Эссе по курсу "Защита информации", кафедра радиотехники, Московский физико-технический институт (ГУ МФТИ), http://www.re.mipt.ru/infsec.
Семерьянов Алексей Сергеевич (8 мая 2005г.)

Безопасность E-mail (Security E-mail)

Многие сферы деятельности человека охвачены информатизацией и с каждым годом их становится все больше и больше. Сейчас, наверное, трудно себе представить какую-либо компанию или организацию, которая обходилась бы без компьютеров и современных средств связи. Сегодняшний рынок диктует свои условия, следовательно все больше и больше людей оказываются втянутыми во «Всемирную паутину». Но с ростом количества пользователей, развитием информационных технологий постоянно увеличивается угроза информационной безопасности. Например, посредством электронной почты с вашим компьютером можно сделать все, что угодно, и если вы не специалист, то даже не узнаете об этом. На сегодняшний день те организации, которые не хотят, чтобы их информация стала доступной, предпринимают различные меры для ее защиты. Над программными продуктами, предназначенными для борьбы с угрозами информационной безопасности, работает огромное количество людей во всем мире.

Существуют различные угрозы информационной безопасности, одной из которых является распространение деструктивного программного кода. Деструктивный код – это программный код, который, внедрившись в вашу систему, может повредить информацию, а вы узнаете об этом в самый последний момент, возможно, когда уже ничего нельзя будет изменить. К видам такого кода относятся всевозможные вирусы, трояны, скрипты. Часто уничтожение или повреждение информации влечет за собой более плачевные последствия, чем, например, поврежденние информационной системы или оборудования. Программы, несущие в себе деструктивный код, могут распространяться различными способами, например, пользователь обратился к ресурсу посредством протокола HTTP. Если ресурс оказался «сомнительным», то компьютер может быть подвергнут действию вируса, а пользователь об этом может даже не подозревать. Все больше и больше людей работают в режиме on-line и все более вероятным становится маршрут доставки вредоносного кода посредством сетевых транспортов.

Можно сказать, что «самым активным распространителем» является протокол SMTP. Электронная почта – самое распространенное средство коммуникации. Число e-mail адресов исчисляется миллионами, наверное, только ленивый, имея доступ в интернет, не зарегистрирует себе электронный почтовый ящик. Ну это и понятно, потому что электронная почта обладает рядом преимуществ по сравнению с обычными способами передачи сообщений. Электронная почта – глобальная система, позволяющая посылать письма в любую точку земного шара за короткое время. С помощью нее возможно передавать различные форматы данных (в одном письме вы сразу можете послать и видео, и фото, и музыкалные файлы). Еще одним преимуществом является дешевизна и доступность этого сервиса. Одно электронное письмо может быть послано различным адресатам без дополнительных затрат. Вдобавок, ко всему перечисленному, e-mail сообщения можно обрабатывать различными программными продуктами, автоматизированно

или автоматически, извлекая нужную информацию, чего уже не получится с обычным бумажным документом. Из всего выше сказанного, можно сделать вывод: электронная почта – один из основных каналов распространения деструктивного программного кода. Значит, нужно задуматься о средствах защиты от атак, действующих через почту.

Атаки могут быть различными и преследовать разные цели. Например, так называемый «почтовый червь», который попадая к вам, распространяется дальше, используя адреса из вашей адресной книги. Атаки на на почтовые сервера, с целью завладения конфиденциальной информацией. Например, если злоумышленник узнает пароль к вашему почтовому ящику, то он сможет слать письма от вашего имени вашим же друзьям или подписать вас на какие-либо рассылки, в результате чего вы будете получать сотни писем в день. Существует несколько вариантов противодействия всякого рода атакам, например, можно использовать программы-антивирусы, которые в данный момент бурно развиваются и совершенствуются. Но часто использование таких программ не позволяет достичь определенного уровня защиты, потому что злоумышленники придумывают различные «способы обмана» антивирусных программ, особенно если знают схему их работы. Поэтому необходимо несколько этапов защиты, начиная с глобального средства, способного проследить весь потенциально опасный поток данных и уменьшить вероятность проникновения вредоносного кода. Одним из способов такого рода защиты является антивирусный почтовый шлюз (SMTP Gateway) – программное обеспечение, позволяющее проверять поток электронных сообщений на наличие в них деструктивного кода. Обычную модель доставки сообщений можно представить следующим образом (рис.1): существуют два SMTP-сервера (сервер отправителя и сервер получателя), DNS-сервер и почтовые клиенты, с помощью которых пользователи отправляют и получают сообщения. SMTP-сервер отправителя запрашивает у DNS-сервера IP-адрес почтового сервера получателя. DNS-сервер обеспечивает трансляцию имен сайтов в IP-адреса. После того, как ответ получен, устанавливается соединение по 25 TCP-порту (стандартный порт) для передачи данных. Чтобы получить сообщения, почтовый клиент использует протокол POP3. Отсюда видно, что данные, проходящие от одного SMTP-сервера к другому, на наличие вирусов не проверяются, значит последние таким образом могут свободно распространяться от одного сервера к другому.

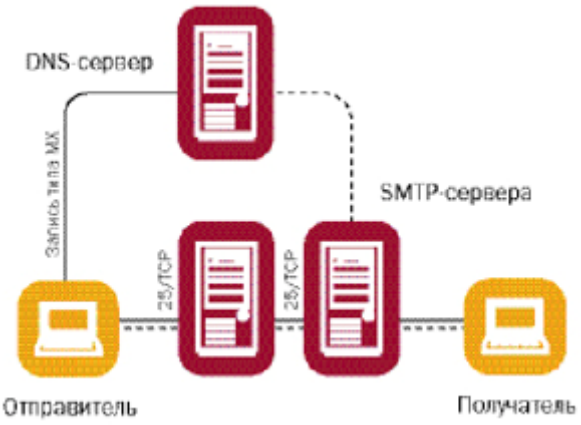

Рис.1 Простая схема.

