Защита электронной почты

Особенности «сторожевых собак»

Электронная почта (наряду с FTP и Telnet) — один из самых первых сервисов, реализованных в компьютерных сетях. В настоящее время для многих компаний это не менее важное средство связи, чем обычная почта. Давайте посмотрим, насколько безопасна работа с электронной почтой, какие подводные камни подстерегают вашу компанию при ее использовании и как их можно избежать.

Почта может быть опасной. Это известно еще с тех времен, когда изобрели ядовитые чернила и додумались вкладывать бомбы в посылки. Письма могут быть поддельными — это также хорошо известно. Электронная почта не является исключением, скорее наоборот: она дает злоумышленникам больше свободы для творчества, и возможный экономический ущерб от такой атаки может быть весьма и весьма велик.

Безопасность электронной почты должна обеспечиваться как на уровне администратора сети, так и на уровне конечного пользователя. И если от администратора мы вправе ожидать определенного профессионализма в этой области, то ситуация с конечными пользователями гораздо сложнее. В большинстве случаев (возможно, это покажется парадоксальным) именно пользователь является агентом злоумышленника, с помощью которого последний осуществляет атаку. Поэтому служба электронной почты предприятия должна быть организована так, чтобы администратор мог перехватить как можно большее число потенциальных инцидентов еще до того, как в игру вступит пользователь. В частности, речь идет о политике ретрансляции, способах аутентификации, сканировании вложений и других мерах, о которых мы расскажем ниже.

Давайте сначала рассмотрим опасности электронной почты и борьбу с ними с точки зрения пользователя, а уже потом перейдем к работе администратора. Предполагается, что читатель второй части знаком с устройством и функционированием электронной почты и другими интернет-технологиями. »

Что подстерегает пользователя

«Посылки с бомбами»

Поскольку опасность для компьютера пользователя могут представлять только запущенные на этом компьютере программы, пересылка текстовых сообщений совершенно безвредна, но любая программа, содержащаяся во вложении (attachment) к письму и неосторожно (либо автоматически) запущенная при его прочтении, может причинить компьютеру любой мыслимый вред. Такие почтовые вирусы получили в последнее время широкое распространение. Причина этого заключается в недостаточной компьютерной грамотности пользователей, а не в недостатках системы электронной почты.

Почтовый вирус «Анна Курникова», появившийся в феврале 2001 г., заключался в файле AnnaKournikova.jpg.vbs. Почтовая программа MS Outlook Express при определенных настройках Windows опускает стандартные расширения, из-за чего невнимательные пользователи считали, что получили изображение в формате JPEG, в то время как на самом деле файл содержал программу на языке Visual Basic.

Вирус SirCam применяет тот же прием, но использует имена файлов-документов, обнаруженных им на предыдущем зараженном компьютере. Таким образом, руководитель предприятия может получить из канцелярии файл под названием «Директору предприятия о совещании.doc.exe», так как на зараженном компьютере канцелярии вирус обнаружил файл «Директору предприятия о совещании.doc». В данном случае расчет, очевидно, делается на имитацию производственной среды атакуемого пользователя.

Некоторые современные почтовые серверы производят автоматическую проверку вложений в проходящих через них письмах на наличие вредоносных программ. Следует проконсультироваться у сетевого администратора или провайдера, производится ли такая проверка и какие именно типы приложений проверяются.

Обман и шпионаж

Второй аспект безопасности электронной почты состоит в том, что фальсификация адреса отправителя в протоколе SMTP, с помощью которого письма пересылаются через Интернет, является абсолютно тривиальной задачей. Правильная конфигурация почтовых серверов может ослабить эту угрозу, но совсем ликвидировать ее нельзя. В итоге, например, пользователь может получить письмо от сетевого администратора с просьбой в связи с технической необходимостью выслать свой пароль входа в систему X на указанный адрес, который на самом деле является адресом злоумышленника.

Надо сказать, что незамысловатый обман с фальсификацией отправителя почти всегда приводит к успеху в случае с неквалифицированными пользователями. Такой тип атак называется social engineering и является скорее психологическим, чем техническим приемом. Для борьбы с ним всем пользователям сети должна быть четко разъяснена политика безопасности на предприятии и, в частности, что администратор никогда не попросит пользователя сообщить свой пароль.

