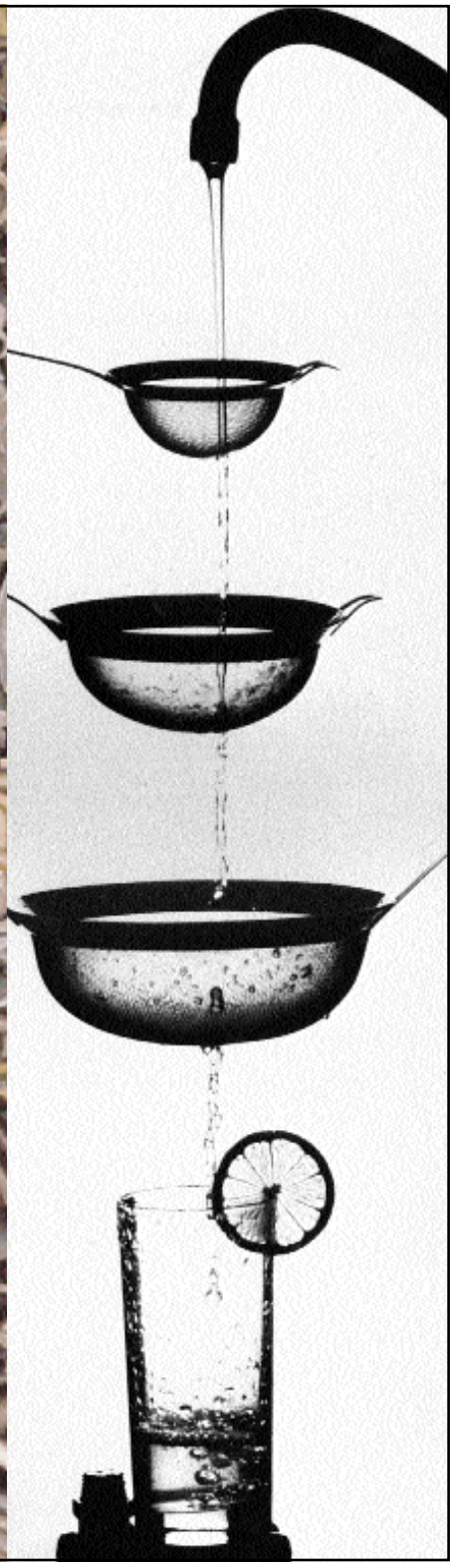
Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 3 (82)/2000

Дополнение к Руководству по информационной безопасности предприятия: Как выбирать поставщика Интернет-услуг



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Дополнение к Руководству по информационной безопасности предприятия:

Как выбирать поставщика Интернет-услуг

Тристан Дебопюи
(редактор)

СОДЕРЖАНИЕ

Аннотация

Данное Дополнение к Руководству по информационной безопасности предприятия [RFC2196] (см. также Jet Info, 1996, 10-11 — прим. перев.) призвано служить для широкой Интернет-общественности контрольным перечнем при обсуждении вопросов информационной безопасности с поставщиками Интернет-услуг, уже выбранными или только выбираемыми. К сожалению, подобные обсуждения требований безопасности происходят пока весьма нечасто.

Дополнение предназначено тем, кто принимает решения о закупке Интернет-услуг (потребителям). В данном документе выделено три типа потребителей: потребители коммуникационных услуг, услуг по размещению ресурсов, а также потребители, разместившиеся там же, где и поставщики услуг.

Еще одна цель Дополнения состоит в том, чтобы, информируя поставщиков Интернет-услуг об ожиданиях общественности, побудить их принять упреждающие меры, сделав безопасность не просто приоритетным направлением развития, но предметом гордости, который демонстрируется всем покупателям. Общепризнано, что производители начинают заботиться о безопасности только под нажимом потребителей. Мы надеемся, что данный документ поможет обеим сторонам яснее выразить степень своей озабоченности вопросами информационной безопасности, и что интенсивность дискуссий общественности с поставщиками Интернет-услуг будет нарастать.

Отметим, что мы выделили весьма широкие категории, так что конкретный потребитель может не соответствовать в точности ни одной из них. По этой причине не все контрольные вопросы применимы ко всем потребителям, равно как и ко всем поставщикам Интернет-услуг.

1. Цели работы

Данное Дополнение к Руководству призвано помочь в выработке политики и процедур безопасности в организациях, информационные системы которых подключены к Интернет (надеемся, впрочем, что Дополнение окажется полезным и для тех, кто пока такого подключения не имеет). Будут перечислены вопросы и аспекты, которые необходимо рассмотреть при выработке в организации собственной политики безопасности. Предлагается ряд рекомендаций, обсуждаются смежные вопросы.

Дополнение к Руководству — это лишь основа для выработки политики и процедур безопасности. Чтобы сделать их эффективными, специалистам организации необходимо принять множество решений, заключить целый ряд соглашений, наконец, довести решения до исполнителей и позаботиться об их проведении в жизнь.

2. Целевая аудитория

В качестве предполагаемых читателей данного документа видятся системные и сетевые администраторы, а также лица, принимающие решения (обычно это руководители среднего звена). По соображениям краткости в последующем тексте мы будем использовать термин «администратор» применительно как к системным, так и сетевым администраторам.

Дополнение не ориентировано на программистов или разработчиков защищенных программ или систем. Изложение концентрируется вокруг политики и процедур, которые необходимо ввести в действие для поддержки технических средств безопасности, имеющихся в организации.

Документ рассчитан в первую очередь на организации, входящие в Интернет-сообщество, однако он может быть полезен для всех, у кого есть внешние коммуникации. В качестве общего руководства по политике безопасности Дополнение, возможно, пригодится и владельцам изолированных систем.

Цель документа — сформулировать требования (или, мягче, ожидания) широкой Интернет-общественности к поставщикам Интернет услуг, касающиеся информационной безопасности.

Мы определяем поставщика Интернет-услуг как организацию, обеспечивающую для других подключение к Интернет, а также иные Интернет-услуги, в том числе размещение Web-серверов, поставка информационного наполнения, услуги электронной почты и т.д. Организации, обслуживаю-

Tristan Debeaupuis (editor). Site Security Handbook Addendum for ISPs. – Internet Draft, GRIP Working Group, 15 August 1999.
Перевод выполнен с небольшими сокращениями и дополнениями.

щие только себя, мы в число поставщиков Интернет-услуг не включаем.

Наша цель состоит в том, чтобы потребители знали, как построить обсуждение вопросов безопасности с потенциальным поставщиком Интернет-услуг, обсуждение, которое, к величайшему сожалению, в наше время является редкостью.

Данный документ предназначен тем, кто принимает решения о закупке Интернет-услуг (потребителям)

Еще одна цель Дополнения — проинформировать поставщиков Интернет-услуг об ожиданиях общественности, побуждая их тем самым принять упреждающие меры, сделав безопасность не просто приоритетным направлением развития, но предметом гордости, который демонстрируется всем покупателям. Общепризнано, что производители начинают заботиться о безопасности только под нажимом потребителей. Мы надеемся, что данный документ поможет обеим сторонам яснее выразить степень своей озабоченности вопросами информационной безопасности, и что интенсивность дискуссий общественности с поставщиками Интернет-услуг будет нарастать.

Разумеется, мы ни в коем случае не навязываем кому-либо какой-то определенный способ ведения дел.

2.1. Соглашения, используемые в данном документе

Ключевые слова «ТРЕБУЕТСЯ», «ДОЛЖЕН», «НЕ ДОЛЖЕН», «СЛЕДУЕТ», «НЕ СЛЕДУЕТ» и «МОЖЕТ» должны интерпретироваться так, как это описано в документе «Key words for use in RFCs to Indicate Requirement Levels» [RFC2119].

3. Реагирование на нарушения безопасности

Группа реагирования на нарушения информационной безопасности (Security Incident Response Team, SIRT) осуществляет, координирует и поддерживает реагирование на нарушения в организациях в пределах зоны ответственности группы. То, что Интернет-сообщество ожидает от подобных групп, описано в документе «Expectations for Computer Security Incident Response» [RFC2350].

Независимо от того, есть ли у поставщика Интернет-услуг группа реагирования, он должен определить и довести до потребителей порядок передачи и обработки докладов о нарушениях. Кроме того, он должен ясно документировать возможности поставщика услуг по реагированию на доклады о нарушениях.

3.1. Поставщики Интернет-услуг и группы реагирования на нарушения информационной безопасности

У некоторых поставщиков Интернет-услуг есть группы реагирования на нарушения информационной безопасности. Однако, не следует предполагать, что потребители услуг подключения к Интернет или те, чьи системы атакованы с площадки данного поставщика, автоматически получают в свое распоряжение помощь соответствующей группы. Такая помощь часто предоставляется в качестве дополнительно оплачиваемой услуги, а группа включает в зону своей ответственности только тех, кто специально подписался (вероятно, небесплатно) на услуги реагирования.

Таким образом, важно уяснить, какие виды реагирования на нарушения и ресурсы безопасности доступны Вам, а также определить цепочку эскалации докладов о нарушениях ДО ТОГО, как нарушение случилось.

