайтом может прийти сразу или возникнуть в процессе анализа ситуации.

Каждый сайт может сам принять решение о прямом контакте с другими сайтами или передаче информации в подходящую группу реагирования на инциденты. Зачастую поиск POC для ответственных лиц удаленного сайта связан с трудностями, а группа по реагированию на инциденты может связаться с ними, имея установленные ранее контакты.

Вопросы ответственности, включая юридическую, при инцидентах будет отличаться для разных сайтов. Важно определить правила для обмена и регистрации информации о других сайтах до инцидента.

Информация о конкретных людях является конфиденциальной и может охраняться законом. Для предотвращения связанных с этим проблем следует удалить не имеющую отношения к делу информацию, а для оставшихся сведений указать правила обращения с ними. Важно четко указать, как может быть использована эта информация. Никто из информаторов (об инциденте) не захочет видеть упоминание о себе в публичной печати. При работе с группами по реагированию на инциденты переданная ответственным POC информация остается защищенной в части анонимности. Однако следует понимать, что анализ системных журналов и информации других сайтов во многих случаях будет раскрывать ваш сайт.

Ни одна из отмеченных выше проблем не должна служить препятствием для привлечения других сайтов. Опыт групп по реагированию на инциденты показывает, что многие сайты, которым сообщали об их вовлеченности в инцидент, даже не подозревали об этом. Без своевременного уведомления другие сайты зачастую просто не смогут предпринять каких-либо действий против нарушителей.

5.2.5 Внутренние коммуникации

Во время серьезных инцидентов очень важно сообщать о принимаемых мерах и давать рекомендации по поведению пользователей (подразделений). В частности, следует четко объяснить пользователям, что им (не) разрешено сообщать во «внешний мир» (включая другие подразделения организации). Например, организации может быть нанесен ущерб, если пользователи станут отвечать заказчикам что-либо типа: «Я извиняюсь, но наша система не работает в результате вторжения и мы пытаемся решить проблему». Значительно лучше будет заранее подготовленную фразу: «Я извиняюсь, наша система недоступна по причине ее обслуживания с целью повышения качества сервиса».

Общение с заказчиками и контрагентами во время инцидентов следует вести разумно и аккуратно. Можно заранее подготовить «шпаргалки» по основным вопросам. При возникновении инцидента эти заготовки можно будет использовать вместе с парой фраз о специфических обстоятельствах в связи с инцидентом.

Во время инцидентов подразделения для внешних связей могут оказаться весьма полезны. Их следует привлекать к планированию действий и при необходимости использовать для внешних контактов во время инцидента.

5.2.6 Связи с общественностью

Было множество публикаций в различных СМИ информации об инцидентах в сфере компьютерной безопасности в США. Эта информация попадала и в другие страны благодаря тому, что сеть Internet продолжает расти и расширяться по всему миру. Читатели из тех стран, где подобная информация еще не публиковалась в СМИ могут обратиться к опыту США и воспользоваться им, повышая свой уровень готовности к инцидентам.

Одним из важнейших вопросов в связи с инцидентами является дозирование и контроль информации, публикуемой в общедоступных СМИ, Для принятия решения по этому вопросу требуется учесть множество аспектов. Первый и наиболее важный заключается в том, что при наличии на сайте службы по связям с общественностью важно

[1]Computer Security Incident Response Team.

использовать ее в качестве связующего звена при контактах со СМИ. Сотрудников службы следует обучать и тренировать в части дозирования и формы предоставления информации об инцидентах — это позволит защитить престиж сайта во время инцидента и после него (если это возможно). Отдел по связям с общественностью обеспечивает некие преимущества — вы можете быть откровенны с ними, а они обеспечат буфер между представителями СМИ и РОС во время инцидента.

При недоступности службы по связям с общественностью предоставлять информация представителям СМИ следует очень осторожно. Если информация конфиденциальна или может затрагивать чьи-либо интересы, может оказаться разумным предоставление прессе минимальной обзорной информации. Существует возможность того, что переданная прессе информация станет доступна организаторам инцидента (злоумышленникам). Следует также отметить, что передача в СМИ искаженной информации зачастую может нанести больше вреда, нежели утечка конфиденциальных сведений.

Заранее сложно определить круг предоставляемой прессе информации, однако некоторые советы могут быть полезны:

(1) Не сообщайте излишних технических деталей. Подробные сведения об инциденте могут попасть к его организаторам или использованы для атак на другие сайты, а также способны воспрепятствовать привлечению виновных к ответственности.

(2) Не выдавайте гипотез представителям СМИ. Гипотезы об причинах инцидента или его мотивах часто являются ошибочными и могут привести к искаженному представлению об инциденте.

(3) Работайте с правоохранителями для обеспечения защиты улик (доказательств). Не сообщайте представителям СМИ о собранных уликах.

(4) Попытайтесь не форсировать интервью с представителями СМИ, если вы к нему не готовы. Популярные издания хотят получить интервью как можно раньше, надеясь первыми опубликовать информацию.

(5) Не позволяйте представителям СМИ отвлекать внимание от обработки инцидента. Всегда помните, что ликвидация (завершение) инцидента является первоочередной задачей.

5.3 Идентификация инцидента

5.3.1 Это реально?

На этом этапе определяется реальное наличие проблемы. Естественно, многие (если не большинство) признаков, часто связываемых с вирусами, проникновением в систему, злоумышленными пользователями и т. п., в реальности обусловлены обычными неполадками (например, неисправность оборудования) или некорректными действиями пользователей. Для проверки реальности инцидента обычно полезны программы детектирования, которые могут быть доступны. Данные аудита также весьма полезны, особенно для обнаружения сетевых атак. При возникновении первых подозрений очень полезно незамедлительно сделать «снимок» системы (snapshot). Со многими инцидентами связаны динамические цепочки событий и исходный «снимок» системы может принести существенную пользу при обнаружении проблемы и источника атаки. Запись системных событий, телефонных разговоров, временных меток и т. п. также могут способствовать обнаружению проблем и будут полезны на дальнейших этапах обработки инцидента.

Ниже перечислены некоторые индикаторы или «симптомы» инцидентов, на которые следует обратить внимание[1]:

(1) Системные отказы («падение», зависание);

(2) учетные записи новых пользователей (например, неожиданно возникший пользователь RUMPLESTILTSKIN) или непонятный рост активности имеющихся пользователей;

(3) новые файлы (обычно со странными именами типа data.xx, k или .xx);

(4) странности в системах учета (например, уменьшение размера файла /usr/admin/lastlog в UNIX-систем может служить серьезным сигналом);

(5) изменение размеров и дат файлов (пользователям MS DOS следует насторожиться, если файлы .EXE неожиданно увеличились более, чем на 1800 байтов);

(6) попытки записи в системные файлы (например, администратор заметил попытку привилегированного пользователя VMS по изменению файла RIGHTSLIST.DAT);

(7) изменение или удаление дат (файлы начинают исчезать);

(8) отказы в обслуживании (например, администратор и обычные пользователи блокируются в UNIX-системе, которая перешла в однопользовательский режим);

(9) необъяснимое снижение производительности;

(10)аномалии (например, текст GOTCHA на терминале или частые и непонятные системные гудки — beeps);

(11)подозрительные события (например, множество попыток входа в систему с другого узла);

(12)подозрительные операции (например, кто-то становится пользователем root в UNIX-системе или просматривает файл за файлом от разных пользователей);

(13)невозможность входа пользователя в систему в результате изменения его учетной записи.

