Рис. 2

Угрозой безопасности компании являются и мобильные устройства сотрудников

ограничения доступа к заведомо вредоносным ресурсам, файлам и папкам и возможности запуска неизвестных программ. Даже если некая программа пошла проверку антивирусным ядром, она не должна запуститься. Задача антивируса (в выполнении которой его ничто не может заменить) – обнаружение ранее неизвестных, уже запущенных вредоносных программ. Никакие иные средства, кроме антивируса, не могут в автоматическом режиме удалить активную угрозу. Правда, и тут есть проблема…

Защита мобильных устройств

Мобильные устройства сотрудников и раньше представляли собой проблему безопасности. Подмена SMS-подтверждений от банков, контроль за переговорами и местоположением владельца аппарата – мобильные устройства всегда давали много возможностей злоумышленникам. Но до 2015 г. со всеми этими угрозами мог справиться антивирус – лишь бы пользователь его не отключил. В 2015 г. в десятку самых популярных вредоносных программ вошли троянцы, устанавливающиеся в системные области и имеющие Root-права. Тут надо пояснить, что в отличие от других операционных систем на Android антивирусы работают не с системными правами, а с правами обычных программ. В результате для лечения таких угроз нужно было разблокировать устройство для получения Root-прав. Обнаруживалась угроза и без наличия Root-прав. А вот в 2016 г. троянец Loki смог попасть в системную область, куда антивирусу доступа уже нет (спасибо корпорации, создавшей ОС, в которой работа вирусов должна быть невозможна, а антивирусы не нужны). И для устранения проблемы устройство можно только перепрошить.

На данный момент сложилась ситуация, в которой пользователи с зараженными устройствами имеют доступ к серверам и сервисам компании – и ни один антивирус не может ничего поделать. Хотя не совсем так – тут самое время разобраться еще с одним мифом.

Рис. 3

Не стоит доверять защите данных на облачном сервере, размещенном за пределами периметра компании и обслуживаемом не ее специалистами

Проверка трафика

Если антивирусная защита рабочих станций осуществляется почти всеми, а файловых серверов – большинством, то количество компаний, устанавливающих проверку трафика на шлюзах и почтовых серверах, невелико – традиционно считается, что этот функционал дублирует функционал, имеющийся на рабочих станциях. На самом деле назначение серверных продуктов совсем иное.

Почтовый антивирус нужен для проверки ранее полученных писем в поисках ранее неизвестных угроз. Клиент компании или ее сотрудник, присоединившись к серверу, не должен получить ранее неизвестное вредоносное вложение или ранее не определявшийся спам. Проверка трафика, в свою очередь, должна защитить от получения вредоносных программ те устройства и компьютеры, установка антивирусной защиты на которые невозможна или не контролируется. Именно поэтому весь входящий и исходящий трафик мобильных устройств и домашних компьютеров сотрудников (если их защита не включена в центр управления антивирусной защиты компании) должен проходить через шлюз.

Данные на облачном сервере

И не забываем об облаках. Использование облачных сервисов бывает оправданно. Неоправданно – доверять защите данных на сервере, размещенном за пределами защищенного периметра компании и обслуживаемом не ее специалистами (все еще помнят взлом одного из серверов Tor). Поэтому, кроме защиты серверов, размещенных на удаленной площадке, весь трафик должен проверяться при получении, и это тоже выполняется на шлюзовом решении.

Сохранность резервных копий

Еще одно частое заблуждение связано с резервными копиями, которые считаются защитой от заражений. К несчастью для полагающихся только на резервные копии, современные вредоносные программы определенных типов рассчитаны на длительное и незаметное пребывание на рабочих станциях и серверах и, соответственно, попадают на резервные копии. В итоге ситуация, когда все имеющиеся резервные копии заражены, вполне реальна. ■