Потребителям следует узнать, есть ли у поставщика Интернет-услуг группа реагирования, какие у нее права, правила работы и предоставляемые услуги. Соответствующую информацию лучше всего оформить в виде, рекомендуемом в приложении D документа [RFC2350]. Если у поставщика Интернет-услуг нет группы реагирования, ему следует определить, какую роль он возьмет на себя (если возьмет вообще) при реагировании на нарушение, и существует ли группа, ответственность которой распространяется на потребителя, так что этой группе можно направлять доклады о нарушениях.

Поставщику Интернет-услуг СЛЕДУЕТ, в соответствии со спецификацией [RFC2142], иметь почтовый ящик SECURITY для сообщений о нарушениях безопасности, ABUSE — для сообщений о ненадлежащем поведении и NOC — для сообщений о проблемах в сетевой инфраструктуре. В спецификации [RFC2142] указаны дополнительные адреса для приема запросов и докладов, касающихся других услуг.

Для предоставления более детальной информации по вопросам, перечисленным в предыдущем абзаце, поставщик Интернет-услуг может использовать общепринятые локаторы ресурсов, например, http://www.имя_поставщика.net/security/.

Кроме того, на поставщике Интернет-услуг лежит обязанность обеспечения полноты, достоверности и доступности своей контактной информации (в сервисе Whois, маршрутном реестре и других хранилищах).

Когда происходит нарушение информационной безопасности, затрагивающее инфраструктуру поставщика Интернет-услуг, следует немедленно сообщить потребителям такие сведения:

- кто координирует реакцию на нарушение;
- какая слабость использована атакующим;
- как нарушение сказалось на предоставляемых услугах;
- что делается для реагирования на нарушение;
- могут ли быть скомпрометированы данные потребителей;
- что делается для устранения выявленной слабости;
- предполагаемый график реагирования, если он может быть составлен.

3.2. Помощь в реагировании на «входящие» нарушения

Если имеет место нарушение, направленное на какого-либо потребителя услуг подключения, поставщик Интернет-услуг должен проинформировать потребителя об атаке. Поставщик Интернет-услуг может также оказать помощь в следующем:

- Проследить «видимый» источник атаки и попытаться определить достоверность каждого шага на этом пути (учитывая, что не исключена подделка исходного адреса). Если исходный адрес подделан, поставщик Интернет-услуг может определить точку в своей сети, через которую поступает поток данных злоумышленника.
- Получить контактную информацию источника атаки, используя whois [RFC1834 и RFC1835], DNS [RFC1034 и RFC1035] или соответствующие общепринятые имена почтовых ящиков [RFC2142].
- Собрать и защитить свидетельства нарушения, предохраняя их от уничтожения или непреднамеренного разглашения.

Если нарушение продолжается, по запросу потребителя поставщик Интернет-услуг может оказать помощь путем протоколирования с целью дальнейшей диагностики проблемы или путем фильтрации определенных видов трафика.

3.3. Помощь в реагировании на «исходящие» или «транзитные» нарушения

Если кто-то из потребителей Интернет-услуг, по-видимому, является источником нарушения информационной безопасности, на поставщика услуг посыпятся многочисленные обращения. Поставщик Интернет-услуг может помочь администраторам источника и цели атаки, вступив с ними в контакт и (что делается чаще всего) переслав потребителю контактную информацию для связи с «пострадавшими».

К поставщику Интернет-услуг могут также обратиться за помощью в случае атак, которые проходят через его сеть, но используют поддельные исходные адреса (например, это может быть SYN flooding, см. [CA-96.21.tcpsynflooding]). В такой ситуации помощь может состоять в использовании сетевой регистрационной информации, генерируемой маршрутизаторами, чтобы найти точку, в которой поток данных с поддельными адресами вошел в сеть поставщика Интернет-услуг. При прослеживании источника подобных атак нередко требуется координация усилий со смежными поставщиками для формирования полной цепочки групп реагирования на всем пути атаки.

3.4. Передача информации и аутентификация

Поставщикам Интернет-услуг СЛЕДУЕТ иметь ясные правила и процедуры, касающиеся разделения информации о нарушении безопасности со своими потребителями, с другими поставщиками или группами реагирования, с правоохранительными органами, средствами массовой информации и общественностью.

> Наша цель состоит в том, чтобы потребители знали, как построить обсуждение вопросов безопасности с потенциальным поставщиком Интернет-услуг, обсуждение, которое, к величайшему сожалению, в наше время является редкостью

Поставщикам Интернет-услуг СЛЕДУЕТ иметь средства для организации защищенного канала с целью передачи подобной информации. Отметим, однако, что не везде законы разрешают защищенные коммуникации.

4. Защита Интернет-сообщества

Поставщики Интернет-услуг играют критически важную роль в повышении безопасности Интернет. В этом и следующем разделах рассматриваются меры, которые, в случае их скоординированного и оперативного принятия поставщиками Интернет-услуг, оказали бы на сетевую безопасность существенное положительное влияние и значительно затруднили злоумышленникам сокрытие следов.

Затем мы относительно подробно рассмотрим вопросы, касающиеся специфических услуг, таких как входная фильтрация и организация от-

крытых систем промежуточного хранения и пересылки почтовых сообщений. Согласованное решение этих вопросов поставщиками Интернет-услуг также дало бы заметный позитивный эффект.

Каждому поставщику Интернет-услуг СЛЕДУЕТ иметь политику добропорядочного пользования.

Контракт между поставщиком и потребителем Интернет-услуг следует составлять с учетом этой политики, быть может, пересматривая политику при продлении контракта. Потребителя следует заранее информировать об изменениях в политике.

В политике следует ясно определить, что потребители могут или не должны делать в разных частях сети и на разных системах, включая допустимые типы трафика.

4.1. Защита данных

Во многих странах есть законы о защите данных. В ситуациях, когда подобные законы применимы, поставщики Интернет-услуг должны проанализировать характер поступающих к ним персональных данных и, если нужно, принять меры, препятствующие противозаконному использованию данных. Учитывая глобальный характер Интернет, поставщикам Интернет-услуг, действующим в странах, где таких законов нет, следует хотя бы ознакомиться с идеей защиты данных, прочитав, например, Data Protection Act [DPR1998].

Каждому поставщику Интернет-услуг СЛЕДУЕТ иметь политику добропорядочного пользования

4.2. Обучение

Важно, чтобы весь штат поставщика Интернет-услуг был соответствующим образом подготовлен, то есть постоянно помнил о проблемах информационной безопасности, с пониманием подходил к их решению, умел должным образом применять средства повышения безопасности. К числу наиболее важных принадлежат вопросы использования защищенных каналов для передачи конфиденциальной информации, риска атак с применением методов морально-психологического воздействия, управления аутентификационными данными и т.д.

5. Сетевая инфраструктура

Поставщики Интернет-услуг ответственны за такое управление сетевой инфраструктурой Интернет, чтобы:

- обеспечивалась разумная устойчивость к появлению известных слабостей в защите;
- атакующие не могли легко и просто организовать плацдарм для последующих атак.

5.1. Маршрутизаторы

Маршрутизаторы не только сами по себе являются притягательными целями атак на безопасность, но и представляют собой отличный плацдарм для организации атак на другие цели.

Многие маршрутизаторы позволяют злоумышленникам делать опасные вещи, например:

- «прослушивать» транзитные потоки данных;
- манипулировать таблицами маршрутизации для перенаправления потоков данных;
- изменять состояние интерфейсов с целью нарушения обслуживания;
- вызывать «трепыхание» маршрутных таблиц, чреватое отказом в обслуживании для крупных частей Интернет;
- создавать пакеты с поддельными адресами и любым желаемым набором флагов;
- порождать штормы ICMP-пакетов, устраивать другие атаки на доступность;
- отправлять потоки данных в «черную дыру» (например, организуя локальный маршрут на пустой или некорректный интерфейс или на некорректный следующий маршрутизатор, который не знает нужного маршрута и не имеет подразумеваемого маршрутизатора, или, что хуже всего, используя протокол динамической маршрутизации для афиширования маршрута с низкой стоимостью, активно втягивая тем самым трафик в черную дыру);
- скрывать обращения по внешним адресам, что облегчается недостаточным протоколированием в маршрутизаторах.

Усилению подобных угроз способствует та центральная роль, которую играют маршрутизаторы в сетевой инфраструктуре, а также нередко доступная им широкая полоса пропускания.

Таким образом, доступ к маршрутизаторам СЛЕДУЕТ основывать на одноразовых паролях или еще более сильных средствах (таких, например, как Kerberos) и ограничивать в максимально возможной степени. Обращения к маршрутизатору следует протоколировать, привлекая ресурсы других систем.

Если маршрутизатор поддерживает различные уровни авторизации, эти уровни следует использовать для ограничения привилегированного доступа к маршрутизатору.

Сеансы взаимодействия с маршрутизаторами следует шифровать для предотвращения краж сеансов или данных и для недопущения атак, основанных на воспроизведении трафика.