Приведенный список не может претендовать на полноту, в нем лишь перечислены некоторые из часто встречающихся признаков. Для принятия решения о возникновении или отсутствии инцидента в текущих обстоятельствах лучше всего обратиться к специалистам.

[1]Многие из перечисленных признаков существенно утратили актуальность или стали трудно применимыми. *Прим. перев.*

5.3.2 Типы и область распространения инцидентов

Помимо обнаружения самого инцидента нужно оценить область его воздействия и степень влияния. Важно корректно идентифицировать границы инцидента для его эффективной обработки и распределения усилий.

Для определения области воздействия и степени влияния инцидента следует определить набор критериев в соответствии с типом сайта и доступных соединений. Некоторые из вопросов представлены ниже.

(1) Инцидент затрагивает более одного сайта?

(2) На сайте затронуто инцидентом много компьютеров?

(3) Инцидент затрагивает конфиденциальную информацию?

(4) Что послужило точкой входа для инцидента (сеть, телефонная линия, локальный терминал и пр.)?

(5) СМИ вовлечены?

(6) Что может быть повреждено в результате инцидента?

(7) Оценка времени на «закрытие» инцидента?

(8) Какие ресурсы нужны для обработки инцидента?

(9) Привлечены ли правоохранительные органы?

5.3.3 Оценка ущерба и масштаба

Для анализа ущерба и оценки масштаба инцидента может потребоваться значительное время, но такой анализ нужен для понимания природы инцидента, расследования и поиска виновных. Сразу же после детектирования вторжения систему в целом и все ее компоненты следует считать подозрительными. Наиболее вероятной целью являются системные программы. Нужно быть готовыми к поиску изменений в системе, которая могла быть повреждена. В этом могут помочь полученные от производителя контрольные суммы, использующие стойкие алгоритмы (см. параграф 4.3).

При наличии исходных носителей программ (дистрибутив от производителя) следует провести анализ всех системных файлов с фиксацией любых отклонений и уведомить о результатах анализа все вовлеченные в инцидент стороны. В некоторых случаях бывает весьма затруднительно определить, какая из резервных копий соответствует корректному состоянию системы. Предположим, например, что инцидент длился месяцы или годы до его обнаружения, а его виновником мог быть сотрудник сайта или иной человек, владеющий информацией о системе и имеющей доступ к ней. В любом случае готовность к инциденту будет определять возможность восстановления после него.

Если в системе централизована запись журнальных файлов (зачастую это так), просмотрите эти файлы на предмет выявления аномалий. Если включен учет процессов и времени подключения, просмотрите профили использования системы. Дополнительный свет на природу инцидента может пролить просмотр использования дискового пространства. Ваши возможности решения всех связанных с инцидентом проблем будут существенно зависеть от результатов проведенного анализа.

5.4 Обработка инцидента

При обработке инцидента требуется выполнить ряд действий. Во всех действиях, связанных с безопасностью, наиболее важным аспектом является наличие и реализация политики безопасности на всех узлах. Без четко определенных правил и задач предпринимаемые действия будут лишены координации. Задачи следует определить заранее с привлечением руководства и юристов.

Одной из важнейших задач является восстановление контроля над затронутыми инцидентом системами и снижение уровня ущерба. В самых сложных ситуациях можно выключить систему или отключить ее от сети (это может оказаться единственным приемлемым решением).

Поскольку операции при обработке инцидента достаточно сложны, следует привлечь свю возможную помощь. При попытке решить проблему своими силами уровень реального ущерба может возрасти за счет задержек или потери информации. Многие администраторы воспринимают поиск злоумышленника, как личный вызов. Следуя таким путем , можно упустить из внимания некоторые задачи, указанные в политике безопасности. Попытки поймать злоумышленника могут иметь значительно более низкий приоритет, нежели сохранение целостности системы (например). Отслеживание деятельности хакеров полезно, но может оказаться несовместимым с риском от продолжения действий злоумышленника в системе.

5.4.1 Типы уведомлений и обмен информацией

Убедившись в наличии инцидента, необходимо уведомить соответствующий персонал. Способ такого уведомления играет важную роль в сохранении контроля за событиями в техническом и эмоциональном плане. Уведомление должно включать подробное изложение обстоятельств, которое позволило бы сразу понять ситуацию. Важно определить круг людей, которым сообщается подробная техническая информация. Например, такие сведения полезно передать команде по обработке инцидентов, поскольку они могут дать полезные советы по устранению уязвимостей, с которыми связан инцидент. С другой стороны, размещение подробной технической информации в общедоступном месте (например, через рассылку USENET или иную почтовую конференцию) может создать риск для проникновения во множество других систем. Ошибочно считать, что все администраторы, читающие списки рассылок, имеют доступ к исходным кодам операционных систем или хотя бы просто имеют уровень понимания, достаточный для выполнения адекватных действий.

Прежде всего, любое оповещение локального или внешнего персонала должно быть явным. Это требует от любого оповещения (электронная почта, телефонный звонок, факсимильное сообщение, звуковой или световой сигнал) ясного, четкого и полного предоставления информации об инциденте. Создание «дымовой завесы» при уведомлении об инциденте потенциальных помощников будет лишь создавать помехи и вносить путаницу. Если предполагается распределение работы, целесообразно каждому участнику предоставить информацию действиях других. Это не только предотвратит «двойную работу», но и предоставит участникам процесса сведения о том, к кому можно обратиться за помощью или информацией по смежным направлениям работ.

Другим важным аспектом информирования об инцидентах является точность изложения фактов. Сокрытие или искажение фактов при уведомлении может не только воспрепятствовать обработке инцидента, но и существенно усугубить ситуацию.

Выбор языка и стиля уведомления об инциденте может играть важную роль в восприятии этой информации. Нагнетание эмоций в уведомлении может увеличить возможный ущерб и породить другие негативные последствия. Важно сохранять спокойный тон в устных и письменных уведомлениях.

Важно понимать, что не все люди говорят на одном языке. Это может служить причиной недоразумений и задержек, особенно при инцидентах, затрагивающих многоязычные области. Другим важным аспектом при инцидентах международного уровня являются различия в законодательстве и культуре разных стран по отношению к инцидентам в сфере безопасности. Следует понимать, что культурные различия могут существовать не только между разными странами. Они имеются и внутри одной страны между разными социальными или национальными группами. Например, администратор университетской системы может спокойно относиться к попыткам подключения по протоколу telnet, а администратор военной системы сочтет такие действия возможной атакой.

Еще один вопрос связан с выбором языка и стиля для уведомления нетехнического и внешнего персонала. Важно точно описать инцидент без неуместного ажиотажа и путаницы. Для далеких от техники людей подготовить описание инцидента сложнее, но зачастую это очень важно. Описание без технических деталей может потребоваться для высшего руководства, прессы или правоохранительных органов. Важность таких коммуникаций не следует недооценивать, поскольку недооценка может привести к эскалации инцидента вместо его преодоления.

При вовлечении групп реагирования на инциденты может потребоваться заполнение формы для обмена информацией. Это может показаться излишним действием, вызывающим дополнительную задержку. Однако информация из таких форм зачастую помогает группе реагирования получить первичные сведения об инциденте. Такая группа поможет справиться с проблемами, которые оказались не по силам местному администратору. При выдаче технической информации таким группам следует указать по крайней мере:

(1) формат времени в системных журналах (местное время или GMT);

(2) сведения об удаленной системе, включая имена хостов, адреса IP и (возможно) идентификаторы пользователей;

(3) все записи журнальных файлов для удаленного сайта;

(4) тип инцидента (что произошло, что насторожило)

Если в журнальных файлах имеется локальная информация (например, идентификаторы пользователей), может потребоваться некоторая «очистка» журналов для сохранения приватности. В общем случае следует предоставлять всю информацию, которая может помочь в обработке инцидента, если локальная политика не запрещает этого.

