Денис ГАСИЛИН:
«Антивирусы – вчерашний день. На повестке дня новые вызовы и новая парадигма ИБ»

Интервью с руководителем отдела маркетинга компании SafenSoft

– За последние годы понятие «проактивной защиты» стало очень популярным. Какой смысл придаете ему вы? В чем его принципиальные отличия от традиционной парадигмы, заложенной в антивирусных продуктах?

– В основе многих антивирусов продолжают использоваться технологии сигнатурного сравнения, но обнаружить все вредоносные программы этим способом невозможно. Существуют технологии эвристического и поведенческого анализа – они позволяют защитить от значительного количества угроз, но, опять же, не от всех. Каналы связи не являются сдерживавшим фактором, процессоры обладают все большей производительностью, но почему мы не видим взрывного роста производительности на конечных устройствах? Давно ходят разговоры о возможности снабдить компьютер дополнительным процессором, который бы выполнял только функции антивирусных программ. Но пока этого нет, мы наблюдаем снижение производительности компьютера при постоянном наращивании его технических характеристик. Более того, явные акценты на таргетированность атак минимизируют эффективность защитных комплексов. В случае использования злоумышленниками новых угроз сигнатурные базы не успеют обновиться, а эвристики с поведенческим анализом не обеспечат должного качества защиты. Проактивная защита, в свою очередь, работает по совершенно иному принципу – мы фокусируемся на защите системы от любых изменений, что не требует ни обновления вирусных баз, ни постоянного сканирования системы с целью обнаружения заражения.

– Технология, предлагая вашей компанией, V.I.P.O. – это, в первую очередь, технология контроля приложений. В чем ее уникальность? Какие ноу-хау, заложены в ней?

– Особенность нашего подхода к контролю приложений и исполняемых модулей заключается в принципе «белых списков». Автоматически собирающийся профиль системы, который можно впоследствии настраивать вручную, определяет заведомо доверенные приложения, а все используемое впоследствии программное обеспечение работает по принципу «что не разрешено, то запрещено» или не работает вообще, если предпринимается попытка несанкционированного воздействия на систему. Все доверенные приложения тоже доступны для тонкой настройки доступа к отдельным частям ОС, например, реестру или элементам файловой системы. Это делается с целью предотвратить вредоносное воздействие на систему даже доверенных программами.

– В портфеле копании целый ряд продуктов и платформ. Для противодействия каким рискам ИБ они предназначены? В какой степени пересекается их функционал? В каких конкретных продуктах и каким образом реализован проактивный подход к защите информации?

– Флагманских продуктов два: SafenSoft Enterprise Suite используется в коммерческих и государственных учреждениях, а SafenSoft TPSecure – в банках и кредитно-финансовых кооперативах. Благодаря модульности конструкции наших продуктов для каждого конкретного заказчика можно собрать отвечающий именно его требованиям продукт. Например, SafenSoft Enterprise Suite Plus дополнительно включает в себя антивирусный модуль с вирусными базами от сотрудничающих с нами антивирусных компаний, а SafenSoft Enterprise Suite Server «заточен» исключительно под защиту корпоративных серверов. Также есть возможность выбрать разные типы удаленного администрирования системы.

– В каких сегментах отечественного рынка ваши решения пользуются наибольшим спросом? Какие продукты наиболее востребованы?

– Традиционно наши продукты пользуются наиболее высоким спросом в банках. Кредитно-финансовые организации весьма требовательно относятся к защите своей информации. Кроме того, в их ИТ-инфраструктуре – большое количество разнотипных элементов, а для успешной кибератаки зачастую достаточно лишь одного плохо защищенного звена цепи. Мы предлагаем решения для всех элементов такой инфраструктуры, от центральных серверов до банкоматов и рабочих мест операционистов. Кроме того, SafenSoft TPSecure – уникальный продукт, поскольку разработчики решений уделяли мало внимания защите устройств самообслуживания. Мы же успели накопить действительно уникальный опыт в этой области, а значит, альтернатив нашему продукту в этой нише нет. ■