> Маршрутизаторы не только сами по себе являются притягательными целями атак на безопасность, но и представляют собой отличный плацдарм для организации атак на другие цели

На маршрутизаторы не следует возлагать выполнение мелких услуг, которые нередко включены по умолчанию. Имеются в виду bootp, chargen, daytime, discard, echo, finger и т.д.

5.2. Коммутаторы, терминальные серверы, модемы и другое сетевое оборудование

Поставщикам Интернет-услуг следует быть столь же бдительными при конфигурировании всех видов сетевого оборудования. К сожалению, многие подобные устройства, находящиеся в эксплуатации, поддерживают лишь слабые методы аутентификации, предоставляют права доступа по принципу «все или ничего» и не протоколируют почти (или совсем) ничего. В прошлом у поставщиков Интернет-услуг не оставалось улик, по которым можно было бы проследить нарушителя, после того как он переконфигурировал коммутаторы, использовал терминальные серверы для атак на сторонние организации или выключил источники бесперебойного питания.

По возможности доступ к сетевому оборудованию следует ограничивать, предоставляя его только уполномоченным сетевым администраторам.

Оборудование, составляющее сетевую инфраструктуру, нередко не поддерживает сколько-нибудь развернутого внутреннего протоколирования, поскольку в нем нет долговременной памяти, такой как жесткие диски компьютеров. Впрочем, многие устройства поддерживают syslog или SNMP-сообщения или, по крайней мере, небольшой внутренний регистрационный журнал или отладочный режим, так что соответствующую информацию можно направить на консоль или в удаленный протокол.

Конфигурационную информацию маршрутизаторов и коммутаторов следует обязательно сопровождать на файловом сервере, чтобы возврат к прежней конфигурации мог быть выполнен легко и быстро. Разумеется, подобные резервные конфигурационные файлы следует защитить от несанкционированной передачи или злоумышленного изменения.

5.3. Анонимный telnet и другие непротоколируемые соединения

Имеется много сетевых устройств, от недорогих маршрутизаторов до принтеров, принимающих соединения по протоколу telnet без запроса пароля. Разумеется, подобные устройства, зачастую лишенные средств протоколирования, весьма популярны среди злоумышленников, желающих скрыть свои следы.

Если в сети поставщика Интернет-услуг есть такое оборудование, доступ к нему следует ограничить. Кроме того, потребителям следует рекомендовать блокировать доступ к подобным устройствам из внешних сетей.

Крайне нежелательно использовать протокол telnet для управления компонентами сети.

5.4. Центр управления сетью и сетевое администрирование

Центр управления сетью (ЦУС) является критически важной частью инфраструктуры поставщика Интернет-услуг, поэтому его работу следует строить с соблюдением должных мер безопасности.

ЦУС зачастую располагает административным контролем над конфигурационной информацией сетевого оборудования, поэтому следует проявить бдительность, ограничив доступ к такой информации. Загрузка конфигурационных файлов в сетевые устройства до сих пор нередко производится по протоколу TFTP [RFC1350], который не только лишен средств аутентификации и использует незащищенные коммуникации, но и требует повышенной осторожности при конфигурировании на серверной стороне (см. [CA-91:18.Active.Internet.tftp.Attacks]).

Как правило, ЦУС выполняет функции мониторинга сети, периодически опрашивая (например, посредством SNMP-сообщения Echo) множество сетевых устройств. При определении набора опрашиваемых устройств следует помнить о критически важной роли оборудования, перечисленного в разделе 5.2.

Помимо простого опроса, ЦУС для взаимодействия с сетевыми устройствами может также использовать управляющий протокол, такой как SNMP. Обычно протокол применяется для выяснения (посредством операции get) значений различных переменных, таких как число пакетов, принятых через определенный интерфейс. Однако, протокол может применяться и для установки переменных (операция set), возможно, с далеко идущими последствиями (такими как переконфигурирование устройства). В любом случае, в протоколе SNMPv1 присутствует только тривиальная аутентификация. По возможности, SNMP следует применять только

как средство чтения, получения (get) информации от удаленных устройств. Полученную информацию следует трактовать как конфиденциальную.

Еще одно применение протокола SNMP состоит в уведомлении управляющей станции о возникновении исключительных ситуаций (SNMP trap). Такую информацию также следует считать конфиденциальной, а в ЦУСе следует проявить осторожность, чтобы подобные SNMP-сообщения сами по себе не вылились в атаку на доступность.

5.5. Физическая безопасность

Физической защите информационных систем следует уделять соответствующее внимание. Это особенно верно, если в одном месте располагается несколько систем, так что к ним имеют доступ сотрудники различных организаций с разной политикой безопасности.

Нас будут особенно интересовать три случая совместного расположения ресурсов:

- оборудование потребителей располагается на площадке поставщика Интернет-услуг;
- оборудование поставщика Интернет-услуг размещено на удаленной площадке под присмотром уполномоченного персонала;
- оборудование поставщика Интернет-услуг располагается на удаленной площадке без контроля физического доступа.

Скорее всего, потребителя может непосредственно затронуть первый случай. Если поставщик Интернет-услуг предоставляет площади для размещения оборудования потребителей, то возникает множество вопросов, связанных с доступом последних к своему оборудованию, соседствующему с системами поставщика услуг.

Потребителя не следует оставлять без присмотра вблизи чужого оборудования

В идеале, каждый потребитель должен получить полностью закрытую, запирающуюся «клетку», то есть небольшую комнату со стенами и проемами для прокладки множества проводов, а также со стойками для монтажа оборудования. Потребителям предоставляется доступ в отведенное помещение в сопровождении сотрудника поставщика Интернет-услуг (либо потребитель получает ключи только от своей комнаты).

Выделение отдельных комнат, однако, может оказаться слишком накладным, так что многие поставщики Интернет-услуг идут на компромисс, собирая все «чужое» оборудование в одном машинном зале и тщательно контролируя все, что делают потребители. К сожалению, этого может оказаться недостаточно, чтобы избежать недоразумений, таких как нечаянное отключение оборудования другого потребителя. Вместо единого открытого пространства, следует разделить зал перегородками, построив для каждого потребителя отдельное помещение с запирающейся дверью.

Потребителя не следует оставлять без присмотра вблизи чужого оборудования. Такое оборудование запрещается трогать, фотографировать или исследовать.

Следует помнить также о безопасности на втором уровне семиуровневой модели, запрещая разделение физического сегмента сети между оборудованием потребителя и компьютерами, принадлежащими другим потребителям или поставщику Интернет-услуг. Нередки случаи, когда злоумышленники пользуются слабостями в защите или незашифрованными удаленными входами в оборудование потребителя, получают контроль над этими устройствами, переводят его в режим прослушивания сегмента локальной сети, потенциально нарушая тем самым конфиденциальность или безопасность других устройств в этом сегменте.

Вопросы безопасности чрезвычайно важны и тогда, когда компоненты сетевой инфраструктуры поставщика Интернет-услуг размещены вне его территории (например, у партнера или в удаленной точке присутствия). Такие компоненты нередко являются жизненно важными с точки зрения топологии сети и, в то же время, они могут стать объектом атаки или пострадать от несчастного случая. Для ограничения физического доступа оборудование в идеальном случае следует размещать в полностью закрытых, запирающихся комнатах или «клетках». Если на чужой площади хранятся запчасти, их также следует защищать от кражи, порчи или встраивания «жучков». По возможности следует использовать системы безопасности и замки, открывающиеся персональными картами. Периодически удаленные компоненты нужно проверять на предмет встраивания постороннего оборудования, которое может использоваться для прослушивания сетевых соединений. Как и на других площадках, компьютеры не следует подключать к транзитным сегментам или допускать подсоединение к сети неиспользуемых физических интерфейсов.

5.6. Инфраструктура маршрутизации

Способность поставщика Интернет-услуг направлять потоки данных к правильному конечному пункту зависит от правил маршрутизации, заданных в виде маршрутных таблиц (см. [RFC1786]). Поставщикам Интернет-услуг следует убедиться, что находящаяся в их ведении маршрутная информация может быть изменена только после надежной аутентификации и что права на внесение изменений должным образом ограничены.

Рис. 1. Входная фильтрация IP-пакетов по исходным адресам.

Двойную осторожность следует проявлять и при решении вопроса о том, кому больше доверять при наличии нескольких маршрутов, ведущих к цели. В прошлом злоумышленное афиширование маршрутной информации приводило к попаданию потоков данных в «черную дыру» или, что хуже, к перехвату соединений. В граничных маршрутизаторах следует аутентифицировать соседей в рамках протокола BGP.

При выборе протоколов внутренней маршрутизации поставщикам Интернет-услуг также следует помнить о безопасности. При конфигурировании не следует предполагать, что перевычисления маршрутов редки и дороги, поскольку это открывает путь для атак на доступность. При изменении маршрутов следует использовать наивысший уровень аутентификации, поддерживаемый протоколом внутренней маршрутизации.

Если от партнеров начинает поступать большое число объявлений о наличии специфических маршрутов к частям выделенного поставщику Интернет-услуг пространства адресов, следует проявлять осторожность, решая, учитывать ли эти объявления. Впрочем, с данной проблемой могут столкнуться только поставщики, допускающие фрагментацию своего пространства адресов (то есть позволяющие потребителям сохранять адреса при смене поставщика Интернет-услуг). Предполагается, что используется бесклассовая междоменная маршрутизация (CIDR).