5.4.2 Защита улик и системных журналов

При обработке инцидентов следует документировать все связанные с этим действия. Это обеспечит важную для вас и других информацию, которая поможет восстановить ход событий. Подробное документирование сбережет ваше время. Если не документировать, например, все телефонные звонки, вы можете забыть важную информацию, которую уже получили и придется звонить заново. Кроме того, документирование обеспечит доказательства для судебных разбирательств. Документирование также будет способствовать окончательной оценке ущерба (ваше руководство и следователи запросят такую оценку) и будет служить основой для последующих этапов обработки инцидента — преодоления последствий, восстановления и извлечения уроков.

На начальных этапах зачастую сложно оценить возможность преследования виновных, поэтому следует документировать все, как при сборе улик для суда. Следует записывать по крайней мере:

(1) все системные события (записи аудита);

(2) все предпринятые действия (с временными метками);

(3) все внешние контакты (включая фамилии и имена людей, дату и время, а также содержание разговора).

Наиболее прямым вариантом документирования являются журнальные записи в хронологическом порядке. Это позволит получить единый источник хронологически упорядоченной информации и избавит от необходимости собирать и упорядочивать сведения из разрозненных страниц. Значительная часть такой информации может послужить доказательством в суде. По этой причине (если предполагается судебная процедура) следует придерживаться определенных правил документирования во избежание некорректной работы с доказательствами. По возможности следует выполнить перечисленные ниже действия.

(1) Регулярно (например, каждый день) делать копии журнала, подписывая их (а также подписывать копии носителей, используемых для записи системных событий), передавая их хранителю.

(2) Хранитель должен обеспечить размещение полученных копий в безопасном месте (например, в сейфе).

(3) Передачу копий в хранилище также следует документировать, отмечая дату и время передачи, и получать от хранителя подписанное подтверждение передачи.

Отказ от соблюдения этих процедур может привести к признанию в суде собранных вами доказательств недействительными.

5.4.3 Сдерживание

Целью сдерживания является ограничение области распространения инцидента. Важной частью процесса сдерживания является принятие решения (например, об отключении системы, отключении от сети, мониторинге сети или системы, установке «ловушек», запрете некоторых функций и т. п.).

Иногда решение очевидно — отключить систему, содержащую конфиденциальную информацию. Следует помнить, что утрата доступа к системе во время инцидента обычно служит для пользователей (включая связанных с проблемой) индикатором того, что администраторы обнаружили проблему — это может оказать негативное воздействие на процесс расследования. В некоторых случаях разумно будет максимально быстро отключить всякий доступ и

функциональность, а затем поэтапно восстанавливать нормальную работу в ограниченных пределах. В других случаях может быть оправдан некоторый риск повреждения системы, если сохранение доступа к ней может помочь в поиске злоумышленника.

Этот этап должен включать выполнение определенных заранее процедур. Вашей организации или сайту следует, например, определить приемлемые во время инцидента риски и описать стратегию и конкретные действия. Это особенно важно для случаев, когда требуется быстро принять решение и нет возможности обсудить ситуацию со всеми вовлеченными сторонами. При отсутствии определенной заранее процедуры человек, отвечающий за обработку инцидента, не всегда имеет полномочия для принятия сложного управленческого решения (например, в связи с потерей данных важного эксперимента в результате отключения системы). Данный этап обработки инцидента следует завершать уведомлением об инциденте соответствующих органов.

5.4.4 Искоренение причин

После завершения инцидента настает время искоренить породившие его возможность причины. Однако до выполнения каких-либо действий на этом этапе следует обратить пристальное внимание на сбор всей необходимой информации о подвергавшейся опасности системе и причинах инцидента, поскольку очистка системы наверняка приведет к потере такой информации.

В процессе искоренения причин могут помочь программы (например, анти-вирусы). Если в системе обнаружены какие-то «поддельные» файлы, перед удалением их следует поместить в специальный архив. В случае вирусной инфекции важно очистить и заново отформатировать все носители, на которых были обнаружены зараженные файлы. Кроме того, следует проверить чистоту резервных копий. Многие случаи заражения сопровождались повторным инфицированием просто за счет того, что зараженные файлы попадали в резервные копии и потом возвращались в систему. После искоренения причин следует сделать новые резервные копии.

Устранение всех уязвимостей, с которыми мог быть связан инцидент является сложной задачей. Ключом к устранению уязвимостей является знание и понимание их природы.

Может потребоваться переустановка системы из исходных дистрибутивов и последующеая настройка конфигурации. Для таких ситуаций следует фиксировать и сохранять параметры настройки вашей систем. В случаях сетевых атак важно установить исправления (patch) для всех операционных систем, чьи уязвимости были использованы в инциденте.

Как было отмечено в параграфе 5.4.2, журналы безопасности (security log) могут сыграть очень важную роль на этом этапе устранения уязвимостей. Журнальные файлы, показывающие обнаружение инцидента и его ход могут в дальнейшем послужить для определения области ущерба при данном инциденте. В идеале следует автоматизировать и регулярно применять тест, который позволил обнаружить инцидент.

Если какая-то уязвимость идентифицирована, как использованная при инциденте, следующим шагом будет поиск механизма защиты системы. Почтовые конференции и бюллетени по безопасности являются хорошим источником информации по этому вопросу, следует также проконсультироваться с группами реагирования на инциденты.

5.4.5 Восстановление

После искоренения причин возникновения инцидента следует организовать восстановление. Целью восстановления является возврат систем в нормальный режим функционирования. В общем случае оптимальной стратегией будет восстановление системных служб по запросам пользователей — это позволит минимизировать доставленные им неудобства. Следует понимать высокую важность процедур восстановления и наличие у каждого сайта специфики при восстановлении.

5.4.6 Последствия

В тот момент, когда вы решите, что «безопасное» состояние системы восстановлено, в ней еще могут сохраняться «дыры» и даже ловушки. Одним из важнейших, но достаточно часто опускаемым этапом обработки инцидентов является «доводка» с учетом инцидента (follow-up). На этом этапе в системе следует организовать мониторинг и поиск элементов, которые могли быть опущены на этапе очистки. В качестве начального шага на этом этапе разумно будет воспользоваться средствами, упомянутыми в разделе 7. Не забывайте, что эти средства не могут заменить собой инструменты регулярного мониторинга и опыт администраторов.

Важнейшим элементом этапа доводки является анализ последствий инцидента. Нужно точно разобраться с тем, что произошло и когда, оценить эффективность действий вовлеченного в обработку инцидента персонала. Кроме того, следует оценить, какая информация была нужна персоналу в первую очередь и как можно ускорить ее получения. Следует также зафиксировать допущенные ошибки, чтобы не повторить при возможных следующих инцидентах.

После инцидента разумно будет подготовить отчет, описывающий всю последовательность действий при обработке — способ обнаружения инцидента, процедуры корректировки и мониторинга, а также обзор обретенного опыта. Это поможет более четкому осознанию проблемы. Восстановление формальной хронологии событий (с временными метками) будет важно для юридических целей.