Необходимо также понимать, что злоумышленник может еще и свободно читать вашу переписку, поскольку почтовые сообщения передаются через Интернет в открытом виде. Обе эти проблемы могут быть решены только с помощью шифрования сообщений и цифровой подписи (например, PGP). Если вы не используете этих технологий, вы должны знать, что любое ваше письмо может быть прочитано злоумышленником. Разумеется, мы не утверждаем, что вышеперечисленные несчастья обязательно происходят с вашей перепиской, но вы должны руководствоваться здравым

Почтовые вирусы

Профилактика заражения

Избежать поражения почтовым вирусом можно, если следовать нескольким простым правилам.

Никогда не конфигурируйте свою почтовую программу на автоматическое открытие (извлечение) приложений.

Имейте в виду, что программа может быть изначально сконфигурирована в этом режиме, поэтому не поленитесь изучить настройки программы и проверить ее поведение на примерах (можете посылать письма с вложениями сами себе).

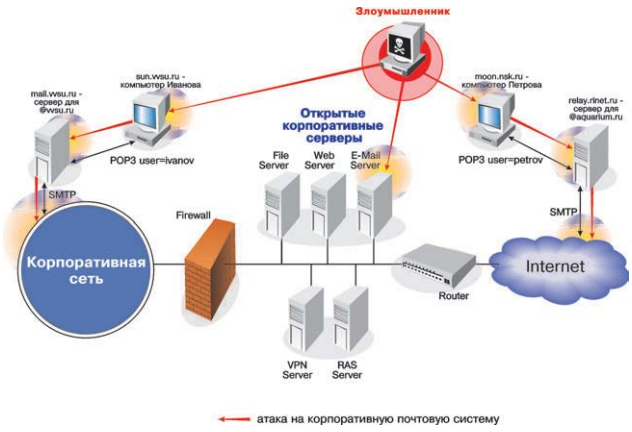
Запомните, что любое вложение в письме от любого корреспондента может быть вредоносной программой, даже если это письмо от хорошо знакомого вам человека. Следует понимать, что письма отправляются не людьми, а программами, и программа, заразившая компьютер вашего друга, просто рассылает себя от его имени по всем адресам, обнаруженным в его адресной книге.

Если ваша почтовая программа не проверяет вложения на наличие вирусов, извлеките вложение в отдельный файл на диске и проверьте его антивирусной программой. Если вы получили письмо с неизвестным вам типом файла или с неожиданным, неадекватным для данного отправителя приложением, попросите у отправителя разъяснений по поводу этого приложения (естественно, до того, как вы его откроете).

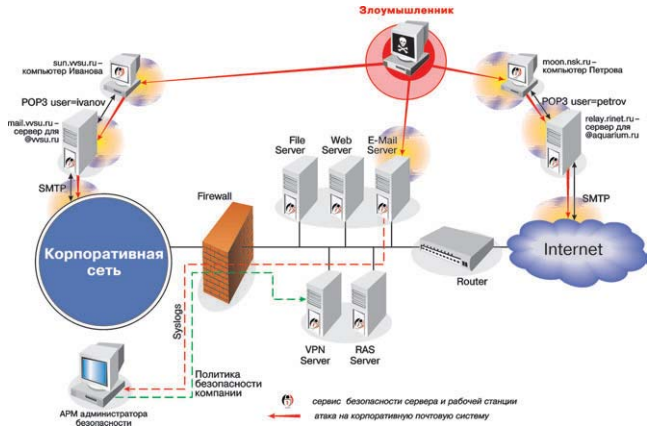
Помните, что не только EXE-файлы, но и файлы Visual Basic Script (VBS), Miscrosoft Office (Word, Excel), файлы HTML, PostScript (PS), Program Information File (PIF) в общем случае являются программами и могут содержать вредоносный код. Если вы не ходите вдаваться в подробности и запоминать опасные и безопасные типы файлов, пользуйтесь общим правилом: любое вложение может содержать вредоносный код.

Убедитесь, что вы видите полное имя файла, содержащегося во вложении, то есть ваша почтовая программа не опускает расширение и не сокращает слишком длинное имя. Система (по крайней мере MS Windows) будет интерпретировать файл по его последнему расширению, то есть файл «Документ.txt.exe» будет интерпретирован как исполняемый EXE-файл.

Своевременно обновляйте базу данных антивирусной программы и проводите периодическую проверку всех файлов системы.



▲ Рис. 1. Служба электронной почты предприятия



▲ Рис. 2. Защита электронной почты

» смыслом, как и в случае с обычной почтой. Иными словами, вы спокойно переписываетесь с друзьями по поводу планов на выходные, но вряд ли отправите в обычном конверте шифр своего банковского сейфа.