5.7. Входная фильтрация по исходным адресам

Направление входной фильтрации — от периферийной системы (потребитель) к Интернет.

Нередко атакующие скрывают следы, подделывая исходные адреса. Чтобы отвлечь внимание от своей системы, они выбирают в качестве исходного адрес невинной удаленной системы или даже из пространства адресов, выделенных для частных объединений сетей [RFC1918]. Кроме того, поддельные исходные адреса часто применяются в атаках, основанных на использовании отношения доверия между узлами сети.

Чтобы уменьшить область распространения атак, основанных на подделке исходных адресов, поставщики Интернет-услуг должны делать следующее. Во всех граничных маршрутизаторах, к которым подключены потребители, следует сразу отфильтровывать потоки данных, идущие от потребителей и имеющие исходные адреса, отличные от выделенных данному потребителю. Более подробно этот вопрос освещен в спецификации [RFC2267].

Иногда возникают ситуации, когда входная фильтрация пока оказывается невозможной. Например, большой агрегирующий маршрутизатор может не выдержать дополнительную нагрузку, вызванную применением пакетных фильтров. Кроме того, подобная фильтрация способна привести к трудностям для мобильных пользователей. Следовательно, хотя использование данного метода для борьбы с подделкой адресов настоятельно рекомендуется, оно не всегда возможно.

В тех редких случаях, когда входная фильтрация на стыке потребителя и поставщика Интернет-услуг невозможна, следует рекомендовать потребителю организовать входную фильтрацию внутри его сети. Вообще, фильтрацию следует производить как можно ближе к хостам.

5.8. Выходная фильтрация по исходным адресам

Направление выходной фильтрации — от Интернет к периферийной системе (потребитель).

В настоящее время в Интернет широко используется много приложений, считающих другие узлы сети надежными, основываясь исключительно на IP-адресах (например, r-команды, пришедшие из BSD). Такие приложения уязвимы по отношению к подделке IP-адресов (см. [CA-95.01.IP.spoofing]). Кроме того, имеются уязвимости по отноше-

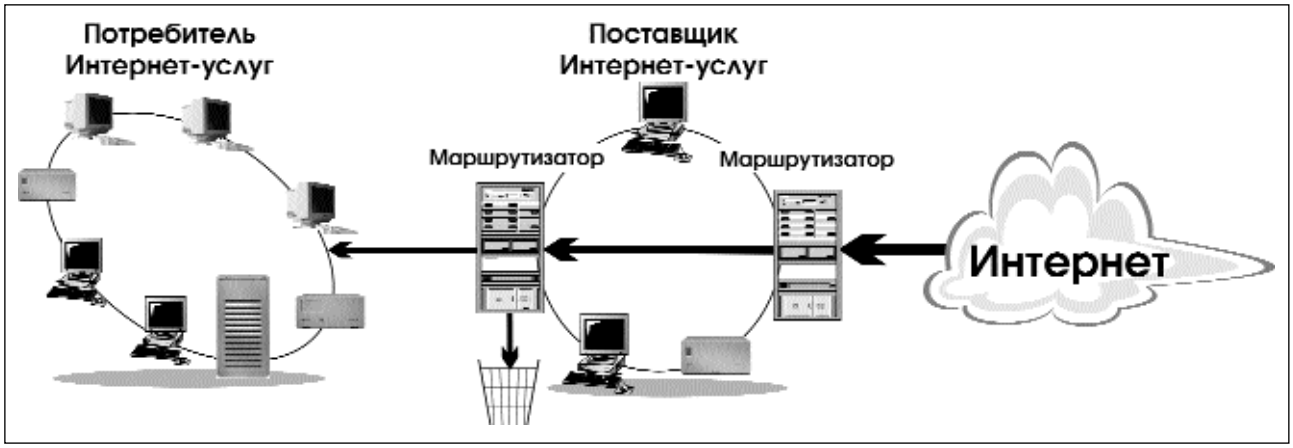


Рис. 2. Выходная фильтрация IP-пакетов по исходным адресам.

нию к злоумышленному использованию адресов, которые предполагаются локальными (например, land, см. [CA-97.28.TeardropLand]).

Чтобы усилить защиту потребителей от атак, основанных на подделке исходных адресов, поставщики Интернет-услуг должны делать следующее. Во всех граничных маршрутизаторах, к которым подключены потребители, следует сразу отфильтровывать потоки данных, идущие к потребителю и имеющие исходные адреса из пространства, выделенного этому потребителю.

Препятствия для входной фильтрации, описанные в пункте 5.7, делают невозможной и выходную фильтрацию.

5.9. Фильтрация маршрутной информации

Избыточные изменения маршрутной информации могут использоваться злоумышленником как средство увеличения загрузки, на базе которого развивается атака на доступность. Как минимум это приведет к деградации производительности.

Поставщикам Интернет-услуг следует отфильтровывать поступающие объявления о маршрутах, игнорируя, например, маршруты к адресам для частных объединений сетей, избегая фиктивных маршрутов и реализуя политику расщепления и агрегирования маршрутов.

Поставщики Интернет-услуг должны применять методы, уменьшающие риск нарастания нагрузки на маршрутизаторы в других частях сети. Следует отфильтровывать «кустарные» маршруты, настойчивое агрегирование и расщепление маршрутов. Все это снижает Ваше воздействие на других, когда Вы производите внутренние изменения, других не касающиеся.

5.10. Направленное вещание

Протокол IP поддерживает направленное вещание — посылку через сеть пакетов, которые в определенной подсети станут широковещательными. Практической пользы от такой возможности весьма немного, зато на ней основывается несколько различных видов атак (в первую очередь, это атаки на доступность, использующие эффект размножения широковещательных пакетов). Следовательно, маршрутизаторы, подключенные к вещательной среде, НЕ СЛЕДУЕТ конфигурировать так, чтобы было возможным непосредственное вещание на эту среду (см. [RFC2644]).

Если приходит пакет, на который маршрутизатор ответил бы, будь пакет послан в «невещательном» режиме, маршрутизатор МОЖЕТ послать (одиночный) ответ. Если он не отвечает (либо потому, что это не нужно, либо потому, что он так сконфигурирован), он МОЖЕТ послать ICMP-ошибку. Допускается также и молчаливое игнорирование подобных пакетов. В любом случае, такие пакеты нужно считать, чтобы выявить возможные попытки злоупотребления вещанием.

6. Системная инфраструктура

То, как поставщик Интернет-услуг управляет своими системами, критически важно для безопасности и надежного функционирования сети. Нарушения в работе систем могут в лучшем случае привести к снижению производительности или функциональности, но могут также вызвать потерю данных или сделать возможным перехват сетевого трафика (быть может, с последующей атакой методом «нелегального посредника»).

Следует действовать по принципу «Боливар на вывезет двоих», распределяя сервисы по системам. Иными словами, предоставление разных услуг следует возлагать на разные системы. Кроме выгод от облегчения системного администрирования, можно сослаться на многократно проверенный факт, что гораздо проще построить защищенную систему, если разные услуги (такие как почта, телеконференции или размещение Web-серверов) поддерживаются на разных системах.

Все обсуждаемые далее услуги выиграют от организации надежной защиты на сетевом уровне средствами IPsec.

6.1. Политика безопасности

Политика поставщика Интернет-услуг по отношению к защите персональных данных, обеспечению аутентичности, подотчетности, наложению защитных заплат, поддержке доступности, реагированию на доклады о нарушениях представляет интерес для потребителей. Ее следует опубликовать в общедоступном месте, например, на Web-сервере поставщика услуг.

Более детальное обсуждение политики безопасности можно найти в Руководстве по информационной безопасности предприятия (см. [RFC2196] и Jet Info, 1996, 10-11).

6.2. Управление системами

Доступ ко всем системам поставщика Интернет-услуг, выполняющим критически важные функции, такие как почта, телеконференции и размещение Web-серверов, следует ограничить, предоставляя его только администраторам соответствующих услуг. Доступ следует предоставлять только после надежной аутентификации и осуществлять по шифруемому каналу. Следует делать доступными из внешних сетей только те порты, на которых ожидают подключения предоставляемые услуги.

Если поставщик услуг ведет учет работы потребителей, то системы, обеспечивающие этот учет, следует изолировать от остальной части сети.

Если распространение и обновление программного обеспечения производится с помощью автоматизированных средств, таких как rdist, им следует предоставлять защищенный канал и надежную аутентификацию, применяя, например, Secure Shell (ssh) [SSH1997].

Системы не следует подключать к транзитным сегментам.

Если допускается применение паролей условно-постоянного действия, пользователей следует ознакомить с правилами выбора и сохранения пароля в тайне, предварительной проверки качества пароля, управления сроком годности пароля. Следует задействовать программы подбора паролей.

6.3. Резервное копирование

Нет смысла лишний раз подчеркивать важность резервного копирования. Однако, резервное копирование может являться самым слабым звеном в системной безопасности, если защита резервных носителей не налажена должным образом.