Отчет о доводке важен по ряду причин. Он может помочь при возникновении других инцидентов. Важно также как можно скорее провести денежную оценку вызванного инцидентом ущерба. В эту оценку следует включать расходы, связанные с потерей программ и файлов (в частности, оценить ущерб в результате утечки «фирменных» (proprietary) данных), повреждением оборудования, и трудозатрат на восстановление файлов, настройку поврежденных систем и т. п. Эта оценка может стать основой для преследования виновных. Отчет также поможет руководству организации оценить состояние безопасности и принять соответствующие меры.

5.5 Последствия инцидента

В связи с инцидентом следует предпринять ряд действий, перечисленных ниже:

(1) Инвентаризация системных активов (с тщательным определением пострадавших от инцидента).

(2) Корректировка мер защиты с учетом обретенного опыта для предотвращения новых инцидентов.

(3) Новый анализ рисков с учетом произошедшего инцидента.

(4) Расследование и привлечение к ответственности лиц, виновных в инциденте (если это нужно).

Если инцидент произошел в результате неадекватной политики безопасности и политика не была изменена, нет оснований сомневаться в повторении инцидента. Сразу же после восстановления сайта политику и процедуры обеспечения безопасности следует пересмотреть с внесением изменений, препятствующих повторению подобных инцидентов. Политику и процедуры обеспечения безопасности разумно пересматривать регулярно даже при отсутствии инцидентов. Современные компьютерные среды быстро меняются и это делает пересмотр политики безопасности обязательным.

Целью данного этапа является развитие мер безопасности для обеспечения защиты сайта от будущих атак. В результате инцидента сайт и организация должны извлечь урок и получить практический опыт преодоления инцидентов. Другим важным следствием инцидента является применение обретенного опыта при обучении пользователей и администраторов с целью предотвращения новых инцидентов.

5.6 Ответственность

5.6.1 Не переступайте черту

Одно дело — защищать свою сеть и совершенно иное — полагать, что нужно нужно защищать другие сети. При обработке инцидента становятся очевидными некоторые уязвимости вашей системы, а также других систем. При этом может возникнуть соблазн попытаться отследить злоумышленника. При таких попытках не следует забывать о возможности «перешагнуть черту», за которой ваши действия по отслеживанию злоумышленника даже с самыми лучшими намерениями станут для кого-либо не лучше действий отслеживаемого.

Для таких случаев пожалуй лучшим правилом будет отказ от использования каких-либо возможностей удаленного сайта, к которым не открыт публичный доступ. Это явно исключает любой вход в систему (удаленный доступ), если такой доступ явно и публично не разрешен. Может возникнуть соблазн вслед за злоумышленником проникнуть на удаленный сайт и посмотреть нанесенные тому повреждения. Не делайте этого! Вместо этого постарайтесь связаться с данным сайтом и проинформировать о проникновении к ним злоумышленника.

5.6.2 Уважайте других

Во время инцидента возможны два варианта поведения — заняться слежкой за злоумышленником в надежде «поймать» его или заняться приведением в порядок системы, предварительно «вышвырнув» из нее нарушителя. Выбор одного из этих вариантов должен быть обдуманным, поскольку оставив систему открытой для отслеживания действий злоумышленника, вы можете сделать свою систему «стартовой площадкой» для проникновения на другой сайт. А это может повлечь за собой юридические последствия. Уважение к другим пользователям Internet требует проинформировать другие сайты о возможном воздействии злоумышленника на них. Обнаружить такие сайты обычно достаточно просто путем беглого анализа журнальных файлов вашей системы.

5.6.3 Административная реакция на инцидент

В политике безопасности сайта следует указывать меры воздействия на пользователей сайта, вовлеченных в инцидент. К пользовательским нарушениям следует относиться серьезно, но важнее понять роль вовлеченного в инцидент пользователя. Послужило ли это результатом его наивности? Не была ли системная брешь воспринята, как воздействие пользователя? Применение административных мер в предположении умышленных действий пользователя в случае обычной пользовательской ошибки или неосторожности не может быть оправданным. Разумней будет в таком случае воспользоваться более подходящими мерами (например, дополнительное обучение) по отношению к допустившему ошибку, оставив суровые меры воздействия реальным злоумышленникам и осознающим свои действия нарушителям правил пользования системой.

6. Текущие действия

Надо полагать, что на вашем сайте имеется продуманная политика безопасности и разработаны процедуры, способствующие поддержке этой политики. Было бы просто здорово, если с этого момента можно было просто расслабиться и ничего не делать! К сожалению, в жизни такое не реально. Ваши системы и сети не являются статическими объектами и требуется регулярно пересматривать политику и процедуры. Существует множество шагов, которые нужно выполнить для поддержания актуальности политики безопасности вашего сайта. Ниже приведен краткий список действий, который может послужить отправной точкой для разработки аналогичного списка с учетом специфики вашего сайта.

(1) Подпишитесь на рассылки групп по реагированию на инциденты (типа координационного центра CERT) и обновляйте свою систему при получении информации об имеющихся в ней недостатках.

(2) Отслеживайте связанные с безопасностью изменения, подготавливаемые производителем используемых вами программ для своевременного получения и установки обновлений.

(3) Следите за конфигурацией своей системы, фиксируйте все возникающие в ней изменения и разбирайтесь в причинах всех аномалий.

(4) Пересматривайте политику и процедуры обеспечения безопасности не реже 1 раза в год.

(5) Читайте соответствующие конференции USENET для получения свежей информации по вопросам администрирования.

(6) Регулярно проверяйте соответствие системы заданной политике и процедурам. Для выполнения такой проверки следует привлекать людей, не связанных с разработкой и реализацией этой политики и процедур.

7. Инструментальные средства

В этом разделе приведен краткий список доступных в сети Internet средств и инструментов защиты. Следует принимать во внимание, что часть перечисленных средств могла стать недоступной с течением времени.

Некоторые из перечисленных ниже инструментов являются обычными пользовательскими программами (клиентами), а другие относятся к системной инфраструктуре (серверы). Некоторые инструменты пользователь никогда не видит, но они используются приложениями или администраторами для поиска неполадок или защиты от вторжений.

Печальный факт заключается в том, что существует достаточно мало доступных приложений в сфере защиты (безопасности). Связано это, в первую очередь с тем, что для безопасной работы многих приложений требуется наличие защитной инфраструктуры. В настоящее время созданию такой инфраструктуры уделяется значительное внимание.

Большинство упомянутых ниже программ и инструментов можно найти на одном из перечисленных сайтов:

(1) CERT Coordination Center

info.cert.org:/pub/tools[1]

(2) DFN-CERT

ftp.cert.dfn.de/pub/tools/

(3) COAST[2]

coast.cs.purdue.edu:/pub/tools

Важно подчеркнуть, что для многих сайтов, включая CERT и COAST, в Internet имеются «зеркала». Старайтесь пользоваться известными зеркалами и не пренебрегайте средствами верификации (контрольные суммы md5 и т. п.) для проверки корректности загруженных программ. Известны случаи распространения вредоносного кода под видом средств защиты.

Инструменты[3]

COPS
DES
Drawbridge
identd (реально не является инструментом защиты)
ISS
Kerberos
logdaemon
lsof
MD5
PEM
PGP
rpcbind/замена portmapper
SATAN
sfingerd
S/KEY
smrsh
ssh
swatch
TCP-Wrapper
tiger
Tripwire[4]
TROJAN.PL

8. Списки рассылок и другие ресурсы

Невозможно перечислить все списки рассылок и иные ресурсы, связанные с безопасностью. Однако ниже приведены некоторые ссылки, способные послужить отправными точками. Все упомянутые ресурсы относятся к сети Internet. Пользуясь приведенными здесь ссылками, можно найти множество более специализированных ресурсов, связанных с безопасностью.