Кража паролей

Третий аспект безопасности — открытая передача имени пользователя и пароля на сервер электронной почты. Для доступа к серверу почтовая программа использует протокол POP или IMAP. Естественно, что для получения почты пользователь должен предоставить пароль, который передается через сеть на сервер; иногда пароль требуется и при отправке сообщения. Перехват пароля позволит злоумышленнику не только свободно читать адресованные пользователю письма или удалять их с сервера до того, как к ним получит доступ адресат. Часто почтовый пароль пользователя совпадает с системным; многие вообще используют один и тот же пароль для получения почты и входа в различные системы предприятия (Unix-узлы, web-серверы, сеть Windows). Перехватив такой пароль, злоумышленник получит доступ к другим, возможно, лучше защищенным и более ответственным системам.

Защититься от перехвата пароля можно, применяя методы аутентификации, не требующие передачи пароля в открытом виде (APOP, SASL), или шифруя все передаваемые между клиентом и сервером данные (SSL). POP-клиент и сервер должны поддерживать используемый протокол APOP или SSL. Отметим, что пользователю необходимо поинтересоваться у администратора, какие методы защищенной аутентификации используются в сети предприятия и поддерживает ли их используемая почтовая программа.

Администратор на страже

Система электронной почты предприятия должна быть организована так, чтобы весь почтовый трафик (по крайней мере трафик между корпоративной сетью и Интернетом) проходил через один почтовый сервер (рис. 1). В этом случае администратор имеет возможность контролировать сообщения на предмет опасных вложений, а также решать другие задачи, например блокирование спама. Если на предприятии используется только один почтовый сервер, то задача «стягивания» почтового трафика в одну точку автоматически решена.

Известные производители антивирусных программ (например, «Лаборатория Касперского») предлагают специальные модули для почтовых серверов (рис. 5), которые производят проверку корреспонденции на наличие вирусов. Например, такой модуль для программы sendmail реализован в виде агента доставки, который используется вместо стандартного агента. Поступившее на сервер сообщение передается программой sendmail модулю AVP и только после успешной проверки доставляется адресату.

Если же инцидент все-таки произошел, то адрес компьютера-отправителя может быть определен исследованием заголовков «Received:» полученного сообщения. В этих заголовках записан путь сообщения через почтовые серверы Интернета начиная от отправителя. Отметим, что крайне маловероятно, чтобы отправителем был компьютер злоумышленника; скорее всего это предыдущая жертва атаки. В любом случае вам следует через региональную регистратуру Интернета (для России и Европы — RIPE, www.ripe.net) по IP-адресу отправителя определить административную принадлежность этого компьютера, связаться с лицом, указанным как технический контакт (tech-c) этой организации и сообщить о произведенной атаке.

Что касается фальсификации почтовых сообщений, то никаких прямых средств борьбы с ними администратор предложить не может. Серьезное затруднение для фальсификаторов составила бы обязательная аутентификация SMTP-сеанса всеми почтовыми серверами. В этом случае происхождение письма будет явно указано, если только злоумышленник не похитил пароль другого пользователя и не использовал его при аутентификации. Однако SMTP-аутентификация в настоящее время применяется редко, кроме того, в Интернете еще много открытых ретрансляторов, чтобы можно было говорить о сколько-нибудь серьезных трудностях в деле фальсификации сообщений. К тому же далеко не каждый пользователь внимательно изучает служебные заголовки писем с целью определения достоверности их источника. В общем же случае только использование цифровой подписи может гарантировать подлинность сообщения (рис. 2). »

> При **использовании** электронной почты вы должны **руководствоваться** здравым **смыслом**, как и в случае с обычной почтой

» Процедуры аутентификации и их защита

Вопросы надежной аутентификации, при которой злоумышленник, прослушивающий сеть, не может перехватить пароль пользователя, заслуживают особого внимания. В системе электронной почты аутентификации подвергается пользовательский агент. По отношению к почтовому серверу он выступает в качестве POP- или IMAP-клиента при получении сообщений и SMTP-клиента — при отправке. Как уже говорилось, аутентификация SMTP-клиента не слишком распространена. Хотя это весьма полезно, если сервер желает ограничить круг обслуживаемых пользователей или работать с мобильными пользователями, не становясь при этом открытым ретранслятором. Необходимость аутентификации POP- и IMAP-клиентов очевидна.

Передача имени и пароля пользователя в открытом виде (команды POP USER/PASS и команда IMAP LOGIN), безусловно, не является хорошим решением. Разработчики протокола POP первыми столкнулись с этой проблемой и внедрили механизм аутентификации APOP.

