Безопасность, данная нам в реальности

текст Вячеслав Медведев, ведущий аналитик отдела развития ООО «Доктор Веб»

Документы регуляторов справедливо требуют использования средств защиты, в том числе антивирусных решений, на стороне финансовых организаций и их клиентов. Но практика показывает, что, выбрав необходимое решение, установив и настроив его, банки и их клиенты не получают желаемого уровня безопасности. Почему? Попробуем рассмотреть некоторые причины.

Откроем Письмо Банка России от 24.03.2014 № 49-Т «О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности»:

2.1.14. Осуществление фильтрации ВК во всех сообщениях электронной почты кредитной организации (применение защитных почтовых шлюзов).

Абсолютно правильное, но в итоге не приводящее к необходимому результату требование. Наиболее опасное вредоносное ПО в ходе разработки тестируется на необнаружение всеми популярными антивирусами. В результате сканирование на вредоносное ПО ничего не даст, вирус или троянец доберется до рабочей станции. Что из этого следует?

К сожалению, компании часто пренебрегают использованием антивируса на почтовых серверах — то же Письмо № 49-Т рекомендует размещать систему фильтрации на почтовых шлюзах. Это происходит, поскольку многие ошибочно считают, что возможности серверного антивируса по защите от вирусов и спама и антивируса для рабочих станций аналогичны. Естественно, это не так, но не это главное. Антивирус для почтовых серверов может сканировать уже полученные сообщения в почтовых базах на ранее неизвестные угрозы, а антивирусы для рабочих станций и шлюзовых решений — нет.

А вот фильтрацию на шлюзе нужно осуществлять не только на вредоносные файлы, но и на подозрительные источники информации. Например, Dr.Web Gateway Security Suite обеспечивает проверку подлинности IP-адреса отправителей и получателей, проверку корректности SMTP-сессии, фильтрацию по заданным правилам и многое другое. В результате вероятность того, что письмо или файл от злоумышленника дойдет до сотрудника, существенно снижается.

Оптимальным является сочетание шлюзового решения, фильтрующего почтовый трафик компании на входе и выходе, и почтового сервера, размещаемого во внутренней сети компании и осуществляющего проверку на ранее неизвестные вредоносные программы — при обращении к конкретному почтовому сообщению или в ходе периодического сканирования почтовых баз.

Но что делать, если фильтрация не помогла, и письмо с вредоносным файлом дошло до получателя? Исключаем наличие неизвестной уязвимости в почтовом клиенте, которое маловероятно. Злоумышленник должен сделать так, чтобы сотрудник компании открыл письмо и (например, но необязательно) запустил вложение. Используемые фишерами приемы социальной инженерии, а также типичные признаки фишинговых писем известны давно. Но насколько эти признаки актуальны?

На первом шаге проверки рекомендуют проверить поле «От» с информацией об отправителе и наличие личного обращения к получателю письма. Считается, что незнание имени и/или должности получателя и отсутствие известного получателю отправителя обычно указывают на спам или фишинг. Обычно это действительно так. Но вспомним недавнюю утечку данных о 300 тыс. владельцев пластиковых карт. Сообщается, что скомпрометированных данных недостаточно для снятия средств. Вполне возможно. Но даже одни только ФИО клиентов вместе с информацией об именах руководящих сотрудников банка позволяют злоумышленникам сформировать письма от имени реально существующих людей конкретным получателям.

Письмо № 49-Т также предписывает:

Изложить требования по защите от ВК клиентских АРМ систем ДБО в договорах (соглашениях), предметом которых является предоставление клиентам услуг ДБО (далее — договоры), а также в эксплуатационной документации на системы ДБО и в памятках, передаваемых клиентам при заключении договоров.

Содержится ли информация о подобных угрозах в договорах с клиентами? Наверное, вопрос философский.

И еще раз процитируем Письмо № 49-Т:

Регулярное проведение обучающих мероприятий и контроля знаний работников кредитной организации по тематике защиты от ВК.

Думаю, всем известна атака на Сбербанк, в ходе которой клиенты банка в панике начали массово снимать свои средства. Готовы ли сотрудники и клиенты финансовых организаций к таким атакам, способны ли они отличать письма злоумышленников в общем потоке сообщений? К сожалению, в Рунете (да и на Западе) крайне мало образовательных программ по фишингу, позволяющих потенциальным жертвам проверить актуальность своих знаний об угрозах, а их рекомендации обычно повторяют друг друга. ВебIQметр от компании «Доктор Веб» — один из немногих проектов, направленных на просвещение пользователей. Для понимания степени уязвимости вашего бизнеса можно пройти, например, SonicWALL Phishing IQ Test, — это позволит реально оценить шансы злоумышленников атаковать вашу компанию.