Списки рассылок

(1) CERT(TM) Advisory[5]

Отправьте сообщение по адресу: cert-advisory-request@cert.org

Текст сообщения: subscribe cert <FIRST NAME> <LAST NAME>

CERT Advisory предоставляет информацию о получении программных исправлений (patch) или деталях решения известных проблем компьютерной безопасности. Координационный центр CERT взаимодействует с разработчиками при внесении изменений в программы, не публикуя сведений об уязвимостях до завершения работы над «заплатками». CERT Advisory может также служить источником информации о распространенных атаках (например, "CA-91:18.Active.Internet.tftp.Attacks").

Консультации CERT регулярно публикуются в почтовой конференции USENET comp.security.announce[6].

Архивы CERT доступны по протоколу FTP с анонимным доступом на сайте info.cert.org[7] в каталоге /pub/cert_advisories.

[1]Данный ресурс больше не поддерживается. *Прим. перев.*
[2]Computer Operations, Audit, and Security Tools — инструменты для аудита, защиты и поддержки работы компьютеров.
[3]Часть приведенных в списке инструментов устарела, появилось также много новых. *Прим. перев.*
[4]CERT и Tripwire — зарегистрированные в U.S. Patent and Trademark Office торговые марки.
[5]Список рассылки в настоящее время не поддерживается. *Прим. перев.*
[6]Не поддерживается с 2009 года. Заменой может служить группа одноименная группа Google. *Прим. перев.*
[7]Сервер в настоящее время не поддерживается. *Прим. перев.*

(2) Список VIRUS-L[1]

Отправьте сообщение по адресу: listserv%lehiibm1.bitnet@mitvma.mit.edu

Текст сообщения: subscribe virus-L FIRSTNAME LASTNAME

VIRUS-L представляет собой модерируемую почтовую рассылку, посвященную компьютерным вирусам. Дополнительную информацию можно найти в файле virus-l.README, доступном по протоколу FTP на сервере cs.ucr.edu в каталоге /pub/virus-l.

(3) Internet Firewalls[2]

Отправьте сообщение по адресу: majordomo@greatcircle.com

Текст сообщения: subscribe firewalls user@host

The Firewalls mailing list is a discussion forum for firewall administrators and implementors.

Рассылки USENET

(1) comp.security.announce[5]

Модерируемая группа comp.security.announce служит исключительно для распространения консультаций CERT.

(2) comp.security.misc[3]

Форум comp.security.misc служит для обсуждения вопросов компьютерной безопасности, преимущественно связанных с операционной системой UNIX(r).

(3) alt.security[4]

В форуме alt.security обсуждаются вопросы компьютерной безопасности, наряду с охранными системами и автомобильными сигнализациями.

(4) comp.virus[5]

Модерируемая группа comp.virus посвящена компьютерным вирусам. Дополнительную информацию можно найти в файле virus-l.README, доступном по протоколу FTP на сервере cs.ucr.edu в каталоге /pub/virus-l.

(5) comp.risks[6]

The comp.risks newsgroup is a moderated forum on the risks to the public in computers and related systems.

Страницы WWW

(1) http://www.first.org/

Computer Security Resource Clearinghouse. Основная тематика связана с реагированием на инциденты, угрозам в сфере компьютерной безопасности, уязвимостям и решению проблем безопасности. В то же время на сайте поддерживается каталог ссылок по разным аспектам компьютерной безопасности, включая риски, приватность, юридические вопросы, вирусы, политику безопасности, обучение.

(2) http://www.telstra.com.au/info/security.html

Каталог ссылок на этом сайте содержит информацию о ресурсах, посвященных сетям и компьютерной безопасности. Актуальность данных в каталоге обеспечивается недостаточно хорошо.

(3) http://www.alw.nih.gov/Security/security.html[7]

Эта страница посвящена общим вопросам компьютерной безопасности. Информация организована по темам, новые публикации выделены в специальный раздел.

(4) http://csrc.ncsl.nist.gov

На этом сайте NIST[8] содержится множество анонсов, программ и документов, связанных с компьютерной безопасностью.

9. Литература

Не все перечисленные ниже документы могут быть доступны в любой стране.

[Appelman, et. al., 1995] Appelman, Heller, Ehrman, White, and McAuliffe, "The Law and The Internet", USENIX 1995 Technical Conference on UNIX and Advanced Computing, New Orleans, LA, January 16-20, 1995.

[ABA, 1989] American Bar Association, Section of Science and Technology, "Guide to the Prosecution of Telecommunication Fraud by the Use of Computer Crime Statutes", American Bar Association, 1989.

[1]Не поддерживается в настоящее время. *Прим. перев.*
[2]На сайте greatcircle.com рассылка анонсируется, как действующая, однако ссылка на страницу списка не работает. *Прим. перев.*
[3]Не поддерживается. Заменой может служить одноименная группа Google. *Прим. перев.*
[4]Не поддерживается. Заменой может служить одноименная группа Google. *Прим. перев.*
[5]Не поддерживается. Заменой может служить одноименная группа Google. *Прим. перев.*
[6]Не поддерживается. Заменой может служить одноименная группа Google. *Прим. перев.*
[7]В настоящее время не поддерживается. *Прим. перев.*
[8]National Institute of Standards and Technology — Национальный институт стандартов и технологии (США).

[Aucoin, 1989] R. Aucoin, "Computer Viruses: Checklist for Recovery", Computers in Libraries, Vol. 9, No. 2, Pg. 4, February 1989.

[Barrett, 1996] D. Barrett, "Bandits on the Information Superhighway", O'Reilly & Associates, Sebastopol, CA, 1996.

[Bates, 1992] R. Bates, "Disaster Recovery Planning: Networks, Telecommunications and Data Communications", McGraw-Hill, 1992.

[Bellovin, 1989] S. Bellovin, "Security Problems in the TCP/IP Protocol Suite"[1], Computer Communication Review, Vol 19, 2, pp. 32-48, April 1989.

[Bellovin, 1990] S. Bellovin, and M. Merritt, "Limitations of the Kerberos Authentication System"[2], Computer Communications Review, October 1990.

[Bellovin, 1992] S. Bellovin, "There Be Dragon", USENIX: Proceedings of the Third Usenix Security Symposium, Baltimore, MD. September, 1992.

[Bender, 1894] D. Bender, "Computer Law: Evidence and Procedure", M. Bender, New York, NY, 1978-present.

[Bloombecker, 1990] B. Bloombecker, "Spectacular Computer Crimes", Dow Jones- Irwin, Homewood, IL. 1990.

[Brand, 1990] R. Brand, "Coping with the Threat of Computer Security Incidents: A Primer from Prevention through Recovery", R. Brand, 8 June 1990.

[Brock, 1989] J. Brock, "November 1988 Internet Computer Virus and the Vulnerability of National Telecommunications Networks to Computer Viruses", GAO/T-IMTEC-89-10, Washington, DC, 20 July 1989.

[BS 7799] British Standard, BS Tech Cttee BSFD/12, Info. Sec. Mgmt, "BS 7799 : 1995 Code of Practice for Information Security Management", British Standards Institution, London, 54, Effective 15 February 1995.

[Caelli, 1988] W. Caelli, Editor, "Computer Security in the Age of Information", Proceedings of the Fifth IFIP International Conference on Computer Security, IFIP/Sec '88.