Команда APOP после имени пользователя передает не открытый пароль, а дайджест пароля. Дайджест получается в результате работы алгоритма MD5 над массивом данных, состоящим из временного штампа и пароля пользователя. Временной штамп выдается сервером в тексте приглашения в начале сеанса и предназначен для предотвращения атак воспроизведением. В приведенном ниже примере приглашения POP-сервера временной штамп имеет вид <9158.989448259@mail.exmpl.ru>, где 9158 — идентификатор процесса, 989448259 — время начала сеанса (в формате UNIX), mail.exmpl.ru — доменное имя сервера.

APOP-аутентификация может выглядеть следующим образом (здесь и далее полужирным шрифтом выделены команды, присылаемые клиентом, а обычным шрифтом — вывод сервера):

```
+OK QPOP starting.
<9158.989448259@mail.exmpl.ru>
APOP ivanov
c4c9334bac560ecc979e58001b3e22fb
```

Значение дайджеста помещается в команду не в кодировке Base64, которая широко используется для представления двоичных данных в текстовом виде, а в виде »

Почтовая аутендификация

Примеры реализации

Рассмотрим пример реализации SASL в протоколе IMAP. В примере используется механизм CRAM-MD5 (RFC-2104), который аналогичен APOP с той разницей, что первый использует несколько более сложный алгоритм для вычисления дайджеста пароля с временным штампом.

```
* OK IMAP4 Server
A0001 AUTHENTICATE CRAM-MD5
+ PDE4OTYuNjk3MTcw0TUyQHBvc3Rv
ZmZpY2UucmVzdG9u
dGltIGI5MTNhNjAyYzdlZGE3YTQ5NWI0
ZTZlNzMzNGQzODkw
A0001 OK CRAM authentication success-
ful
```

После того как клиент выдал команду AUTHENTICATE, сервер откликнулся запросом.

Признаком запроса является символ + с последующим пробелом, с которых начинается строка.

Запрос представляет собой временной штамп <9158.989448259@mail.exmpl.ru>, закодированный с помощью Base64.

Отклик клиента, как и в APOP, — это строка, состоящая из имени пользователя и дайджеста пароля пользователя с присланным временным штампом. Отклик клиента также кодируется по алгоритму Base64.

Для того чтобы определить, какие механизмы аутентификации поддерживаются IMAP-сервером, клиент может подать команду CAPABILITY:

```
abcd CAPABILITY
* CAPABILITY IMAP4rev1
AUTH=KERBEROS_V4 AUTH=CRAM-MD5
abcd OK CAPABILITY completed
```

Аналогично обстоят дела в протоколе POP3 (с той разницей, что команда называется AUTH):

```
+OK POP server ready
AUTH CRAM-MD5
+ PDE4OTYuNjk3MTcw0TUyQHBvc3RvZm
ZpY2UucmVzdG9u
dGltIGI5MTNhNjAyYzdlZGE3YTQ5NWI0
ZTZlNzMzNGQzODkw
+OK CRAM authentication successful
```

Для того чтобы определить, какие механизмы аутентификации поддерживаются POP-сервером, клиент может подать команду CAPA:

```
CAPA
+OK Capability list follows
TOP
USER
SASL CRAM-MD5 KERBEROS_V4
```

Наличие в выводе команды функции SASL говорит, что сервер поддерживает команду AUTH с указанными механизмами.

И наконец, реализация SASL в протоколе SMTP также представлена командой AUTH:

```
220 mail.exmpl.ru ESMTP server ready
EHLO eldorado.com
250-mail.exmpl.ru
250 AUTH CRAM-MD5 DIGEST-MD5
AUTH CRAM-MD5
334 PDE4OTYuNjk3MTcw0TUyQHB
vc3RvZmZpY2UucmVzdG9u
dGltIGI5MTNhNjAyYzdlZ
GE3YTQ5NWI0ZTZlNzMz
NGQzODkw
235 Authentication successful.
```

Наличие в выводе команды EHLO дополнительной функции AUTH говорит, что сервер поддерживает команду AUTH с указанными механизмами.

» последовательности шестнадцатеричных цифр в нижнем регистре.

Для проверки правильности указанного пользователем пароля сервер со своей стороны вычисляет аналогичный дайджест и сравнивает его с тем, который прислал пользователь в команде APOP.

Позднее был предложен общий подход к аутентификации, пригодный для любых протоколов, обменивающихся командами и откликами в текстовом виде, в том числе POP, IMAP и SMTP. Подход называется SASL — Simple Authentication and Security Layer (RFC-2222).

