ЗАЩИТА ЭЛЕКТРОННОЙ ПОЧТЫ

- Электронная почта стала повсеместно используемой «коммунальной» услугой, однако, нельзя не признать, она не достигла пока такого же совершенства в своем функционировании, как водопровод.

- Уровень защиты данных в системе электронной почты влияет на общий уровень информационной безопасности организации, а, следовательно, и эффективность ее деятельности. Это обуславливает важность создания надежной защиты для этого вида коммуникаций.

- Большинство проблем, с которыми сталкиваются пользователи электронной почты (спам, вирусы, разнообразные атаки на конфиденциальность писем и т. д.), связано с недостаточной защитой современных почтовых систем.
- С этими проблемами приходится иметь дело и пользователям общедоступных публичных систем, и организациям. Практика показывает, что одномоментное решение проблемы защиты электронной почты невозможно. Спамеры, создатели и распространители вирусов, хакеры изобретательны, и уровень защиты электронной почты, вполне удовлетворительный вчера, сегодня может оказаться недостаточным. Для того чтобы защита электронной почты была на максимально возможном уровне, а достижение этого уровня не требовало чрезмерных усилий и затрат, необходим систематический и комплексный, с учетом всех угроз, подход к решению данной проблемы.

БОРЬБА СО СПАМОМ И ВИРУСАМИ

- Сегодня доступно множество программных продуктов, в том и числе и бесплатных, предназначенных для борьбы с этой угрозой. Самыми яркими представителями российских антивирусных средств можно назвать продукты компаний «Лаборатория Касперского» и «Диалог-Наука», на основе которых осуществляется защита от вирусов, встраиваемая в почтовые клиенты и публичные почтовые системы. Что же касается решений по борьбе со спамом, здесь возможно несколько вариантов защиты.
- Можно реализовать систему фильтров, позволяющих отсекать входящую корреспонденцию по адресу, теме или содержанию письма. Фильтры обычно размещаются на клиентской стороне, и пользователь сам может задавать необходимые параметры. В качестве примера можно назвать системы Spam Buster производства компании Contact Plus, MailWasher, Active Email Monitor (VicMan Software), eMailTrackerPro (Visualware), Spamkiller (Novasoft) и др. Кроме фильтрации спама такие программы могут выполнять функции очистки почтового ящика, проверки почты, чтения заголовков писем и т.д.

ХАКЕРЫ

- Предпосылки некоторых проблем, связанных непосредственно с конфиденциальностью почтовых сообщений, закладывались при возникновении электронной почты три десятилетия назад. Во многом они не разрешены до сих пор.
- Ни один из стандартных почтовых протоколов (SMTP, POP3, IMAP4) не включает механизмов защиты, которые гарантировали бы конфиденциальность переписки.
- Отсутствие надежной защиты протоколов позволяет создавать письма с фальшивыми адресами. Нельзя быть уверенным на 100% в том, кто является действительным автором письма.
- Электронные письма легко изменить. Стандартное письмо не содержит средств проверки собственной целостности и при передаче через множество серверов, может быть прочитано и изменено; электронное письмо похоже сегодня на открытку.
- Обычно в работе электронной почты нет гарантий доставки письма. Несмотря на наличие возможности получить сообщение о доставке, часто это означает лишь, что сообщение дошло до почтового сервера получателя (но не обязательно до самого адресата).

ОСНОВНЫЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ОТ АТАК НА ЭЛЕКТРОННУЮ ПЕРЕПИСКУ

- Для защиты сетевой инфраструктуры используется немало всевозможных заслонов и фильтров: SSL (Secure Socket Layer), TSL (Transport Security Layer), виртуальные частные сети. Основные методы защиты от атак хакеров строятся именно на основе этих средств. Это, прежде всего, сильные средства аутентификации, например, технология двухфакторной аутентификации, при которой происходит сочетание того, что у вас есть, с тем, что вы знаете. Эта технология используется, например, в работе обычного банкомата, который идентифицирует по карточке и по коду. Для аутентификации в почтовой системе тоже потребуется «карточка» — программное или аппаратное средство, генерирующая по случайному принципу уникальный однократный пароль. Его перехват бесполезен, поскольку он будет уже использован и выведен из употребления. Однако такая мера эффективна только против перехвата паролей, но не против перехвата другой информации (например, сообщений электронной почты).

- Но самый эффективный метод защиты – криптография.
  Криптография - не предотвращает перехвата информации и не распознает работу программ для этой цели, но делает эту работу бесполезной. Криптография также помогает от IP-спуфинга, если используется при аутентификации. Наиболее широко для криптографической защиты передаваемых по каналам связи данных, включая письма электронной почты, применяется протокол SSL, в котором для шифрования данных используются ключи RSA. Однако SSL защищает письма только при передаче; если не используются другие средства криптозащиты, то письма при хранении в почтовых ящиках и на промежуточных серверах находятся в открытом виде.
  Совокупность всех этих средств можно представить как многоуровневую эшелонированную систему обороны. И, тем не менее, как показывает практика, существует возможность пробраться сквозь все эти уровни и получить доступ к данным.

«СИЛЬНЫЕ» КРИПТОАЛГОРИТМЫ

- Самым эффективным способом защиты писем электронной почты от перехвата специалисты по безопасности компьютерных сетей признают их кодирование на основе «сильных» криптографических алгоритмов.

- Существует 2 вида криптоалгоритмов:
  1. Частичное кодирование. Примером системы с частичным кодированием передаваемых данных является популярный почтовый клиент Eudora (вместе с дополнительным модулем, выпущенным в 2001 году), который обеспечивает передачу закодированных писем на двух участках маршрута письма: от отправителя до ближайшего почтового сервера и от получателя до ближайшего почтового сервера. Из российских систем к этому классу относятся Hotbox и Zmail, которые осуществляют защиту переписки на основе SSL.

  2. Полное кодирование. Полное или сквозное (end-to-end) кодирование заключается в том, что кодирование электронного письма выполняется на компьютер отправителя и раскодирование только на компьютере получателя, а его пересылка по Сети, включая хранение на промежуточных серверах, происходит в закодированном виде.

Спасибо за внимание