[Carroll, 1987] J. Carroll, "Computer Security", 2nd Edition, Butterworth Publishers, Stoneham, MA, 1987.

[Cavazos and Morin, 1995] E. Cavazos and G. Morin, "Cyber-Space and The Law", MIT Press, Cambridge, MA, 1995.

[CCH, 1989] Commerce Clearing House, "Guide to Computer Law", (Topical Law Reports), Chicago, IL., 1989.

[Chapman, 1992] B. Chapman, "Network(In) Security Through IP Packet Filtering", USENIX: Proceedings of the Third UNIX Security Symposium, Baltimore, MD, September 1992.

[Chapman and Zwicky, 1995] B. Chapman and E. Zwicky, "Building Internet Firewalls", O'Reilly and Associates, Sebastopol, CA, 1995.

[Cheswick, 1990] B. Cheswick, "The Design of a Secure Internet Gateway", Proceedings of the Summer Usenix Conference, Anaheim, CA, June 1990.

[Cheswick1] W. Cheswick, "An Evening with Berferd In Which a Cracker is Lured, Endured, and Studied", AT&T Bell Laboratories.

[Cheswick and Bellovin, 1994] W. Cheswick and S. Bellovin, "Firewalls and Internet Security: Repelling the Wily Hacker", Addison-Wesley, Reading, MA, 1994.

[Conly, 1989] C. Conly, "Organizing for Computer Crime Investigation and Prosecution", U.S. Dept. of Justice, Office of Justice Programs, Under Contract Number OJP-86-C-002, National Institute of Justice, Washington, DC, July 1989.

[Cooper, 1989] J. Cooper, "Computer and Communications Security: Strategies for the 1990s", McGraw-Hill, 1989.

[CPSR, 1989] Computer Professionals for Social Responsibility, "CPSR Statement on the Computer Virus", CPSR, Communications of the ACM, Vol. 32, No. 6, Pg. 699, June 1989.

[CSC-STD-002-85, 1985] Department of Defense, "Password Management Guideline", CSC-STD-002-85, 12 April 1985, 31 pages.

[Curry, 1990] D. Curry, "Improving the Security of Your UNIX System", SRI International Report ITSTD-721-FR-90-21, April 1990.

[Curry, 1992] D. Curry, "UNIX System Security: A Guide for Users and Systems Administrators", Addision-Wesley, Reading, MA, 1992.

[DDN88] Defense Data Network, "BSD 4.2 and 4.3 Software Problem Resolution", DDN MGT Bulletin #43, DDN Network Information Center, 3 November 1988.

[1]Копия этой статьи доступна на сайте http://www.cs.columbia.edu/~smb/papers/ipext.pdf. *Прим. перев.*
[2]Копия этой статьи доступна на сайте http://www.cs.columbia.edu/~smb/papers/kerblimit.usenix.pdf. *Прим. перев.*

[DDN89] DCA DDN Defense Communications System, "DDN Security Bulletin 03", DDN Security Coordination Center, 17 October 1989.

[Denning, 1990] P. Denning, Editor, "Computers Under Attack: Intruders, Worms, and Viruses", ACM Press, 1990.

[Eichin and Rochlis, 1989] M. Eichin, and J. Rochlis, "With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988", Massachusetts Institute of Technology, February 1989.

[Eisenberg, et. al., 89] T. Eisenberg, D. Gries, J. Hartmanis, D. Holcomb, M. Lynn, and T. Santoro, "The Computer Worm", Cornell University, 6 February 1989.

[Ermann, Willians, and Gutierrez, 1990] D. Ermann, M. Williams, and C. Gutierrez, Editors, "Computers, Ethics, and Society", Oxford University Press, NY, 1990. (376 pages, includes bibliographical references).

[Farmer and Spafford, 1990] D. Farmer and E. Spafford, "The COPS Security Checker System", Proceedings of the Summer 1990 USENIX Conference, Anaheim, CA, Pgs. 165-170, June 1990.

[Farrow, 1991] Rik Farrow, "UNIX Systems Security", Addison-Wesley, Reading, MA, 1991.

[Fenwick, 1985] W. Fenwick, Chair, "Computer Litigation, 1985: Trial Tactics and Techniques", Litigation Course Handbook Series No. 280, Prepared for distribution at the Computer Litigation, 1985: Trial Tactics and Techniques Program, February-March 1985.

[Fites 1989] M. Fites, P. Kratz, and A. Brebner, "Control and Security of Computer Information Systems", Computer Science Press, 1989.

[Fites, Johnson, and Kratz, 1992] Fites, Johnson, and Kratz, "The Computer Virus Crisis", Van Hostrand Reinhold, 2nd edition, 1992.

[Forester and Morrison, 1990] T. Forester, and P. Morrison, "Computer Ethics: Tales and Ethical Dilemmas in Computing", MIT Press, Cambridge, MA, 1990.

[Foster and Morrision, 1990] T. Forester, and P. Morrison, "Computer Ethics: Tales and Ethical Dilemmas in Computing", MIT Press, Cambridge, MA, 1990. (192 pages including index.)

[GAO/IMTEX-89-57, 1989] U.S. General Accounting Office, "Computer Security - Virus Highlights Need for Improved Internet Management", United States General Accounting Office, Washington, DC, 1989.

[Garfinkel and Spafford, 1991] S. Garfinkel, and E. Spafford, "Practical Unix Security", O'Reilly & Associates, ISBN 0-937175-72-2, May 1991.

[Garfinkel, 1995] S. Garfinkel, "PGP:Pretty Good Privacy", O'Reilly & Associates, Sebastopol, CA, 1996.

[Garfinkel and Spafford, 1996] S. Garfinkel and E. Spafford, "Practical UNIX and Internet Security", O'Reilly & Associates, Sebastopol, CA, 1996.

[Gemignani, 1989] M. Gemignani, "Viruses and Criminal Law", Communications of the ACM, Vol. 32, No. 6, Pgs. 669-671, June 1989.

[Goodell, 1996] J. Goodell, "The Cyberthief and the Samurai: The True Story of Kevin Mitnick-And The Man Who Hunted Him Down", Dell Publishing, 1996.

[Gould, 1989] C. Gould, Editor, "The Information Web: Ethical and Social Implications of Computer Networking", Westview Press, Boulder, CO, 1989.

[Greenia, 1989] M. Greenia, "Computer Security Information Sourcebook", Lexikon Services, Sacramento, CA, 1989.

[Hafner and Markoff, 1991] K. Hafner and J. Markoff, "Cyberpunk: Outlaws and Hackers on the Computer Frontier", Touchstone, Simon & Schuster, 1991.

[Hess, Safford, and Pooch] D. Hess, D. Safford, and U. Pooch, "A Unix Network Protocol Security Study: Network Information Service", Texas A&M University.

[Hoffman, 1990] L. Hoffman, "Rogue Programs: Viruses, Worms, and Trojan Horses", Van Nostrand Reinhold, NY, 1990. (384 pages, includes bibliographical references and index.)

[Howard, 1995] G. Howard, "Introduction to Internet Security: From Basics to Beyond", Prima Publishing, Rocklin, CA, 1995.

[Huband and Shelton, 1986] F. Huband, and R. Shelton, Editors, "Protection of Computer Systems and Software: New Approaches for Combating Theft of Software and Unauthorized Intrusion", Papers presented at a workshop sponsored by the National Science Foundation, 1986.

[Hughes, 1995] L. Hughes Jr., "Actually Useful Internet Security Techniques", New Riders Publishing, Indianapolis, IN, 1995.