При копировании по сети следует пользоваться защищенным каналом. Если в процессе резервного копирования данные помещаются на промежуточные диски, то доступ к этим дискам следует ограничить в максимально возможной степени.

После нарушения безопасности резервные копии приобретают дополнительное значение как носители данных для анализа.

Отслужившие срок носители должны уничтожаться, а не выбрасываться.

Пользователей систем и услуг следует информировать о том, что сохраняется на резервных копиях, а что нет. Более того, если пользователю сообщили, что определенные данные не сохраняются, то их не следует копировать.

6.4. Распространение программного обеспечения

Поставщикам Интернет-услуг приходится часто распространять прикладное программное обеспечение. Целостность ПО должна гарантироваться путем вычисления и распространения вместе с ПО криптографических контрольных сумм, таких, например, как в алгоритме SHA-1 [SHA].

7. Доменная система имен

Доменная система имен (DNS) играет критически важную роль в повседневной деятельности миллионов пользователей Интернет. Прискорбно, что приложения зачастую слепо доверяют информации DNS, уверены в постоянной доступности DNS. Однако, до введения протокола DNSSEC [RFC2065], в DNS явно недоставало средств защиты, а реализации содержали серьезные слабости (см. [VIX1995]).

Хотя далее и предлагаются некоторые методы повышения защищенности и надежности DNS, хочется подчеркнуть, что аутентификация, основанная на именах, внутренне небезопасна.

Политика поставщика Интернет-услуг по отношению к защите персональных данных, обеспечению аутентичности, подотчетности, наложению защитных заплат, поддержке доступности, реагированию на доклады о нарушениях должна быть документирована и опубликована

7.1. Администрирование DNS-сервера

В дополнение к мерам, описанным в разделе 6, поставщикам Интернет-услуг при администрировании DNS-серверов следует обратить внимание еще на несколько аспектов:

- Мониторинг. Следует контролировать доступность DNS (способность отвечать на запросы).
- Синхронизация часов. Серверам следует синхронизировать часы с помощью протокола NTP (см. [RFC1305]) с аутентификацией. Следует использовать по крайней мере два NTP-сервера.

7.2. Надежная доменная система имен

Надежный сервер в смысле DNS обладает локальным знанием DNS-зоны, поэтому для ответов на запросы по этой зоне ему не нужно обращаться к другим серверам. Потребителям следует обдумать (см. [RFC2182]), на каких вторичных DNS-серверах остановить свой выбор.

Поставщики Интернет-услуг обычно выполняют для своих потребителей роль вторичных (подчиненных) серверов, и эти серверы могут обслуживать тысячи зон. Независимо от числа зон, администраторам серверов следует ознакомиться с документом «Operational Criteria for Root Name Servers» [RFC2010] как с отправной точкой на пути обеспечения высокой доступности службы имен. В частности, следует руководствоваться такими положениями:

- При обработке запросов следует запретить рекурсию.
- Передачу зон следует ограничить. Помимо значительной нагрузки, вызываемой передачей зон и увеличивающей риск атак на доступность, поставщикам Интернет-услуг следует учесть, что некоторые из потребителей считают свои файлы зон конфиденциальными.
- Производительность следует контролировать, отслеживая такие ключевые характеристики, как число запросов в секунду и средняя задержка.

7.3. Услуга DNS-разрешения

Как правило, поставщик Интернет-услуг предоставляет своим потребителям сервис DNS-разрешения. При этом потребители конфигурируют свои «DNS-разрешители» (клиенты) так, чтобы те обращались к серверам DNS-разрешения поставщика Интернет-услуг, которому следует руководствоваться такими положениями:

- При обработке запросов следует допускать рекурсию. Это значит, что поставщик Интернет-услуг не должен использовать один и тот же сервер для сервисов разрешения и надежного DNS.
- Передачу зон следует запретить. Хотя при нормальной работе зоны передавать и не придется, лучше лишний раз защититься от атак на доступность.
- Производительность следует контролировать, отслеживая такие ключевые характеристики, как число запросов в секунду и средняя задержка. Кроме того, следует периодически сообщать о хостах, генерирующих наибольшее число запросов.
- В программном обеспечении сервера имен не должно быть слабости, связанной с «отравлением» кэша, когда злоумышленные или ошибочные данные, полученные от удаленного сервера имен, кэшируются и становятся доступными для DNS-разрешения.

8. Почтовые услуги

Электронная почта стала целью ряда наиболее известных атак, а также тысяч детских шуток и шалостей.

Поставщики Интернет-услуг играют главную роль в защите общества от злоупотреблений, а также в обучении своих потребителей соответствующим методам обеспечения информационной безопасности.

8.1. Администрирование почтовых серверов

При конфигурировании почтовых серверов поставщикам Интернет-услуг следует руководствоваться такими положениями:

- Выбор программного обеспечения. По возможности следует использовать ПО с раздельными агентами приема/отправки и обработки. Идея состоит в том, чтобы агент приема/отправки, взаимодействующий с удаленными почтовыми

Критически важно, чтобы поставщики Интернет-услуг и, в частности, их группы реагирования на нарушения информационной безопасности, располагали средствами защищенного обмена сообщениями

Поставщики Интернет-услуг играют главную роль в защите общества от злоупотреблений, а также в обучении своих потребителей соответствующим методам обеспечения информационной безопасности

серверами, выполнялся с минимальными привилегиями.

- Ограничение удаленного запуска очередей сообщений. Запуск очередей по запросу (предоставляемый для удобства потребителей, получающих почту в своем домене и не имеющих постоянного соединения) должен быть ограничен, желательно средствами надежной аутентификации. Удаленный запуск очередей сообщений реализуется разными механизмами, такими, например, как ETRN — расширение SMTP-сервиса (см. [RFC1985]).
- Отключение VRFY and EXPN. Не следует предоставлять информацию о локальных пользователях или механизмах доставки, выходящую за рамки необходимого.
- Синхронизация часов. Серверам следует синхронизировать часы с помощью протокола NTP (см. [RFC1305]) с аутентификацией. Следует использовать по крайней мере два NTP-сервера.
- Информирование об исключительных ситуациях. Исключительные ситуации, такие как повторяющиеся неудачи аутентификации, зацикливание почты, ненормальная длина очереди, следует выявлять и генерировать соответствующие доклады.
- Ограничение доступа к регистрационной информации о почте. Регистрационная информация о работе почты должна быть доступна на чтение только системному администратору.

8.2. Защищенная почта

Как отмечалось в разделе 3.4, критически важно, чтобы поставщики Интернет-услуг и, в частности, их группы реагирования на нарушения информационной безопасности, располагали средствами защищенного обмена сообщениями.

8.3. Открытые системы промежуточного хранения и пересылки почты

Говорят, что почтовый SMTP-сервер функционирует в режиме «открытой» системы промежуточного хранения и пересылки почты, если он допускает прием и пересылку нелокальным адресатам таких сообщений, которые были порождены нелокально (иными словами, адреса как отправителя, так и получателя являются нелокальными). Такие открытые системы пересылки почты нередко используются «спамерами», организующими массовую незапрошенную рассылку с сокрытием инициатора. Только в весьма специфических обстоятельствах можно оправдать решение администратора сделать систему пересылки в Интернет полностью открытой.

Способы ограничения пересылки почты хорошо документированы. Весьма прискорбно, что некоторые крупные поставщики программного обеспечения поставляют свои агенты передачи сообщений с включенной по умолчанию опцией пересылки.

Безопасность электронной почты — забота общая, но поставщикам Интернет-услуг следует быть особенно бдительными, отключая функцию открытой пересылки на администрируемых ими серверах, поскольку доступная им широкая полоса пропускания делает их серверы особенно привлекательными в качестве плацдарма спамера.

Поставщикам Интернет-услуг следует настоятельно рекомендовать своим потребителям запретить открытую пересылку на «потребительских» почтовых серверах. Ситуации, в которых разрешена организация открытой пересылки почты, следует документировать в «Политике допустимого использования» поставщика Интернет-услуг.

8.4. Представление сообщений для отправки

Чтобы облегчить проведение в жизнь политики безопасности, представлять сообщения для отправки следует через порт MAIL SUBMIT (587), как это предлагается в проводимой в настоящее время работе «Message Submission and Relay», а не через SMTP-port (25). Кроме того, представление сообщения следует аутентифицировать с помощью расширения AUTH SMTP-сервиса (в соответствии с проводимой в настоящее время работой «SMTP Service Extension for Authentication»). При таком подходе функции SMTP-порта (25) могут быть ограничены локальной доставкой.

Перечисленные меры не только защищают поставщика Интернет-услуг от превращения в плацдарм спамера, но и позволяют поддерживать подотчетность представления сообщений в ситуациях, когда потребитель рассылает спам. Далее, использование порта MAIL SUBMIT в сочетании с функцией SMTP AUTH имеет еще и то преимущество перед ограничениями по IP-адресам на представление сообщений, что оно дает потребителям дополнительную гибкость, позволяя представлять

сообщения, даже если они подключились не через сеть своего обычного поставщика Интернет-услуг (например, при отправке письма с работы). Кроме того, обеспечивается большая устойчивость к подделке IP-адресов и сохраняется возможность модернизации механизмов аутентификации при появлении новых мощных средств.

