чего бояться, или в домике ли мы?

безопасность бывает только комплексной, а эффективной она становится, когда при ее создании есть четкое понимание, что может и что не может средство защиты

текст **Софья Мороз**

Новостные ленты 2014 года были переполнены новостями о санкциях, новых требованиях регуляторов, сообщениями о разработке инфекций для систем, традиционно считающихся неуязвимыми. Естественно, это вызвало интерес заказчиков к применению новых для них средств защиты. Но изменило ли это ситуацию с безопасностью в финансовых учреждениях?

Прошедший год был ознаменован ростом интереса злоумышленников к банкоматам. Появились новые троянские программы (те же Trojan.Skimer.19 и Trojan.PWS.OSMP.21). «Управление К», входящее в состав БСТМ, отчиталось о выявлении ботсети, ориентированной на хищение денег со счетов российского банка (по словам начальника БСТМ МВД Алексея Мошкова, используемая для создания ботнета программа давала возможность скрытно отправлять и принимать управляющие SMS-сообщения системы мобильного банкинга, что позволяло ей узнавать баланс на счетах и осуществлять несанкционированные переводы). Скимминг перешел на промышленные рельсы: применяемые сейчас скиммеры помещаются в антискимминговые устройства.

Естественно, это не могло не привлечь внимания регуляторов и финансовых учреждений. Для последних это выразилось ростом интереса к системам защиты банкоматов (к сожалению, аналогичного роста интереса к защите терминалов пока не отмечено). Но само по себе внимание клиента, увы, не означает, что защита будет реализована. Даже не касаясь финансовых вопросов и трудностей внедрения, возникший интерес сразу стали эксплуатировать поставщики, решениями которых невозможно ни закрыть проблемы безопасности, ни выполнить требования регуляторов.

Несмотря на то что в Положении Банка России № 382-П и PCI DSS четко прописаны требования по использованию антивирусных средств защиты, многие клиенты, введенные в заблуждение умелыми толкователями имеющихся требований, не только не подозревают об этом, но и отрицают сам факт упоминаний антивирусных средств в этих документах. Во многих случаях выдержки из пятого требования PCI DSS для них становятся открытием. Часто вместо антивирусов заказчикам предлагаются средства контроля целостности, не обеспечивающие ни антивирусной проверки до внедрения новых приложений, ни защиты от ранее неизвестных угроз. Только антивирусные средства, имеющие возможности по лечению активных инфекций, могут помочь тем, на кого ведется целевая (APT) атака.

Еще одной проблемой, не позволяющей снизить финансовые потери, была, есть и, к сожалению, продолжает оставаться безграмотность как клиентов, так и отдельных пользователей. Даже если пользователи замечают новую информацию об угрозах, далеко не факт, что она будет понята так, как нужно. Так, рост упоминаний банкоматных троянцев в СМИ автоматически привел к тому, что пользователи стали считать, что вероятность потерять деньги связана только с ними – возможность расстаться со средствами по результатам деятельности скиммеров, по их мнению, отошла на второй план. При этом 21% считает, что для защиты от Trojan.Skimmer достаточно удостовериться, что банкомат не оборудован замаскированной видеокамерой или накладкой на считыватель банковских карт, а 47% уверены, что для защиты необходимо установить антивирусное ПО непосредственно в чип банковской карты. Это возвращает нас к документам регуляторов, которые требуют от организаций работы и со своим персоналом, и со своими клиентами в целях увеличения их знаний в области защиты.

Безопасность бывает только комплексной, а эффективной она становится, когда при ее создании есть четкое понимание, что может и что не может средство защиты. Игнорирование защиты своего персонала, его безграмотность зачастую становятся причиной падения даже, казалось бы, непробиваемой защиты.