[IAB-RFC1087, 1989] Internet Activities Board, "Ethics and the Internet", RFC 1087, IAB, January 1989. Also appears in the Communications of the ACM, Vol. 32, No. 6, Pg. 710, June 1989.

[Icove, Seger, and VonStorch, 1995] D. Icove, K. Seger, and W. VonStorch, "Computer Crime: A Crimefighter's Handbook", O'Reilly & Associates, Sebastopol, CA, 1995.

[IVPC, 1996] IVPC, "International Virus Prevention Conference '96 Proceedings", NCSA, 1996.

[Johnson and Podesta] D. Johnson, and J. Podesta, "Formulating A Company Policy on Access to and Use and Disclosure of Electronic Mail on Company Computer Systems".

[Kane, 1994] P. Kane, "PC Security and Virus Protection Handbook: The Ongoing War Against Information Sabotage", M&T Books, 1994.

[Kaufman, Perlman, and Speciner, 1995] C. Kaufman, R. Perlman, and M. Speciner, "Network Security: PRIVATE Communication in a PUBLIC World", Prentice Hall, Englewood Cliffs, NJ, 1995.

[Kent, 1990] S. Kent, "E-Mail Privacy for the Internet: New Software and Strict Registration Procedures will be Implemented this Year", Business Communications Review, Vol. 20, No. 1, Pg. 55, 1 January 1990.

[Levy, 1984] S. Levy, "Hacker: Heroes of the Computer Revolution", Delta, 1984.

[Lewis, 1996] S. Lewis, "Disaster Recovery Yellow Pages", The Systems Audit Group, 1996.

[Littleman, 1996] J. Littleman, "The Fugitive Game: Online with Kevin Mitnick", Little, Brown, Boston, MA., 1996.

[Lu and Sundareshan, 1989] W. Lu and M. Sundareshan, "Secure Communication in Internet Environments: A Hierarchical Key Management Scheme for End-to-End Encryption", IEEE Transactions on Communications, Vol. 37, No. 10, Pg. 1014, 1 October 1989.

[Lu and Sundareshan, 1990] W. Lu and M. Sundareshan, "A Model for Multilevel Security in Computer Networks", IEEE Transactions on Software Engineering, Vol. 16, No. 6, Page 647, 1 June 1990.

[Martin and Schinzinger, 1989] M. Martin, and R. Schinzinger, "Ethics in Engineering", McGraw Hill, 2nd Edition, 1989.

[Merkle] R. Merkle, "A Fast Software One Way Hash Function", Journal of Cryptology, Vol. 3, No. 1.

[McEwen, 1989] J. McEwen, "Dedicated Computer Crime Units", Report Contributors: D. Fester and H. Nugent, Prepared for the National Institute of Justice, U.S. Department of Justice, by Institute for Law and Justice, Inc., under contract number OJP-85-C-006, Washington, DC, 1989.

[MIT, 1989] Massachusetts Institute of Technology, "Teaching Students About Responsible Use of Computers", MIT, 1985-1986. Also reprinted in the Communications of the ACM, Vol. 32, No. 6, Pg. 704, Athena Project, MIT, June 1989.

[Mogel, 1989] Mogul, J., "Simple and Flexible Datagram Access Controls for UNIX-based Gateways", Digital Western Research Laboratory Research Report 89/4, March 1989.

[Muffett, 1992] A. Muffett, "Crack Version 4.1: A Sensible Password Checker for Unix"

[NCSA1, 1995] NCSA, "NCSA Firewall Policy Guide", 1995.

[NCSA2, 1995] NCSA, "NCSA's Corporate Computer Virus Prevention Policy Model", NCSA, 1995.

[NCSA, 1996] NCSA, "Firewalls & Internet Security Conference '96 Proceedings", 1996.

[NCSC-89-660-P, 1990] National Computer Security Center, "Guidelines for Formal Verification Systems", Shipping list no.: 89-660-P, The Center, Fort George G. Meade, MD, 1 April 1990.

[NCSC-89-254-P, 1988] National Computer Security Center, "Glossary of Computer Security Terms", Shipping list no.: 89-254-P, The Center, Fort George G. Meade, MD, 21 October 1988.

[NCSC-C1-001-89, 1989] Tinto, M., "Computer Viruses: Prevention, Detection, and Treatment", National Computer Security Center C1 Technical Report C1-001-89, June 1989.

[NCSC Conference, 1989] National Computer Security Conference, "12th National Computer Security Conference: Baltimore Convention Center, Baltimore, MD, 10-13 October, 1989: Information Systems Security, Solutions for Today - Concepts for Tomorrow", National Institute of Standards and National Computer Security Center, 1989.

[NCSC-CSC-STD-003-85, 1985] National Computer Security Center, "Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments", CSC-STD-003-85, NCSC, 25 June 1985.

[NCSC-STD-004-85, 1985] National Computer Security Center, "Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements", CSC-STD-004-85, NCSC, 25 June 1985.

[NCSC-STD-005-85, 1985] National Computer Security Center, "Magnetic Remanence Security Guideline", CSC-STD-005-85, NCSC, 15 November 1985.

[NCSC-TCSEC, 1985] National Computer Security Center, "Trusted Computer System Evaluation Criteria", DoD 5200.28-STD, CSC-STD-001-83, NCSC, December 1985.

[NCSC-TG-003, 1987] NCSC, "A Guide to Understanding DISCRETIONARY ACCESS CONTROL in Trusted Systems", NCSC-TG-003, Version-1, 30 September 1987, 29 pages.

[NCSC-TG-001, 1988] NCSC, "A Guide to Understanding AUDIT in Trusted Systems", NCSC-TG-001, Version-2, 1 June 1988, 25 pages.

[NCSC-TG-004, 1988] National Computer Security Center, "Glossary of Computer Security Terms", NCSC-TG-004, NCSC, 21 October 1988.

[NCSC-TG-005, 1987] National Computer Security Center, "Trusted Network Interpretation", NCSC-TG-005, NCSC, 31 July 1987.

[NCSC-TG-006, 1988] NCSC, "A Guide to Understanding CONFIGURATION MANAGEMENT in Trusted Systems", NCSC-TG-006, Version-1, 28 March 1988, 31 pages.

[NCSC-TRUSIX, 1990] National Computer Security Center, "Trusted UNIX Working Group (TRUSIX) rationale for selecting access control list features for the UNIX system", Shipping list no.: 90-076-P, The Center, Fort George G. Meade, MD, 1990.

[NRC, 1991] National Research Council, "Computers at Risk: Safe Computing in the Information Age", National Academy Press, 1991.

[Nemeth, et. al, 1995] E. Nemeth, G. Snyder, S. Seebass, and T. Hein, "UNIX Systems Administration Handbook", Prentice Hall PTR, Englewood Cliffs, NJ, 2nd ed. 1995.

[NIST, 1989] National Institute of Standards and Technology, "Computer Viruses and Related Threats: A Management Guide", NIST Special Publication 500-166, August 1989.

[NSA] National Security Agency, "Information Systems Security Products and Services Catalog", NSA, Quarterly Publication.

[NSF, 1988] National Science Foundation, "NSF Poses Code of Networking Ethics", Communications of the ACM, Vol. 32, No. 6, Pg. 688, June 1989. Also appears in the minutes of the regular meeting of the Division Advisory Panel for Networking and Communications Research and Infrastructure, Dave Farber, Chair, November 29-30, 1988.