Согласно SASL аутентификация начинается с команды, которую подает клиент. Команда сопровождается обязательным параметром, указывающим механизм (алгоритм) аутентификации. Далее следует обмен запросами и ответами: сервер делает некоторый запрос, клиент на основании этого запроса вычисляет ответ и возвращает его серверу. Смысл запросов и ответов определяется используемым механизмом операции. Если рассматривать в рамках этого подхода механизм APOP, то запросом является временной штамп, выставляемый сервером при открытии соединения, а ответом — дайджест пароля пользователя и временного штампа. Некоторые алгоритмы предусматривают многократный обмен запросами и ответами.

В общем, при получении ответа от клиента сервер может реагировать одним из трех способов: выставить следующий запрос, объявить об успешном завершении аутентификации или о том, что аутентификация провалилась. Со своей стороны клиент при получении запроса может возвратить ответ или объявить об отказе от аутентификации.

Наиболее распространенными являются механизмы, основанные на MD5: DIGEST-MD5 и CRAM-MD5. Все механизмы, исключая тривиальный PLAIN, обеспечивают защищенную аутентификацию. Естественно, и клиент, и сервер должны поддерживать выбранный механизм, и именно это требование, скорее всего, будет определять выбор механизма в каждом конкретном случае. К сожалению, некоторые программы поддерживают только механизм PLAIN, оставляя пароли пользователей без всякой защиты.

Подчеркнем, что никакая из схем аутентификации не спасает от злоумышленника, способного осуществить перехват TCP-соединения. В этом случае он сначала ретранслирует команды аутентификации между клиентом и сервером, а после того, как аутентификация прошла успешно, блокирует сегменты клиента и сам начинает давать команды от его имени.

> При использовании **нестандартных** агентов доставки необходимо тщательно **проверять** их **«доверчивость»** к вводу

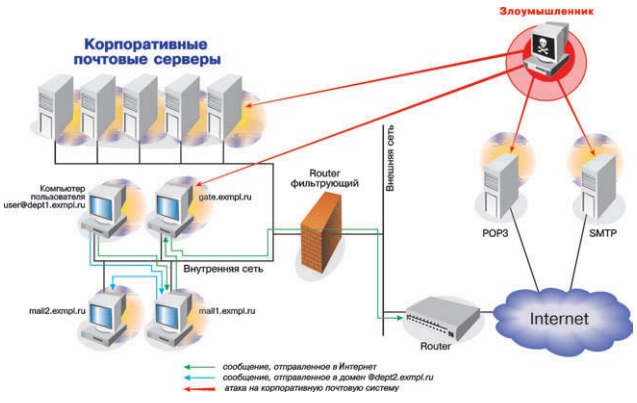
Мой сервер — моя крепость

Действия злоумышленника могут быть также направлены не против конечных получателей сообщений, а против собственно почтового сервера (рис. 3).

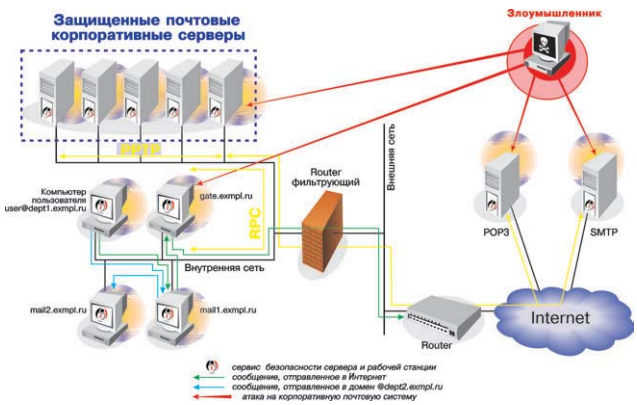
В этом случае почтовое программное обеспечение служит для злоумышленника дверью в операционную систему сервера. Разумеется, администратор должен держать эту дверь плотно закрытой. В качестве исторического примера открытой двери упомянем знаменитую ошибку в ранних версиях sendmail, позволявшую SMTP-клиенту выполнить любую команду в операционной системе сервера, причем с правами суперпользователя. Впрочем, мы не будем обсуждать ошибки в программировании, которые, будучи обнаруженными, быстро исправляются. В этом контексте от администратора требуется только своевременное обновление программного обеспечения.

