27. Обеспечение безопасности электронной почты

Использование электронной почты

Электронная почта, или e-mail, — самый популярный вид использования Интернета. С помощью электронной почты в Интернете вы можете послать письмо миллионам людей по всей планете. Существуют шлюзы частных почтовых систем в интернетовский e-mail, что значительно расширяет ее возможности.

Помимо взаимодействия «один-один» e-mail может поддерживать списки электронных адресов для рассылки, поэтому человек или организация может послать e-mail всему этому списку адресов людей или организаций.

Иногда списки рассылки e-mail имеют элементы, являющиеся указателями на другие списки рассылки, поэтому одно письмо может быть в конце концов доставлено тысячам людей.

Разновидностью списков рассылки являются дискуссионные группы на основе e-mail.

Их участники посылают письмо центральному серверу списка рассылки, и сообщения рассылаются всем другим членам группы. Это позволяет людям, находящимся в разных временных зонах или на разных континентах, вести интересные дискуссии.

При помощи специальных программ люди могут подписаться на список или отписаться от него без помощи человека. Серверы списков рассылки часто предоставляют другие сервисы, такие как получение архивов, дайджестов сообщений или связанных с сообщениями файлов. Группы новостей USENET являются усовершенствованием дискуссионных почтовых групп.

Электронная почта становится все более важным условием ведения повседневной деятельности. Организациям нужны политики для электронной почты, чтобы помочь сотрудникам правильно ее использовать, уменьшить риск умышленного или неумышленного неправильного ее использования, и чтобы гарантировать, что официальные документы, передаваемые с помощью электронной почты, правильно обрабатываются. Организациям нужно разработать политику для правильного использования электронной почты, такую же как для телефона.

Политика должна давать общие рекомендации в следующих областях:

- использование электронной почты для ведения деловой деятельности;
- использование электронной почты для ведения личных дел;
- управление доступом и сохранение конфиденциальности сообщений;
- администрирование и хранение электронных писем.

Основы e-mail

Основными почтовыми протоколами в Интернете (не считая частных протоколов, шлюзуемых или туннелируемых через Интернет) являются SMTP (Simple Mail Transport Protocol), POP (Post Office Protocol) и IMAP (Internet Mail Access Protocol).

- **SMTP**

SMTP — это почтовый протокол хост-хост. SMTP-сервер принимает письма от других систем и сохраняет их в почтовых ящиках пользователей. Сохраненные письма могут быть прочитаны несколькими способами.

Пользователи с интерактивным доступом на почтовом сервере могут читать почту с помощью локальных почтовых приложений. Пользователи на других системах могут загрузить свои письма с помощью программ-почтовых клиентов по протоколам POP3 и IMAP.

UNIX-хосты сделали самым популярным SMTP. Широко используемыми SMTP-серверами являются Sendmail, Smail, MMDF и PP. Самым популярным SMTP-сервером в Unixe является Sendmail, написанный Брайаном Эллманом. Он поддерживает создание очередей сообщений, переписывание заголовков писем, алиасы, списки рассылки и т.д.

Обычно он конфигурируется так, что должен работать как привилегированный процесс. Это означает, что, если его защиту можно будет обойти каким-нибудь способом, атакующий сможет нанести вред, далеко превышающий удаление электронных писем.

• **POP**

POP — это самый популярный протокол приема электронной почты. POP-сервер позволяет POP-клиенту загрузить письма, которые были получены им от другого почтового сервера. Клиенты могут загрузить все сообщения или только те, которые они еще не читали.

Он не поддерживает удаление сообщений перед загрузкой на основе атрибутов сообщения, таких как адрес отправителя или получателя. POP версии 2 поддерживает аутентификацию пользователя с помощью пароля, но пароль передается серверу в открытом (незашифрованном) виде.

POP версии 3 предоставляет дополнительный метод аутентификации, называемый APOP, который прячет пароль. Некоторые реализации POP могут использовать Kerberos для аутентификации.

• **IMAP**

IMAP — это самый новый, и наименее популярный протокол чтения электронной почты.

Как сказано в RFC: IMAP4rev1 поддерживает операции создания, удаления, переименования почтовых ящиков, проверки поступления новых писем; оперативное удаление писем; установку и сброс флагов операций; разбор заголовков в формате RFC-1822 и MIME-IMB; поиск среди писем; выборочное чтение писем.

IMAP более удобен для чтения почты в путешествии, чем POP, так как сообщения могут быть оставлены на сервере, что избавляет от необходимости синхронизировать списки прочитанных писем на локальном хосте и на сервере.