Рис.2 Схема с использованием антивирусного шлюза.

Некоторый уровень безопасности может обеспечить антивирусная программа, установленная на компьютере пользователя, но не во всех случаях этого оказывается достаточно. Чтобы глобально проверять весь поток данных, приходящих на сервер, и используют антивирусный почтовый шлюз. Он встраивается в изложенную выше схему в виде обычного SMTP-сервера. Таким образом, сообщения отправителя сначала попадают на антивирусный шлюз, а затем, после их проверки, пересылаются дальше получателю. Для антивирусного шлюза разрабатываются специальное программное обеспечение, которое позволяет выявлять вредоносный код, отсеивать нежелательные сообщения (спам). Можно назвать несколько программных продуктов, используемых для глобальной антивирусной проверки. Это WebSchield SMTP, Symantec AntiVirus for SMTP и другие. Каждый из этих продуктов успешно применяется в корпоративных сетях и имеет свои особенности.
Есть еще один вариант глобальной проверки почты – технология CVP (Content Vectoring Protocol). Суть его работы в том, чтобы перенаправить поток данных на специальный сервер, на котором специальным образом этот поток будет обработан.
Все выше сказанное применяется, как я уже сказал, для глобальной проверки всего потока данный, идущего от сервера к серверу. Спустимся на уровень ниже, если можно так выразиться.
Одной из распространенных атак почтовой системы является подмена текста сообщения или же автора сообщения. Будет неприятно, если вы получите сообщение от своего начальника, проделаете какую-либо работу, а потом окажется, что такого сообщения ваш начальник не посылал. И хорошо, если в результате все этого не будет нанесен существенный ущерб вам и вашей организации! Одим из способов защиты от такого рода атак является электронная цифровая подпись, т.е в теле письма передается некоторая буквенно-числовая последовательность, полученная с помощью определенного алгоритма, подтверждающая личность отправителя и позволяющая определить неизменность отправления. Таким образом можно обнаружить было ли письмо изменено и при необходимости запросить еще одну копию, возможно по другому каналу. Но такие алгоритмы указывают только на то, что сообщение было перехвачено, а

следовательно нужно принимать какие-то меры для избежания утечки информации и ее защиты, но не позволяют защититься от перехвата сообщений.
Чтобы защитить сообщение от нежелательного читателя, используют локальные методы шифрования информации, предоставляемые либо почтовыми клиентами либо другими специальными программными продуктами, т.е. перед отправкой сообщение шифруется определенным методом на локальной машине отправителя и отправляется получателю уже в зашифрованном виде, а на локальной машине получателя расшифровывается.
Также, можно упомянуть еще об одном виде программных продуктов, используемых для защиты информации в корпоративных сетях. Это такие продукты, которые осуществляют мониторинг сообщений, как внешних так и внутренних. При попадании сообщения в систему производится полный анализ его содержимого по разным критериям, а при удовлетворении какому-либо критерию над письмом производятся определенные действия. Также такие программные продукты реагируют на нарушения правил использования электронной почты. Но все эти программы, которые пишутся для защиты от разного рода атак касаются технической стороны дела, но задача безопасности не может быть решена только техническими средствами.
Кроме централизованной проверки почты, использования локальных программных продуктов в каждой организации, если она заинтересована в сохранении целостности и недоступности своей информации должна проводиться корпоративная политика использования электронной почты. Необходимо, чтобы каждый сотрудник знал азы (правила) безопасности при работе с электронной почтой, знал о последствиях, которые могут возникнуть при нарушении этих правил, потому как вирус, проникнув благодаря всего лишь одному «неверному» движению на один компьютер, может повредить не только информацию, находящуюся на нем, но и, как обычно и бывает, информацию на других машинах в сети. Поэтому, чтобы по глупости не подвергнутся воздействию вредоносной программы, даже если установленный антивирус не сообщил вам об этом, не нужно без необходимости открывать письма от незнакомых вам людей, а тем более запускать программы, прикрепленные к такому сообщению. Чтобы уменьшить риск атаки вашего почтового ящика, особенно это касается спамерских рассылок, не стоит указывать свой e-mail в различных конференциях, чатах и на такого рода публичных сайтах, иначе вас замучают рекламой и всякой ерундой, ну а если такие спамерские рассылки приходят, то не стоит тратить время на их прочтение.
Итак, из всего выше сказанного видно, что SMTP-протокол является полностью небезопасным, т.е не обеспечивает целостность информации (письмо может быть перехвачено и заменено), не поддерживает аутентификацию пользователей (при перехвате письма можно также заменить его автора или получателя), позволяет распространяться вредоносным программам.
Еще хотелось бы добавить, что угрозы информационной безопасности постоянно расширяются, следуя за ними увеличивается и разнообразие программ им противодействующих и эта гонка будет продолжаться с ростом компьютерных технологий. В связи с этим проблема компьютерной безопасности становится все более актуальной, а следовательно ее нужно уделять особое внимание.

Ссылки:

1. «Безопасность электронной почты». А. Иржавский, 06.10.2003г, http://www.cio-world.ru/bsolutions/e-safety/29383/
2. «Эффективность и безопасность использования электронной почты». А.Таранов, В.Цишевский, О.Слепов, 22.04.2002г. http://jetinfo.isib.ru/2001/9/2/article2.9.2001.html