Концептуальную проблему в обеспечении безопасности почтового сервера представляют собой агенты доставки. Фактически, приход сообщения с локальным адресом вызывает запуск некоторой программы, на вход которой подается почтовое сообщение. Что именно делает эта программа и содержит ли она ошибки, транспортному агенту неизвестно — но, вероятно, хорошо известно злоумышленнику, который может использовать свойства агента доставки для проникновения в операционную систему сервера или осуществления отказа в обслуживании.

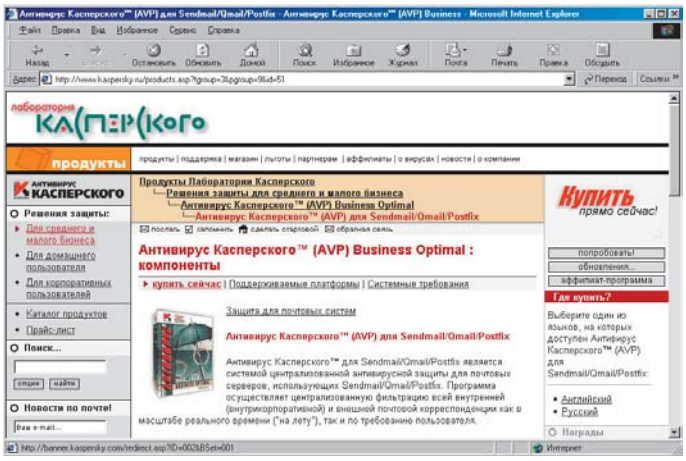
Скорее всего, администратору не стоит беспокоиться по этому поводу, если на почтовом сервере используется только стандартный агент доставки (программа mail): эта программа находится в непрерывной эксплуатации на огромном числе хостов и любые обнаруженные в ней ошибки будут немедленно опубликованы. Однако при использовании нестандартных, а особенно самодельных агентов необходимо тщательно проверить их функциональность и «доверчивость» к вводу включая возможность переполнения буферов. Понятие доверчивости включает также проверку ввода на соответствие определенному шаблону. Например, »



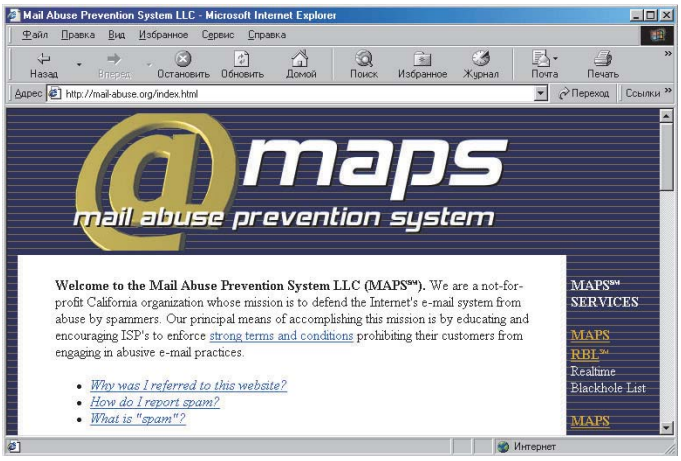
▲ Рис. 3. Электронная почта в корпоративной сети



▲ Рис. 4. Защита корпоративной электронной почты



▲ Рис. 5. Антивирус Касперского для Sendmail/Qmail/Postfix



▲ Рис. 6. Антиспамерская оранизация MAPS

» если агент доставки открывает в системе файл, имя которого извлекается из текста или заголовков сообщения, то в программе агента должна быть проверка на отсутствие в имени файла специальных символов, которые позволяют открыть файл в другом каталоге или вместо открытия файла запустить программу.

Со своей стороны транспортный агент может предпринять следующие меры, ограничивающие возможности агента доставки и, следовательно, потенциальный ущерб из-за некорректной работы последнего. Транспортный агент может запустить агента доставки с низкими привилегиями, а также ограничить ему видимость файловой системы только определенным каталогом и его подкаталогами.

Многие почтовые серверы позволяют своим пользователям перенаправлять содержимое поступающих на их адреса писем на ввод указанных пользователем программ (в Unix/sendmail это делается в файле .forward). В этом случае администратору стоит позаботиться, чтобы пользователям было разрешено подключать для обработки своих писем только проверенные, одобренные программы.

