Антивирусная защита серверов: мифы и реальность

Середина февраля 2016 г. прошла под знаком обсуждения планов ФСТЭК России по выпуску новых, действительно важных и не первый год ожидаемых документов. Новые приказы и методические рекомендации должны появиться уже вот-вот. Правда, радость омрачается воспоминанием, что и в прошлом (и позапрошлом) году нам обещали много "вкусного" – но не сложилось. Так что ждем… Однако никакие документы сами по себе обеспечить защиту не могут. Действующие приказы ФСТЭК России № 17 и 31 довольно неплохие – перечисленных в них мер защиты вполне достаточно для обеспечения безопасности компании любого размера. Но почему же ситуация с вирусами/утечками/вымогательством не становится лучше?

Вячеслав Медведев
Ведущий аналитик отдела развития,
ООО "Доктор Веб"

Причин создавшейся ситуации с вирусами/утечками/вымогательством много – от засилья мифов среди тех, кто отвечает за антивирусную безопасность (от простых пользователей, обеспокоенных защитой своих домашних компьютеров и личных устройств, и до ИТ-профессионалов, отвечающих за комплексную безопасность компаний и организаций), и до невозможности закупки всего необходимого для обеспечения защиты. Охватить все проблемы невозможно, рассмотрим лишь некоторые.

Зачем нужен антивирус?

Первое и основное – для чего нужен антивирус? Кажется, глупый и детский вопрос, но попытайтесь ответить на него лично для себя. Типичных ответов несколько. Если отбросить варианты "Ставят все" и "Требуют регуляторы", то, как правило, ответ сводится к тому, что антивирус "должен ловить все поступающие в компанию вирусы". А это принципиально неверно и даже теоретически недостижимо!

Не меньший разброд царит в терминологии, связанной с антивирусной защитой. В итоге до сих пор встречаются рекомендации о необходимости установки, помимо антивируса, решений типа антиспуваре, антируткит и т.д. и т.п. По сути, этого не требуется – антивирус ловит все типы вредоносных файлов, никакое дополнительное ПО в добавление к антивирусу не нужно. Более того, поскольку наиболее правильное определение вредоносных файлов – "программы, функционал которых отличается от обещанного пользователю (вспоминаем фишинг и набивших оскомину троянцев для Android), а также файлы, установка и запуск которых не разрешены пользователем", то современные антивирусы могут не только перекрывать кислород известным антивирусному ядру вирусам, но и ограничивать запуск на компьютере всем программам, кроме разрешенных пользователем (к слову, на самом деле, это очень непростая задача).

Обнаружение неизвестных угроз

И сразу об известности вредоносных программ антивирусу. Подавляющее большинство пользователей считает, что антивирус должен знать все вредоносные программы ("а что тут странного – они же ими и пишутся"). В реальности, вопреки всем мифам, антивирус может определять только те вредоносные программы, которые могут перехватываться с помощью используемых технологий антивируса (как бы ни была хороша вирусная база, вирус сначала нужно поймать) и сигнатуры и процедуры для обнаружения которых вошли в вирусную базу (а значит, образцы уже попали ранее в антивирусную лабораторию). Похожий миф гласит, что эвристические механизмы могут определять неизвестные программы. Частично это действительно так, но только частично. С помощью эвристических механизмов можно определять вредоносные программы только известных типов, то есть антивирус может находить только угрозы,

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.

подобные ранее обнаруженным (есть, правда, одно исключение, но о нем ниже). Соответственно, если антивирус используется в качестве средства, предотвращающего попадание вредоносных программ на компьютер, устройство или сеть, то он бессилен против вредоносных программ, протестированных злоумышленниками на необнаружение на актуальных версиях продукта (точнее, продукта, установленного по умолчанию, – это крайне важно, так как большинство не использует входящие в состав антивирусов средства офисного контроля, существенно снижающие риск проникновения неизвестных программ).

Но вернемся к неизвестным угрозам. Именно благодаря тому, что для защиты используется только антивирус, установленный по умолчанию, шифровальщики могут беспрепятственно пополнять кошельки злоумышленников. Для антивирусной защиты нужно использовать не только антивирус, а комплекс средств – систему

Рис. 1

Современные антивирусы могут блокировать работу не только вредоносных файлов, но и всех программ на компьютере, кроме разрешенных пользователям