Заслуживает внимания и (недокументированное) расширение XTND XMIT POP3, позволяющее клиентам отправлять почту в рамках сеанса POP3, а не по протоколу SMTP. При этом обеспечивается поддержка мобильных пользователей при отключенной функции открытой пересылки, предоставляется аутентифицированное, протоколируемое соединение.

Политика поставщика Интернет-услуг по отношению к защите персональных данных, обеспечению аутентичности, подотчетности, наложению защитных заплат, поддержке доступности, реагированию на доклады о нарушениях должна быть документирована и опубликована

8.5. Сервисы POP и IMAP

Поставщикам Интернет-услуг, представляющим своим потребителям доступ к почтовым ящикам по протоколам POP или IMAP, следует, как минимум, поддерживать механизмы аутентификации CRAM-MD5 [RFC2195] или APOP [RFC1939]. Следует рассмотреть возможность использования более сильной аутентификации, равно как и запрет на аутентификацию на основе передаваемых в открытом виде имен и паролей.

9. Телеконференции (NNTP)

Как и SMTP, протокол NNTP [RFC977], используемый в телеконференциях, страдает от недостаточной аутентификации, поэтому подделка сообщения не составляет труда. Злоумышленник может обойти процесс модерирования, удалить легальное сообщение и опустошить серверы, поддерживающие активные файлы.

Недостаток средств шифрования в протоколе, а также укоренившиеся способы администрирования многих серверов телеконференций создают проблемы с защитой персональной тайны, поскольку позволяют выяснить постороннему, какие группы и статьи Вы читаете.

9.1. Администрирование серверов телеконференций

При конфигурировании серверов телеконференций поставщикам Интернет-услуг следует руководствоваться такими положениями:

- Выбор программного обеспечения. Следует использовать ПО, устойчивое к вредоносным управляющим сообщениям и к переполнению буферов.
- Отключение других сервисов. Зная склонность телеконференций потреблять все доступное дисковое пространство и вычислительные ресурсы, следует освободить сервер телеконференций от выполнения каких-либо иных функций.
- Отказ от интерпретации пакетов. Если поддерживаются входящие пакеты статей, эти пакеты не следует подавать на вход командного интерпретатора.
- Ограничение доступа к регистрационной информации о телеконференциях. Регистрационная информация о работе телеконференций должна быть доступна на чтение только системному администратору.
- Аутентификация принятых сообщений. Желательно обеспечивать криптографическую аутентификацию принятых сообщений, особенно если эти сообщения — управляющие.

9.2. Представление статей

Поскольку многие проблемы открытых систем пересылки почты (см. выше раздел 8.3) имеют место и для телеконференций, поставщикам Интернет-услуг следует ограничить круг тех, кто имеет право представлять статьи, включив в него только допущенных потребителей. Кроме того, следует в максимально возможной степени ограничить множество сетей (и телеконференций), из (и для) которых принимаются статьи.

9.3. Управляющие сообщения

Управляющие сообщения пытаются заставить сервер телеконференций выполнить действия, выходящие за рамки размещения и распространения статей. Отдельные управляющие сообщения, особенно учитывая легкость, с которой их могут подделать, следует обрабатывать с осторожностью. Хотя выполнение запрошенных действий оставляется на усмотрение поставщика Интернет-услуг, он должен, по крайней мере, распространить сообщения, даже если он их не понимает. Целесообразно придерживаться таких правил:

- Запросы «whogets», «sendsys», «version» следует игнорировать.

- Сообщения 'cancel' должны выполняться и распространяться, хотя их наплыв может порой «смыть» сервис, а факт явно компьютерной генерации таких сообщений является настораживающим.
- В системах, требующих поддержки активных файлов, следует проявлять чрезвычайную осторожность при решении вопроса о том, какие сообщения управления группами (checkgroups, newgroup, rmgroup) принимать к исполнению.

9.4. Фильтрация статей

Наиболее очевидной формой нарушения информационной безопасности телеконференций является «утечка» статей, не предназначенных для широкого распространения. Алгоритм затопления — замечательное средство выявления путей, по которым статьи могут покидать подсеть с вроде бы контролируемыми границами. От администратора требуются значительные усилия, чтобы локальные телеконференции на самом деле оставались локальными (см. [SPE1994]).

Поставщикам Интернет-услуг, предоставляющим своим потребителям возможность удаленного манипулирования входными фильтрами, следует использовать для подобных действий надежную аутентификацию.

Поставщикам Интернет-услуг не следует распространять статьи, поступающие из слишком многих источников. Обычно величина в 10 источников считается чрезмерной.

Поставщикам Интернет-услуг следует установить верхнюю границу на размер распространяемых сообщений.

10. Услуги размещения Web-серверов

Многие организации передают свои Web-серверы поставщикам Интернет-услуг вместе с обязанностями по эксплуатации и администрированию. Главную роль при принятии такого решения играют соображения информационной безопасности. Тема данного раздела — размещение Web-серверов и сопутствующие услуги. Более детальную информацию можно найти в работах [GAR1997] и [HUG1995].

10.1. Администрирование сервера с размещенными Web-серверами

Помимо аспектов, описанных в разделе 6, поставщикам Интернет-услуг при администрировании сервера с размещенными Web-серверами следует руководствоваться такими положениями:

Поставщики Интернет-услуг играют главную роль в защите общества от злоупотреблений, а также в обучении своих потребителей соответствующим методам обеспечения информационной безопасности

- Постоянный мониторинг. Следует контролировать доступность сервиса (способность отвечать на HTTP-запросы).
- Синхронизация часов. Серверам следует синхронизировать часы с помощью протокола NTP (см. [RFC1305]) с аутентификацией. Следует использовать по крайней мере два NTP-сервера.
- Разумное использование DNS. В момент подключения клиента не следует выполнять поиск его имени, поскольку это делает Web-серверы уязвимыми для атак на доступность и заметно сказывается на производительности.
- Минимизация привилегий. Web-демон следует выполнять от имени пользователя и группы, специально выделенных для этой цели и имеющих минимальные привилегии. Ответственный за информационное наполнение Web-сервера должен работать от имени другого пользователя.
- Контроль DocumentRoot. Все, что располагается ниже этого каталога, следует тщательнейшим образом проконтролировать. Желательно использовать системный вызов chroot для смены корневого каталога HTTP-демона.
- Контроль UserDir. На сервере не следует иметь других пользователей, кроме администраторов. Если такие пользователи все-таки есть, директиве «UserDir» (если она разрешена) не следует предоставлять доступ к информации пользователей. В частности, не следует разрешать выполнение командных процедур от имени этих пользователей.
- Разбиение на виртуальные серверы. Единый сервер, на котором размещено множество серверов (виртуальных доменов), СЛЕДУЕТ организовать так, чтобы все данные, программы и регистрационные журналы различных виртуальных серверов были отделены друг от друга и чтобы доступ к «чужой» конфигурации или данным был невозможен. Кроме того, следует исключить доступ к данным или программам на сервере одного потребителя через локатор ресурсов, в хостовой части которого указано имя сервера другого потребителя.

- Управление доступом. Следует сделать возможным разграничение доступа к определенным частям сервера на основе механизмов надежной аутентификации, таких как сертификаты или одноразовые пароли. Другим возможным вариантом является применение хорошо выбранных паролей в сочетании с протоколом SSL, который по крайней мере исключает передачу паролей по сети в открытом виде.

Программы на серверной стороне, поддерживающие CGI или какой-либо другой интерфейс, важны для гибкости web как коммуникационной среды. Однако эта гибкость достигается ценой появления угроз безопасности, а слабая программа может сделать уязвимыми все виртуальные серверы

- Установка заплат и сервисных дополнений. Эксплуатация Web-сервера — деятельность особо ответственная, поэтому администраторам следует быть особенно аккуратными в установке заплат и сервисных дополнений по мере их появления.

10.2. Программы на серверной стороне

Программы на серверной стороне, поддерживающие CGI или какой-либо другой интерфейс, важны для гибкости web как коммуникационной среды. Однако, эта гибкость достигается ценой появления угроз безопасности, а слабая программа может сделать уязвимыми все виртуальные домены на сервере. Политика поставщика Интернет-услуг при разделении программ на допустимые и недопустимые является показательным аспектом всей его политики безопасности.