[NTISSAM, 1987] NTISS, "Advisory Memorandum on Office Automation Security Guideline", NTISSAM COMPUSEC/1-87, 16 January 1987, 58 pages.

[OTA-CIT-310, 1987] United States Congress, Office of Technology Assessment, "Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information", OTA-CIT-310, October 1987.

[OTA-TCT-606] Congress of the United States, Office of Technology Assessment, "Information Security and Privacy in Network Environments", OTA-TCT-606, September 1994.

[Palmer and Potter, 1989] I. Palmer, and G. Potter, "Computer Security Risk Management", Van Nostrand Reinhold, NY, 1989.

[Parker, 1989] D. Parker, "Computer Crime: Criminal Justice Resource Manual", U.S. Dept. of Justice, National Institute of Justice, Office of Justice Programs, Under Contract Number OJP-86-C-002, Washington, D.C., August 1989.

[Parker, Swope, and Baker, 1990] D. Parker, S. Swope, and B. Baker, "Ethical Conflicts: Information and Computer Science, Technology and Business", QED Information Sciences, Inc., Wellesley, MA. (245 pages).

[Pfleeger, 1989] C. Pfleeger, "Security in Computing", Prentice-Hall, Englewood Cliffs, NJ, 1989.

[Quarterman, 1990] J. Quarterman, J., "The Matrix: Computer Networks and Conferencing Systems Worldwide", Digital Press, Bedford, MA, 1990.

[Ranum1, 1992] M. Ranum, "An Internet Firewall", Proceedings of World Conference on Systems Management and Security, 1992.

[Ranum2, 1992] M. Ranum, "A Network Firewall", Digital Equipment Corporation Washington Open Systems Resource Center, June 12, 1992.

[Ranum, 1993] M. Ranum, "Thinking About Firewalls", 1993.

[Ranum and Avolio, 1994] M. Ranum and F. Avolio, "A Toolkit and Methods for Internet Firewalls", Trustest Information Systems, 1994.

[Reinhardt, 1992] R. Reinhardt, "An Architectural Overview of UNIX Network Security"

[Reinhardt, 1993] R. Reinhardt, "An Architectural Overview of UNIX Network Security", ARINC Research Corporation, February 18, 1993.

[Reynolds-RFC1135, 1989] The Helminthiasis of the Internet, RFC 1135, USC/Information Sciences Institute, Marina del Rey, CA, December 1989.

[Russell and Gangemi, 1991] D. Russell and G. Gangemi, "Computer Security Basics" O'Reilly & Associates, Sebastopol, CA, 1991.

[Schneier 1996] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", John Wiley & Sons, New York, second edition, 1996.

[Seeley, 1989] D. Seeley, "A Tour of the Worm", Proceedings of 1989 Winter USENIX Conference, Usenix Association, San Diego, CA, February 1989.

[Shaw, 1986] E. Shaw Jr., "Computer Fraud and Abuse Act of 1986", Congressional Record (3 June 1986), Washington, D.C., 3 June 1986.

[Shimomura, 1996] T. Shimomura with J. Markoff, "Takedown:The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw-by the Man Who Did It", Hyperion, 1996.

[Shirey, 1990] R. Shirey, "Defense Data Network Security Architecture", Computer Communication Review, Vol. 20, No. 2, Page 66, 1 April 1990.

[Slatalla and Quittner, 1995] M. Slatalla and J. Quittner, "Masters of Deception: The Gang that Ruled Cyberspace", Harper Collins Publishers, 1995.

[Smith, 1989] M. Smith, "Commonsense Computer Security: Your Practical Guide to Preventing Accidental and Deliberate Electronic Data Loss", McGraw-Hill, New York, NY, 1989.

[Smith, 1995] D. Smith, "Forming an Incident Response Team", Sixth Annual Computer Security Incident Handling Workshop, Boston, MA, July 25-29, 1995.

[Spafford, 1988] E. Spafford, "The Internet Worm Program: An Analysis", Computer Communication Review, Vol. 19, No. 1, ACM SIGCOM, January 1989. Also issued as Purdue CS Technical Report CSD-TR-823, 28 November 1988.

[Spafford, 1989] G. Spafford, "An Analysis of the Internet Worm", Proceedings of the European Software Engineering Conference 1989, Warwick England, September 1989. Proceedings published by Springer-Verlag as: Lecture Notes in Computer Science #387. Also issued as Purdue Technical Report #CSD-TR-933.

[Spafford, Keaphy, and Ferbrache, 1989] E. Spafford, K. Heaphy, and D. Ferbrache, "Computer Viruses: Dealing with Electronic Vandalism and Programmed Threats", ADAPSO, 1989. (109 pages.)

[Stallings1, 1995] W. Stallings, "Internet Security Handbook", IDG Books, Foster City CA, 1995.

[Stallings2, 1995] W. Stallings, "Network and InterNetwork Security", Prentice Hall, , 1995.

[Stallings3, 1995] W. Stallings, "Protect Your Privacy: A Guide for PGP Users" PTR Prentice Hall, 1995.

[Stoll, 1988] C. Stoll, "Stalking the Wily Hacker", Communications of the ACM, Vol. 31, No. 5, Pgs. 484-497, ACM, New York, NY, May 1988.

[Stoll, 1989] C. Stoll, "The Cuckoo's Egg", ISBN 00385-24946-2, Doubleday, 1989.

[Treese and Wolman, 1993] G. Treese and A. Wolman, "X Through the Firewall, and Other Applications Relays", Digital Equipment Corporation, Cambridge Research Laboratory, CRL 93/10, May 3, 1993.

[Trible, 1986] P. Trible, "The Computer Fraud and Abuse Act of 1986", U.S. Senate Committee on the Judiciary, 1986.

[Venema] W. Venema, "TCP WRAPPER: Network monitoring, access control, and booby traps", Mathematics and Computing Science, Eindhoven University of Technology, The Netherlands.

[USENIX, 1988] USENIX, "USENIX Proceedings: UNIX Security Workshop", Portland, OR, August 29-30, 1988.

[USENIX, 1990] USENIX, "USENIX Proceedings: UNIX Security II Workshop", Portland, OR, August 27-28, 1990.

[USENIX, 1992] USENIX, "USENIX Symposium Proceedings: UNIX Security III", Baltimore, MD, September 14-16, 1992.

[USENIX, 1993] USENIX, "USENIX Symposium Proceedings: UNIX Security IV", Santa Clara, CA, October 4-6, 1993.

[USENIX, 1995] USENIX, "The Fifth USENIX UNIX Security Symposium", Salt Lake City, UT, June 5-7, 1995.

[Wood, et.al., 1987] C. Wood, W. Banks, S. Guarro, A. Garcia, V. Hampel, and H. Sartorio, "Computer Security: A Comprehensive Controls Checklist", John Wiley and Sons, Interscience Publication, 1987.

[Wrobel, 1993] L. Wrobel, "Writing Disaster Recovery Plans for Telecommunications Networks and LANS", Artech House, 1993.

[Vallabhaneni, 1989] S. Vallabhaneni, "Auditing Computer Security: A Manual with Case Studies", Wiley, New York, NY, 1989.

Вопросы безопасности

Весь документ посвящен обсуждению вопросов безопасности.

Сведения о редакторе

Barbara Y. Fraser

Software Engineering Institute

Carnegie Mellon University

5000 Forbes Avenue

Pittsburgh, PA 15213

Phone: (412) 268-5010

Fax: (412) 268-6989

EMail: byf@cert.org

Перевод на русский язык

Николай Малых

nmalykh@protocols.ru