знания, усиливающие защиту

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

Откуда мы получаем информацию, когда принимаем решения при построении системы антивирусной безопасности? Как правило, из новостей о вирусных инцидентах и об успехах в поимке преступников, из сообщений исследователей о возможностях взлома и отчетов организаций, занимающихся информационной безопасностью, из требований регуляторов. Проблема, как представляется, в инертности системы и вопросах, связанных с особенностями восприятия информации на психологическом уровне.

Особенность человеческой психики заключается в том, что отдельные, но яркие факты затмевают общую статистику. Мало кто боится ездить на автомобиле, но большинство опасается летать на самолетах, хотя статистика говорит, что авиаперелеты безопаснее.

Так же и в сфере информационной безопасности. В результате демонстрации новых, впечатляющих угроз зачастую остается в тени тот факт, что реализация этих угроз на практике крайне редка. Когда появляются новости о новейших троянцах, за бортом остается статистика отлаженного выпуска вредоносных приложений известной, но неуловимой группировкой, создающей по сто новых троянцев в день, ни один из которых не обнаруживается антивирусом.

Казалось бы, кому как ни банкам знать, почему их клиенты или они сами теряют деньги – тем более в условиях требований закона «О национальной платежной системе», когда приходится вкладывать вполне реальные (и немаленькие) средства для минимизации своих потерь. Имеется статистика количества атак различных типов, уровня уязвимости используемых приложений и сервисов. Имеется, наконец, статистика эффективности мер защиты, в том числе представленная на Межбанковском форуме в Магнитогорске. Казалось бы, есть все, что необходимо для создания эффективной системы безопасности, тем не менее количество ошибок в построенных системах крайне велико.

Мы традиционно со скепсисом относимся к инициативам правительства о создании чего-либо и зачастую оказываемся правы в своих сомнениях относительно нужности или актуальности этих инициатив. Но одна из них заслуживала лучшей доли – идея построения системы информирования. Проблема большинства документов, регулирующих безопасность (даже если они требуют выполнения действительно нужных вещей), в том, что они создаются на основе устаревшей информации, например, на основе зарубежных стандартов – пусть они тщательно сделаны, но ситуация в ИТ меняется постоянно.

Поэтому для реализации некой цели мало просто озвучить ее, ввести налог с продаж ПО и набрать «научные роты». Во что мы упираемся? В менеджеров проектов и ведущих аналитиков. С. П. Королев в первую очередь был не столько создателем ракеты (хотя, естественно, эту его заслугу отрицать нельзя), выведшей человека в космос, сколько человеком, координировавшим деятельность тысяч людей и десятков предприятий.

А пока для получения информации нужно опираться на опыт вендоров. На ряд ключевых вопросов могут ответить только они. Например, почему нужно ставить антивирусную защиту на шлюз, если возможности таких решений не превосходят на порядок функциональность разработок для рабочих станций и файловых серверов? Почему и как на самом деле нужно защищать почтовый сервер, если возможности решений ограничены имеющимся API почтового сервера? Зачем защищать банкоматы антивирусом, если специализированных троянцев для банкоматов единицы, а производители поведенческих анализаторов обещают выполнить все требования регуляторов? Как говорится, об этом и многом другом можно узнать из учебных курсов или напрямую спросив представителей вендора.