• **MIME**

MIME — это сокращение для Многоцелевых расширений интернетовской почты (Multipurpose Internet Mail Extensions). Как сказано в RFC 2045, он переопределяет формат сообщений электронной почты, чтобы позволить:

• передачу текстов в кодировке, отличной от US-ASCII,
• передачу в письме нетекстовой информации в различных форматах,
• сообщения из нескольких частей, и
• передачу в заголовке письма информации в кодировке, отличной от US-ASCII.

Он может использоваться для поддержки таких средств безопасности, как цифровые подписи и шифрованные сообщения. Он также позволяет посылать по почте выполняемые файлы, зараженные вирусами, или письма с РПС.

Как и веб-браузеры, программы чтения почты могут быть сконфигурированы автоматически запускать приложения-помощники для обработки определенных типов MIME-сообщений.

Потенциальные проблемы с электронной почтой

1. Случайные ошибки.

Можно легко допустить ошибку при работе с электронной почтой. Письмо может быть послано случайно. Простое нажатие клавиши или щелчок мышкой могут послать письмо по неправильному адресу. Почтовые сообщения могут храниться годами, поэтому плохое выражение может аукнуться через много времени. Архивы писем могут возрасти до такой степени, что система будет аварийно завершаться.

Неправильно настроенная программа чтения групп новостей может привести к посылке сообщения не в те группы. Ошибки в списках рассылки могут привести к долгому блужданию писем между почтовыми серверами, причем число писем может увеличиться до такой степени, что почтовые серверы аварийно завершатся.

Если почтовая система организации присоединена к Интернету, последствия ошибок могут привести к тяжелым последствиям. Вот некоторые из способов предотвратить ошибки:

- учить пользователей что делать, если они совершили ошибку, и как правильно работать с электронной почтой
- конфигурировать программы электронной почты так, чтобы стандартные действия пользователя, использующие установки по умолчанию, были бы самыми безопасными

- использовать программы, которые строго реализуют протоколы и соглашения Интернета. Каждый раз, когда онлайновый сервис шлюзует письмо из частной почтовой системы в интернетовскую электронную почту, слышатся вопли протеста из-за появления большого числа сообщений с ошибками, возникшими в результате неправильных настроек почтовых серверов этого сервиса.

2. *Персональное использование.*

Так как письма обычно используются для обеспечения деятельности организации, как и телефон и факс, использование его в личных целях должно быть ограничено или запрещено (это зависит от организации).

Хотя проще всего определить, что электронная почта используется только для решения задач организации, все понимают, что эту политику тяжело претворить в жизнь. Мудрее будет установить четкие границы использования e-mail в личных целях.

Если вы используете служебный телефон для того, чтобы позвонить в химчистку, то маловероятно, что ваш звонок будет восприниматься как официальный запрос компании. Но посылка электронного письма с электронным почтовым адресом, содержащим адрес организации, будет похожа на посылку бумажного письма на фирменном бланке компании. Если отправитель использует свой логин в компании для посылки электронной почты в группу новостей, может показаться, что компания одобряет мнение, высказываемое им в письме.

3. *Маркетинг.*

В прошлом, когда Интернет был исследовательской сетью, ее коммерческое использование было запрещено. Кроме того, слишком мало компаний и людей имели доступ к интернетовской почте, поэтому было нецелесообразно использовать ее для коммерческих целей.

Сейчас Интернет расширился и разрешается использовать его в коммерческих целях, поэтому компании стали поддерживать списки рассылки для обмена информацией со своими клиентами. Как правило, клиенты должны послать запрос для того, чтобы попасть в список рассылки.

Когда большие онлайновые сервисы стали шлюзовать письма в Интернет, неожиданно обнаружилось, что таким образом можно передать информацию гораздо большей аудитории. Так родился маркетинг в Интернете с помощью посылки отдельных почтовых сообщений.

Люди написали программы для автоматизации поддержания списков рассылки и образовали компании для сбора и продажи списков электронных почтовых адресов организациям, занимающимся маркетингом.

Конгресс США принял билль, согласно которому прямой маркетинг с помощью электронной почты должен осуществляться в соответствии с теми же правилами, которыми ограничивается использование массовой посылки писем, чтобы лица, занимающиеся таким маркетингом, вели списки адресов, владельцы которых не желают получать рекламу в электронных письмах.

Угрозы, связанные с электронной почтой

Основные протоколы передачи почты (SMTP, POP3, IMAP4) обычно не осуществляют надежной аутентификации, что позволяет легко создать письма с фальшивыми адресами. Ни один из этих протоколов не использует криптографию, которая могла бы гарантировать конфиденциальность электронных писем.

Хотя существуют расширения этих протоколов, решение использовать их должно быть явно принято, как составная часть политики администрации почтового сервера. Некоторые такие расширения используют уже имеющиеся средства аутентификации, а другие позволяют клиенту и серверу согласовать тип аутентификации, который будет использоваться в данном соединении.