Открытые ретрансляторы и борьба со спамом

Транспортный агент, принимающий почтовые сообщения, следующие от кого угодно кому угодно, называется открытым ретранслятором (open relay). Открытые — умышленно или по неопытности администратора — ретрансляторы используются для рассылки спама и вредоносных сообщений. Действительно, ничто не мешает любому злоумышленнику установить SMTP-сеанс с открытым ретранслятором, указать произвольный список получателей и передать произвольное сообщение. Транспортный агент добросовестно разошлет сообщение по всем указанным адресам. Кроме того что злоумышленник употребил для своих целей ресурсы чужого компьютера и чужой сети, потраченные на, возможно, массивную рассылку, локализовать злоумышленника в этом случае крайне сложно, поскольку транспортный агент не имеет к злоумышленнику никакого отношения.

Чтобы не быть открытым ретранслятором, транспортный агент должен принимать решение о возможности обработки сообщения на основании IP-адреса SMTP-клиента, почтовых адресов отправителя и получателя. Правила принятия таких решений называются политикой ретрансляции.

Разумной является политика, когда принимаются любые сообщения от клиентов, расположенных в собственной сети (домене) сервера, а от внешних клиентов принимаются только сообщения, адресованные в домен сервера (такая политика реализована в sendmail по умолчанию). Однако эта политика не позволяет пользователям сервера, находящимся вне сети организации (так называемым мобильным пользователям) передавать серверу сообщения для отправки. Действительно, если ivanov@exmpl.ru находится на выезде, он не может использовать сервер mail.exmpl.ru для отправки письма на адрес jose@eldorado.com, потому что в данном случае SMTP-клиент Иванова находится во внешней сети и письмо не направится в домен exmpl.ru. Можно было бы разрешить обработку сообщений с обратным адресом типа @exmpl.ru, но в этом случае любой злоумышленник, тривиально указав в качестве адреса отправителя любой адрес из @exmpl.ru, мог бы свободно пользоваться сервером, фактически превратив его в открытый ретранслятор.

Подделать IP-адрес SMTP-клиента, заменив его адресом из сети exmpl.ru, конечно, тоже возможно, но гораздо сложнее, чем просто указать разрешенный адрес в команде MAIL FROM.

Чтобы разрешить отправку сообщений через сервер только определенным пользователям независимо от того, где они находятся, следует использовать аутентификацию SMTP-клиента. При этом автоматически решится проблема обслуживания мобильных пользователей. Если же SMTP-аутентификация сервером mail.exmpl.ru не поддерживается, то Иванову придется искать SMTP-сервер в сети той организации, через которую он в данный момент подключен к Интернету.

Формулируя политику ретрансляции сообщений, администратор сервера может реализовать борьбу со спамом: не принимать сообщения из доменов или с адресов, которые зарекомендовали себя как распространители спама. В Интернете существует организация MAPS (http://mail-abuse.org), поддерживающая базу данных адресов хостов, которые умышленно или по недосмотру являются открытыми ретрансляторами или замечены как источники спама (рис. 6). Доступ к базе данных осуществляется через DNS, за деталями отсылаем читателя на вышеуказанный интернет-сайт. Отметим, что программа sendmail может быть настроена на проверку IP-адресов отправителей по черным спискам MAPS. При этом, конечно, следует учитывать, что заблокировав прием сообщений от некоторого хоста, администр- »

Почтовые агенты

Три разновидности

Напомним, что в почтовой системе различают три вида агентов: транспортные агенты, агенты доставки и пользовательские агенты. Транспортные агенты осуществляют прием сообщений, обработку заголовков и выбор агента доставки. Агенты доставки могут доставлять сообщение следующими способами: дописыванием в конец файла, сохранением в базу данных, отправкой через сеть и т. п. Пользовательский агент — это почтовая программа конечного пользователя.

» ратор отфильтровывает не только спам, но и вообще все следующие от этого сервера сообщения.

Электронная почта и брандмауэры

Обсудим особенности работы электронной почты в сети, защищенной брандмауэром (рис. 4).

Во внутренней (защищаемой) сети работает один или несколько почтовых серверов, обслуживающих почтовые домены предприятия. Например, @exmpl.ru обслуживается сервером mail.exmpl.ru, @dept1.exmpl.ru обслуживается сервером mail1.exmpl.ru, @dept2.exmpl.ru обслуживается сервером mail2.exmpl.ru и т. д.

Для пересылки сообщений между этими доменами серверы взаимодействуют непосредственно друг с другом, поскольку все они находятся во внутренней сети. Однако для обмена сообщениями с Интернетом каждый сервер должен устанавливать соединения с SMTP-серверами, находящимися в Интернете. Это не лучшее решение с точки зрения безопасности, поскольку каждый почтовый сервер становится открытым, видимым для потенциального злоумышленника и правила фильтрации брандмауэра должны позволять любому хосту Интернет устанавливать соединение по порту 25 с любым почтовым сервером, находящимся во внутренней сети. К тому же некоторые внутренние почтовые серверы могут находиться вне непосредственного административного контроля сетевого администратора предприятия.