Поставщику Интернет-услуг следует руководствоваться такими положениями:

- Политика безопасности. Поставщику Интернет-услуг следует выработать для своих потребителей ясную методику написания безопасных программ в имеющейся среде размещения Web-серверов и отдельно описать приемы программирования, при применении которых программы будут отвергаться.
- Установка программ. Потребителям не следует разрешать устанавливать собственные программы. Все программы и командные процедуры следует передавать поставщику Интернет-услуг для первоначальной проверки на соответствие политике безопасности. Программы СЛЕДУЕТ устанавливать так, чтобы только администратор сервера мог их модифицировать.
- Выбор пользователя и группы процесса. Программы следует выполнять от имени пользователя и группы, специально выбранных для этой цели и имеющих минимальные привилегии (часто используют «nobody»).
- Отображение в навигаторах. Ни при каких обстоятельствах НЕ СЛЕДУЕТ допускать отображения программ в навигаторах. Следствие: программы НЕ СЛЕДУЕТ размещать под DocumentRoot.
- Разделение виртуальных серверов. Программы НЕ СЛЕДУЕТ делать доступными через сервер другого потребителя или для Web-мастера другого потребителя.
- Обработка пользовательского ввода. В пользовательском вводе НЕ СЛЕДУЕТ вычислять выражения, если нет механизма изоляции небезопасных действий (как, например, в Perl).
- Лимитирование потребления ресурсов. Для всех программ СЛЕДУЕТ ввести лимит потребляемого астрономического и процессорного времени, а также дискового пространства.
- Маршрутные имена. Все маршрутные имена СЛЕДУЕТ делать абсолютными или начинающимися с DocumentRoot. Переменную PATH следует устанавливать системному администратору.

10.3. Данные и базы данных

Данные, которые пишет программа серверной стороны, следует считать конфиденциальными. Чтобы сделать невозможным доступ к таким данным через навигаторы, права следует устанавливать так, чтобы у Web-демона не было права на чтение этих данных.

Если через Web-сервер предоставляется доступ к базам данных, то программам, осуществляющим такой доступ, следует выделить только те полномочия, которые абсолютно необходимы для их функционирования.

Данные, относящиеся к управлению состояниями (идентифицирующие цепочки — cookies), следует считать конфиденциальными. Следует исключить возможность доступа к ним из навигаторов.

10.4. Обработка регистрационной и статистической информации

Регистрационная информация, генерируемая Web-демоном, может быть полезна с точки зрения информационной безопасности, поскольку в ней содержатся сведения об операциях, выполнявшихся сервером. Чаще, однако, эту информа-

цию используют для выставления счетов, а также для маркетингового анализа или улучшения информационного наполнения.

Регистрационную информацию следует считать весьма конфиденциальной. Для реализации этого положения:

- Поставщику Интернет-услуг следует разрешить выполнение лишь необходимых операций с регистрационной информацией — генерацию счетов и периодическую ротацию.
- Регистрационную информацию следует хранить вне дерева с корнем в DocumentRoot, чтобы исключить возможность доступа через навигаторы.
- Регистрационную информацию в первоначальном или обработанном виде следует передавать потребителю только по защищенному каналу.

10.5. Услуги принудительной или потоковой передачи

Нередко поставщики Интернет-услуг дают своим потребителям возможность доставлять информацию с помощью протоколов, отличных от HTTP. При наличии подобных дополнительных услуг и поставщику-Интернет-услуг, и потребителям следует осознать их воздействие на информационную безопасность.

10.6. Электронная коммерция

Многие поставщики Интернет-услуг предоставляют своим потребителям средства для продажи товаров или услуг через размещенные у поставщика Web-серверы. И хотя сервер, способный обмениваться информацией с навигатором по протоколу SSL, иногда называют «защищенным», этот термин в данном случае нельзя понимать буквально. Поставщику Интернет-услуг, разместившему у себя приложения электронной коммерции, следует руководствоваться такими положениями:

- Шифрование транзакций. Транзакции ни в коем случае не следует хранить на сервере в открытом виде. Может использоваться криптография с открытыми ключами, так что только потребитель сможет расшифровать транзакции. Отметим, что даже если транзакции передаются напрямую в финансовое учреждение или потребителю, поставщик Интернет-услуг может сохранять у себя какую-то часть данных для обеспечения подотчетности.
- Передача транзакций. Если транзакции не обрабатываются немедленно, а передаются потребителю пакетами, то передачу следует производить по защищенному (например, средствами SSL) каналу и только после проведения надежной аутентификации. Следует аккуратно производить ротацию транзакционных файлов, чтобы каждая транзакция выполнялась ровно один раз.
- Резервное копирование. Если транзакции записываются на резервные носители, следует гарантировать физическую безопасность этих носителей.

Регистрационную информацию следует считать весьма конфиденциальной

10.7. Загрузка информационного наполнения и распределенное авторство

Загрузку информационного наполнения на сервер поставщика Интернет-услуг следует производить по защищенному каналу.

Если сервер поддерживает средства для распределенного авторства, их следует администрировать с особой осторожностью, гарантируя, что имеет место надежная аутентификация, что доступ предоставляется только к виртуальному серверу потребителя и только для лиц, управляющих информационным наполнением.

10.8. Поисковые машины и другие средства

Поставщики Интернет-услуг нередко предоставляют для использования потребителями поисковые машины, средства контроля целостности ссылок и т.д. Зачастую такие средства создают весьма существенную дополнительную нагрузку, поэтому их запуск по запросу следует запретить, чтобы защититься от атак на доступность.

Поисковые машины следует сконфигурировать так, чтобы поиск ограничивался частями Web-сервера, доступными всем.

Результат проверки целостности ссылок следует считать конфиденциальным. Доступ к нему следует предоставить только лицу, управляющему информационным наполнением.

11. Литература

[CA-91:18.Active.Internet.tftp.Attacks] Active Internet tftp Attacks. — ftp://info.cert.org/pub/certadvisories/.

[CA-95.01.IP.spoofing] IP Spoofing Attacks and Hijacked Terminal Connections. — ftp://info.cert.org/pub/certadvisories/.

[CA-96.21.tcpsynflooding] TCP SYN Flooding and IP Spoofing Attacks. — ftp://info.cert.org/pub/certadvisories/.

[CA-97.28.TeardropLand] IP Denial-of-Service Attacks. — ftp://info.cert.org/pub/certadvisories/.

[DPR1998] The UK Data Protection Act 1998 (c. 29). — http://www.hmso.gov.uk/acts/acts1998/19980029.htm.

[GAR1997] Garfinkel S. Web Security and Commerce. — O'Reilly and Associates, Sebastopol, CA, 1997.

[HUG1995] Hughes Jr., L. Actually Useful Internet Security Techniques. — New Riders Publishing, Indianapolis, IN, 1995.

[RFC977] Kantor B. Lapsley P. Network News Transfer Protocol. — RFC 977, February 1986. http://www.rfc-editor.org/rfc/rfc977.txt.

[RFC1034] Mockapetris P.V. Domain names — concepts and facilities. — STD 13, RFC 1034, November 1987. http://www.rfc-editor.org/rfc/rfc1034.txt.

[RFC1035] Mockapetris P.V. Domain names — implementation and specification. — STD 13, RFC 1035, November 1987. http://www.rfc-editor.org/rfc/rfc1035.txt.

[RFC1305] Mills D. Network Time Protocol (Version 3) Specification, Implementation. — RFC 1305, March 1992. http://www.rfc-editor.org/rfc/rfc1305.txt.

[RFC1350] Sollins K.R. The TFTP Protocol (revision 2). — STD 33, RFC 1350, July 1992. http://www.rfc-editor.org/rfc/rfc1350.txt.

[RFC1786] Bates T., Gerich E., Joncheray L., Jouanigot J-M., Karrenberg D., Terpstra M., Yu J. Representation of IP Routing Policies in a Routing Registry (ripe-81++). — RFC 1786, March 1995. http://www.rfc-editor.org/rfc/rfc1786.txt.

[RFC1834] Gargano J., Weiss K. Whois and Network Information Lookup Service. — RFC 1834, August 1995. http://www.rfc-editor.org/rfc/rfc1834.txt.

[RFC1835] Deutsch P., Schoultz R., Faltstrom P., Weider C. Architecture of the WHOIS++ service. — RFC 1835, August 1995. http://www.rfc-editor.org/rfc/rfc1835.txt.

[RFC1918] Rekhter Y., Moskowitz B., Karrenberg D., de Groot G.J., Lear E. Address Allocation for Private Internets. — BCP 5, RFC 1918, February 1996. http://www.rfc-editor.org/rfc/rfc1918.txt.

[RFC1939] Myers J., Rose M. Post Office Protocol. Version 3. — RFC 1939, May 1996. http://www.rfc-editor.org/rfc/rfc1939.txt.

[RFC1985] De Winter, J. SMTP Service Extension for Remote Message Queue Starting. — RFC 1985, August 1996. http://www.rfc-editor.org/rfc/rfc1985.txt.

[RFC2010] Manning B., Vixie P. Operational Criteria for Root Name Servers. — RFC 2010, October 1996. http://www.rfc-editor.org/rfc/rfc2010.txt.

[RFC2065] Eastlake 3rd D., Kaufman C. Domain Name System Security Extensions. — RFC 2065, January 1997. http://www.rfc-editor.org/rfc/rfc2065.txt.

[RFC2119] Bradner S. Key words for use in RFCs to Indicate Requirement Levels. — RFC 2119, March 1997. http://www.rfc-editor.org/rfc/rfc2119.txt.

[RFC2142] Crocker D. Mailbox Names for Common Services, Roles and Functions. — RFC 2142, May 1997. http://www.rfc-editor.org/rfc/rfc2142.txt.