Фальшивые адреса отправителя. Адресу отправителя в электронной почте Интернета нельзя доверять, так как или отправитель может указать фальшивый обратный адрес, или заголовок может быть модифицирован в ходе передачи письма, или отправитель может сам

соединиться с SMTP-портом на машине, от имени которой он хочет отправить письмо, и ввести текст письма.

Перехват письма. Заголовки и содержимое электронных писем передаются в чистом виде. В результате содержимое сообщения может быть прочитано или изменено в процессе передачи его по Интернету. Заголовок может быть модифицирован, чтобы скрыть или изменить отправителя, или для того чтобы перенаправить сообщение.

Почтовые бомбы. Почтовая бомба - это атака с помощью электронной почты. Атакуемая система переполняется письмами до тех пор, пока она не выйдет из строя. Как это может случиться, зависит от типа почтового сервера и от того, как он сконфигурирован.

Угрожающие письма. Так как любой человек в мире может послать вам письмо, может оказаться трудным заставить его прекратить посылать их вам. Люди могут узнать ваш адрес из списка адресов организации, списка лиц, подписавшихся на список рассылки, или писем в Usenet. Если вы указали ваш почтовый адрес какому-нибудь веб-сайту, то он может продать ваш адрес "почтовым мусорщикам".

Некоторые веб-браузеры сами указывают ваш почтовый адрес, когда вы посещаете веб-сайт, поэтому вы можете даже не понять, что именно вы его дали. Много почтовых систем имеют возможности фильтрации почты, то есть поиска указанных слов или словосочетаний в заголовке письма или его теле и последующего помещения писем в определенный почтовый ящик или удаления. Но большинство пользователей не знает, как использовать механизм фильтрации. Кроме того, фильтрация у клиента происходит после того, как письмо уже получено или загружено, поэтому таким образом тяжело удалить большие объемы писем.

Для безопасной атаки можно использовать анонимный ремэйлер. Когда кто-то хочет послать оскорбительное или угрожающее письмо и при этом скрыть свою личность, он может воспользоваться анонимным ремэйлером. Если человек хочет послать электронное письмо, не раскрывая свой домашний адрес тем, кто может угрожать ему, он может тоже использовать анонимный ремэйлер. Если он начнет вдруг получать нежелательные письма по своему текущему адресу, он может отказаться от него и взять новый.

Одним часто используемым средством защиты, применяемым некоторыми пользователями Usenet, является *конфигурирование своих клиентов для чтения новостей* таким образом, что в поле Reply-To (обратный адрес) письма, посылаемого ими в группу новостей, помещается фальшивый адрес, а реальный адрес помещается в сигнатуре или в теле сообщения. Таким образом, программы сбора почтовых адресов, собирающие адреса из поля Reply-To, окажутся бесполезными.

В конгрессе США было подано несколько биллей об ограничениях на работу таких программ-мусорщиков. В одних предлагалось создать списки стоп-слов и помещать слово "реклама" в строку темы письма, в другом предлагалось считать их просто незаконными.

Защита электронной почты

- *Защита от фальшивых адресов.*

От этого можно защититься с помощью использования присоединения к письмам электронных подписей.

- *Защита от перехвата.*

От него можно защититься с помощью шифрования сообщения или канала, по которому он передается. Одним из самых популярных приложений является PGP. Коммерческая версия PGP включает в себя плагины для нескольких популярных почтовых программ, что делает ее особенно удобной для включения в письмо электронной подписи и шифрования письма клиентом. Последние версии PGP используют версию алгоритма шифрования RSA.

- *Корректное использование электронной почты*

Все служащие должны использовать электронную почту так же, как и любое другое официальное средство организации. Из этого следует, что когда письмо посылается, то как отправитель, так и получатель должны гарантировать, что взаимодействие между ними осуществляется согласно принятым правилам взаимодействия. Взаимодействие с помощью

почты не должны быть неэтичным, не должно восприниматься как конфликтная ситуация или содержать конфиденциальную информацию.

- Защита электронных писем и почтовых систем

Защита писем, почтовых серверов и программ должна соответствовать важности информации, передаваемой по сетям. Как правило, должно осуществляться централизованное управление сервисами электронной почты и должна быть разработана политика, в которой указывался бы нужный уровень защиты.

Примеры политик безопасности для электронной почты

- Низкий риск
  - Пользователь.

Использование служб электронной почты для целей, явно противоречащих интересам организации или противоречащих политике безопасности организации, явно запрещено, так же, как и чрезмерное использование их в личных целях. Использование адресов организации в письмах-пирамидах запрещено.