Оптимальное решение состоит в том, чтобы для обмена почтовыми сообщениями с Интернетом использовался один почтовый сервер (например, gate.exmpl.ru), играющий роль форвардера (или, иными словами, прокси-сервера) для остальных почтовых серверов предприятия. Каждый из серверов mail.exmpl.ru, mail1.exmp.ru, mail2.exmpl.ru и т. п. должен быть сконфигурирован так, чтобы все сообщения, адресованные в Интернет, перенаправлялись им на gate.exmpl.ru, который в свою очередь взаимодействует с почтовыми серверами Интернета.

Фильтрующий маршрутизатор настраивается для пропуска SMTP-трафика, идущего только от или к gate.exmpl.ru (признаком SMTP-сегмента является порт назначения 25).

Теперь требуется решить обратную задачу: чтобы все сообщения, следующие из Интернета в домены @exmpl.ru, @dept1.exmpl.ru, @dept2.exmpl.ru, доставлялись серверами Интернета на gate.exmpl.ru, а тот в свою очередь рассылал эти сообщения внутренним серверам, обслуживающим домен адресата.

Для этого следует использовать расщепление зоны DNS. Во внешнюю версию базы данных зоны вносится запись:

```
*.exmpl.ru      IN   MX   10 gate.exmpl.ru
```

А во внутренней версии содержится полная информация о почтовых доменах:

```
exmpl.ru        IN   MX   10 mail.exmpl.ru
dept1.exmpl.ru  IN   MX   10 ail1.exmpl.ru
dept2.exmpl.ru  IN   MX   10 ail2.exmpl.ru
```

Хосты в Интернете пользуются внешней версией баз данных и поэтому отсылают все сообщения, направленные в домен exmpl.ru и любые его поддомены, SMTP-серверу gate.exmpl.ru. Последний пользуется внутренней, полной версией зоны. Следовательно, получив сообщение, он ретранслирует его на соответствующий внутренний почтовый сервер.

Естественно, на gate.exmpl.ru должна быть разрешена ретрансляция сообщений следующих из и в домен exmpl.ru и его поддомены.

Использование централизованного сервера для отправки и приема сообщений позволяет также реализовать корпоративную политику борьбы со спамом, проверять входящие и исходящие сообщения на наличие вирусов, решать различные задачи учета и контроля почтового трафика.

Что касается протоколов POP и IMAP, то они обычно используются только во внутренней сети, никак не взаимодействуя с брандмауэром. Если необходим доступ по этим протоколам внешних клиентов к внутренним серверам или, наоборот, внутренних клиентов к внешним серверам, то ситуация существенно ухудшается. В отличие от протокола SMTP, работающего по принципу store-and-forward (передача сообщения через промежуточные станции), протоколы POP и IMAP рассчитаны только на прямое соединение между пользовательской станцией и почтовым сервером, иными словами, в этих протоколах не предусмотрена возможность использования какого-либо прокси-сервиса. Следовательно, при необходимости использования POP или IMAP между внутренней сетью и Интернетом администратору брандмауэра придется открыть доступ к или от внутренних хостов по соответствующим портам. Очевидно, следует предпринять максимум усилий, чтобы избежать этого.

В ситуации, когда внутренним пользователям требуется обеспечить доступ к внешним POP- или IMAP-серверам (например, к mail.ru и ему подобным) можно предложить создание приложения на почтовом сервере gate.exmpl.ru, автоматически и периодически забирающего почту пользователей с внешних POP-серверов. В этом случае необходимо разрешить исходящие в Интернет POP-соединения только для одного сервера, находящегося под контролем администратора.

Обратный случай — обслуживание мобильных пользователей, желающих получить свою почту с сервера предприятия. Если у предприятия только один почтовый сервер gate.exmpl.ru, то администратор брандмауэра разрешает входящие из Интернета POP- или IMAP-соединения на этот защищенный и контролируемый сервер, и вопрос снимается. Для предприятий со сложной многосерверной структурой почтовой системы потребуется существенно менее тривиальное решение, например модификация POP-сервера на gate.exmpl.ru, с тем чтобы он при поступлении соединения от внешнего клиента одновременно обращался к соответствующему внутреннему POP-серверу и таким образом выступал в качестве ретранслятора.

■ ■ ■ Максим Мамаев, Сергей Петренко