[RFC2182] Elz R., Bush R., Bradner S., Patton M. Selection and Operation of Secondary DNS Servers. — RFC 2182, July 1997. http://www.rfc-editor.org/rfc/rfc2182.txt.

[RFC2195] Klensin J., Catoe R., Krumviede P. IMAP/POP AUTHorize Extension for Simple Challenge/Response. — RFC 2195, September 1997. http://www.rfc-editor.org/rfc/rfc2195.txt.

[RFC2196] Fraser B. Site Security Handbook. — RFC 2196, September 1997. http://www.rfc-editor.org/rfc/rfc2196.txt.

[RFC2267] Ferguson P., Senie D. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. — RFC 2267, January 1998. http://www.rfc-editor.org/rfc/rfc2267.txt.

[RFC2350] Brownlee N., Guttman E. Expectations for Computer Security Incident Response. — RFC 2350, June 1998. http://www.rfc-editor.org/rfc/rfc2350.txt.

[RFC2644] Senie D. Changing the Default for Directed Broadcasts in Routers. — RFC 2644, August 1999. http://www.rfc-editor.org/rfc/rfc2644.txt.

[SHA] Secure Hash Standard. — NIST, FIPS PUB 180-1, April 1995.

[SPE1994] Spencer H. News Article Format and Transmission. — ftp://ftp.zoo.toronto.edu/pub/news.txt.Z.

[SSH1997] SSH (secure Shell) Remote Login Program. — http://www.cs.hut.fi/ssh/.

[VIX1995] Vixie P. DNS and BIND Security Issues. — ftp://ftp.vix.com/pri/vixie/ bindsec.psf, 1995.

12. Контактная информация

Tristan Debeaupuis Herve Schauer Consultants
142, rue de Rivoli 75001 Paris France

Phone: +33 141 409 700

Email: Tristan.Debeaupuis@hsc.fr

13. Приложение 1. Вопросник

13.1. Вопросы, которые целесообразно выяснить потребителям услуг подключения к Интернет

13.1.1. Политики

Есть ли у поставщика Интернет-услуг документированная политика безопасности?

Если есть, то как с ней можно ознакомиться?

Есть ли у поставщика Интернет-услуг документированная политика добропорядочного пользования?

Если есть, то как с ней можно ознакомиться?

Если у поставщика Интернет-услуг есть документированная политика добропорядочного пользования, то каковы санкции за ненадлежащее поведение?

Если у поставщика Интернет-услуг есть документированная политика добропорядочного пользования, то уведомляет ли он потребителей об изменениях в политике, и если уведомляет, то каким образом?

13.1.2. Реагирование на нарушения информационной безопасности

Есть ли у поставщика Интернет-услуг группа реагирования на нарушения информационной безопасности?

Если есть, то:

- Какие у нее права, правила работы и предоставляемые услуги?
- Какова цепочка эскалации докладов, которой должен следовать потребитель?
- Опубликована ли информация о группе где-либо (например, в Web)?
- Какова стоимость использования различных услуг группы реагирования?

Если группы реагирования нет, то:

- Какую роль играет поставщик Интернет-услуг в реагировании на нарушения информационной безопасности?
- Есть ли какая-нибудь группа реагирования, к которой потребитель может обратиться?

Имеются ли у поставщика Интернет-услуг еще какие-либо ресурсы в области информационной безопасности?

Если имеются, то сколько они стоят?

Оказывает ли поставщик Интернет-услуг какие-либо дополнительные услуги в области информационной безопасности?

Если оказывает, то сколько они стоят?

Информирует ли поставщик Интернет-услуг своих потребителей об атаках против них?

Оказывает ли поставщик Интернет-услуг помощь в прослеживании источника атаки?

Осуществляет ли поставщик Интернет-услуг сбор и сохранение улик нарушения информационной безопасности?

Защищает ли поставщик Интернет-услуг от уничтожения подобных улик?

Защищает ли поставщик Интернет-услуг от непреднамеренного разглашения сведений о нарушениях информационной безопасности?

Какую информацию сообщает поставщик Интернет-услуг своим потребителям при обнаружении слабостей в предоставляемых им сервисах?

Информирует ли поставщик Интернет-услуг своих потребителей заранее или только после нарушений безопасности?

Как и когда информация о слабостях передается потребителям?

Какие сведения включаются в доклады о слабостях?

К кому может обратиться потребитель по электронной почте для прояснения вопросов информационной безопасности?

К кому может обратиться потребитель по электронной почте для доклада о ненадлежащем поведении сторонних пользователей?

К кому может обратиться потребитель по электронной почте для прояснения вопросов работы сетевой инфраструктуры?

Каков график работы службы поддержки потребителей и службы эксплуатации?

Если в нерабочее время предоставляется ограниченная поддержка потребителей, куда обращаться в случае нарушения информационной безопасности?

Как организованы коммуникации между поставщиком Интернет-услуг и потребителями, если, по-видимому, имеет место нарушение информационной безопасности?

Какая информация сообщается сторонним организациям и лицам?

13.1.3. Сетевая защита

Какие меры принимает поставщик Интернет-услуг, чтобы не допустить несанкционированной маршрутизации потоков данных в свою сеть или через нее?

Разделены на сегменты сети, поддерживающие потребителей услуг подключения и услуг размещения серверов?

Какие общие меры применяет поставщик Интернет-услуг для защиты производственных сервисов, предоставляемых по Интернет потребителями, от атак на доступность, вторжений, подделок?

13.1.4. Защитные заплаты

Насколько быстро поставщик Интернет-услуг накладывает защитные заплаты на программное и микропрограммное обеспечение, функционирующее на производственном оборудовании?

13.1.5. Другие услуги в области безопасности

Сканируются ли поставщиком Интернет-услуг порты в сетях потребителей и сообщается ли им о найденных аномалиях?

Если сканируются, то сколько стоит такая услуга?

Предоставляется дополнительная услуга по аудиту безопасности и усиления защиты систем потребителей?

Если предоставляется, то сколько она стоит?

Есть ли у поставщика Интернет-услуг система активного аудита, обнаруживающая в реальном времени сетевые и системные атаки?

Возможна ли проверка защищенности поставщика Интернет-услуг путем отслеживания хода тестовой атаки во взаимно согласованное время?

13.1.6. Ссылки

Предоставляет ли поставщик Интернет-услуг список избранных потребителей?

13.2. Вопросы, которые целесообразно выяснить потребителям услуг размещения серверов

13.2.1. Политика добропорядочного пользования

Какова политика добропорядочного пользования для информационного наполнения Web-сервера, размещенного у поставщика Интернет-услуг?

13.2.2. Физическая защита

Как организована физическая защита оборудования, использующегося для размещения серверов потребителей?

13.2.3. Резервное копирование

Как часто производится резервное копирование информационного наполнения Web-серверов?

Как часто резервные носители передаются на внешнее хранение?

13.2.4. Выделение полосы пропускания

Осуществляет ли поставщик Интернет-услуг балансировку нагрузки, чтобы предотвратить насыщение сети трафиком других других потребителей?

13.2.5. Резервное оборудование

Какое резервное оборудование может быть использовано в случае поломок?

Как быстро оно может быть развернуто?

13.2.6. Управление информационной безопасностью

Предоставляет ли поставщик услуги по управлению информационной безопасностью потребителей?

13.2.7. Управление информационным наполнением

Какие виды доступа предоставляются для управления информационным наполнением размещенных у поставщика серверов?

Какие виды информационного наполнения разрешается размещать у поставщика?

13.2.8. Защищенные Web-серверы

Предоставляет ли поставщик Интернет-услуг защищенные Web-серверы (https)?

Если предоставляет, то каков сертификат хоста, поддерживаемый известным доверенным центром?

Достаточно ли отделено информационное наполнение защищенного Web-сервера от наполнения других серверов?

Закрыт ли доступ к информационному наполнению защищенного Web-сервера для других потребителей?

Как передавать информационное наполнение на защищенный Web-сервер?

13.3. Вопросы, которые целесообразно выяснить потребителям, разделяющим площади с поставщиком Интернет-услуг

13.3.1. Политика добропорядочного пользования

Какова политика добропорядочного пользования для потребителей, разделяющих площади с поставщиком Интернет-услуг?

13.3.2. Физическая защита

Как организована физическая защита оборудования потребителей, размещенного на площадях поставщика Интернет-услуг?

Как контролируются посетители совместно используемых площадей?

13.3.3. Безопасность электропитания

Как обеспечена разводка по сети питания для оборудования разных потребителей, размещенного на общих площадях?

13.3.4. Сетевая безопасность

Как обеспечено сетевое разделение для оборудования разных потребителей, размещенного на общих площадях?

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Галатенко В.А. *(galat@jet.msk.su)*
Технический редактор: Антонов А.Н. *(silver@jet.msk.su)*
Россия, 103006, Москва, Краснопролетарская, 6
тел. (095) 972 11 82, 972 13 32
факс (095) 972 07 91
e-mail: JetInfo@jet.msk.su, http://www.jetinfo.ru
Подписной индекс по каталогу Роспечати 32555