Организация предоставляет своим сотрудникам электронную почту для выполнения ими своих обязанностей. Ограниченное использование ее в личных целях разрешается, если оно не угрожает организации.

Использование электронной почты для получения личной коммерческой выгоды запрещено.

  - Менеджер.

Все сотрудники должны иметь адреса электронной почты. Справочники электронных адресов должны быть доступны для общего доступа.

Если организация обеспечивает доступ к электронной почте внешних пользователей, таких как консультанты, контрактные служащие или партнеры, они должны прочитать правила доступа к электронной почте и расписаться за это.

Содержимое почтовых сообщений считается конфиденциальным, за исключением случая проведения расследований органами внутренних дел.

Сотрудник отдела автоматизации. POP-сервер должен быть сконфигурирован так, чтобы исключить использование незашифрованных паролей с локальных машин.

- Средний риск
  - Пользователь.

Электронная почта предоставляется сотрудникам организации только для выполнения ими своих служебных обязанностей. Использование ее в личных целях запрещено.

Конфиденциальная информация или информация, являющаяся собственностью организации, не может быть послана с помощью электронной почты.

Могут использоваться только утвержденные почтовые программы. Нельзя устанавливать анонимные ремэйлеры. Служащим запрещено использовать анонимные ремэйлеры.

  - Менеджер.

Конфиденциальная информация или информация, являющаяся собственностью организации, не может быть послана с помощью электронной почты.

Если будет установлено, что сотрудник в личных целях использует электронную почту, он будет наказан.

  - Сотрудник отдела автоматизации.

Почтовая система должна обеспечивать только один внешний электронный адрес для каждого сотрудника. Этот адрес не должен содержать имени внутренней системы или должности.

Должен вестись локальный архив MIME-совместимых программ для просмотра специальных форматов, который был бы доступен для внутреннего использования.

- Высокий риск
  - Пользователь.

Электронная почта предоставляется сотрудникам организации только для выполнения своих служебных обязанностей. Использование ее в личных целях запрещено.

Все электронные письма, создаваемые и хранимые на компьютерах организации, являются собственностью организации и не считаются персональными.

Организация оставляет за собой право получить доступ к электронной почте сотрудников, если на, то будут веские причины. Содержимое электронного письма не может быть раскрыто, кроме как в целях обеспечения безопасности или по требованию правоохранительных органов.

Пользователи не должны позволять кому-либо посылать письма, используя их идентификаторы. Это касается их начальников, секретарей, ассистентов или других сослуживцев. Организация оставляет за собой право осуществлять наблюдение за почтовыми отправлениями сотрудников. Электронные письма могут быть прочитаны организацией, даже если они были удалены и отправителем, и получателем. Такие сообщения могут использоваться для обоснования наказания.

- Менеджер.

Справочники электронных адресов сотрудников не могут быть сделаны доступными всем. Если с помощью электронного письма должна быть послана конфиденциальная информация или информация, являющаяся собственностью организации, она должна быть зашифрована так, чтобы ее мог прочитать только тот, кому она предназначена, с использованием утвержденных в организации программ и алгоритмов.

Никто из посетителей, контрактников или временных служащих не имеет права использовать электронную почту организации.

Должно использоваться шифрование всей информации, классифицированной как критическая или коммерческая тайна, при передаче ее через открытые сети, такие как Интернет.

Выходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение политики.

- Сотрудник отдела автоматизации. Входящие письма должны проверяться на вирусы или другие РПС.

Почтовые серверы должны быть сконфигурированы так, чтобы отвергать письма, адресованные не на компьютеры организации.

Журналы почтовых серверов должны проверяться на предмет выявления использования неутвержденных почтовых клиентов сотрудниками организации, и о таких случаях следует докладываться.

Почтовые клиенты должны быть сконфигурированы так, чтобы каждое сообщение подписывалось с помощью цифровой подписи отправителя.

Хранение электронных писем

Официальные документы организации, передаваемые с помощью электронной почты, должны быть идентифицированы и должны администрироваться, защищаться и сопровождаться настолько долго, насколько это нужно для деятельности организации, аудита, юристов или для других целей.

Когда электронная почта - это единственный способ передачи официальных документов компании, то к ним применяются те же самые процедуры, как если бы они передавались на бумаге.

Для предотвращения случайного удаления писем сотрудники должны направлять копии таких сообщений в официальный файл или архив. Должны храниться как входящие, так и выходящие сообщения с приложениями. Любое письмо, содержащее формальное разрешение или выражающее соглашение организации с другой организацией, должно копироваться в соответствующий файл (или должна делаться его печатная копия) для протоколируемости и аудита. Период хранения всех писем определяется юристами.