PCWEEK RUSSIAN EDITION REVIEW
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И РЕШЕНИЯ ДЛЯ БИЗНЕСА
ИТ-БЕЗОПАСНОСТЬ
НОЯБРЬ • 2012 • МОСКВА
http://www.pcweek.ru

Защита конечных точек в современных условиях

ВАЛЕРИЙ ВАСИЛЬЕВ

Согласно данным компании Gartner, объем рынка систем защиты конечных точек (Endpoint Protection Platform, EPP) составил в 2011 г. более 3,2 млрд. долл. В нынешнем году, по прогнозам этой компании, он вырастет на 5—7%.Большая часть этого объема приходится на антивирусные продукты, которые относятся к основным средствам защиты конечных точек и в настоящее время представляют собой комплексные системы, совмещающие в себе многоуровневую защиту от вредоносных программ, защиту от спама, межсетевое экранирование, защиту от внешних вторжений.

ОБЗОРЫ

Другим компонентом системы защиты конечных точек являются агентские решения, устанавливаемые на конечные точки и контролирующие исполнение принятых в компании политик информационной безопасности (ИБ). Среди них в самостоятельную группу выделились системы, называемые Network Access Protection (NAP) или Network Access Control (NAC).

Важным звеном в защите конечных точек стали системы управления доступом (Identity management, IDM). IDM-системы повышают защищенность конечных точек от несанкционированного использования за счет автоматизации управления доступом, реализации многофакторной аутентификации, автоматизированного управления учетными записями пользователей, а также благодаря возможности организовать правильное с позиции ИБ-политик подключение мобильных устройств к корпоративным ресурсам.

Все чаще системы защиты конечных точек стали включаться в единую систему обеспечения корпоративной ИБ, предоставляя содержащимся в ней средствам анализа и корреляции ИБ-событий информацию о состоянии конечных точек, в том числе о действиях пользователей и корреляции событий ИБ с целью выявления аномалий и комбинаций, представляющих ИБ-угрозы.

Согласно данным исследовательских компаний, в целом на обеспечение ИБ конечных точек сегодня расходуется примерно половина корпоративных ИБ-бюджетов. Объяснить такое распределение в расходах предприятий и организаций на ИБ можно тем, что в сегменте конечных точек, обеспечивающих пользовательский доступ к корпоративным ИТ-ресурсам, в настоящее время происходят существенные изменения. В настоящем обзоре мы постараемся выявить суть этих изменений и определить их влияние на состояние корпоративной ИБ.

Факторы воздействия

Изменения, происходящие в организации потребления корпоративных ИТ-ресурсов, среди которых прежде всего следует отметить консьюмеризацию корпоративных ИТ-инструментов, расширение спектра используемых в офисах устройств доступа (в том числе за счет реализации программы "принеси свое собственное устройство", BYOD), а также выход пользователей за традиционный периметр защиты (что связано с ростом популярности работы вне офиса, мобильностью персонала и распространением публичных облачных ИТ-сервисов, предназначенных для поддержки совместной работы), обусловливают необходимость пересмотра подходов к построению защиты конечных точек, обеспечивающих доступ пользователей к корпоративным ИТ-ресурсам.

По мнению руководителя отдела специальных проектов компании "Аквариус" Сергея Лышенко, каждое подключение мобильной конечной точки к корпоративной сети должно восприниматься как подключение недоверенного ресурса. Восстановление доверенных отношений с нею сопряжено с выполнением требований, гарантирующих, как он формулирует, "стерильность" подключаемого ресурса. Это значительно усложняет процесс аутентификации, обязывает добавлять в набор средств защиты информации (СЗИ) новые агенты систем обнаружения атак, способных собирать информацию о том, что происходит с мобильным устройством доступа даже тогда, когда оно не подключено к корпоративной сети, а затем, при его возвращении в сеть, передавать информацию на сервер обработки и анализа ИБ-событий.

К актуальным факторам воздействия на подходы к построению защиты конечных точек аналитик компании "Доктор Веб" Вячеслав Медведев добавляет необходимость соблюдения требований законодательства, в частности по защите персональных данных, сохраняющую особую актуальность из-за продолжающейся на протяжении нескольких лет чрезвычайной несогласованности действий госрегуляторов с предложениями экспертного ИБ-сообщества.

Со своей стороны, генеральный директор компании "Аванпост" Андрей Конусов добавляет к движителям развития рынка защиты конечных точек развивающуюся в российской корпоративной среде практику юридического противодействия компьютерным преступлениям. Это направление, относящееся прежде всего к организационным способам обеспечения ИБ, предполагает взаимодействие компаний с правоохранительными органами как напрямую, так и через посредников — провайдеров услуг по расследованию преступлений в компьютерной среде.

Изменения в функциональном составе

Следует помнить, что и в условиях масштабных изменений, происходящих в современных ИТ, основные задачи защиты конечных точек, поддерживающих пользовательский доступ к корпоративным ИТ-ресурсам, по своей сути остаются прежними. Они включают обеспечение каждому сотруднику бесперебойного доступа лишь к тем ресурсам, которые предписаны ему бизнес-ролью, только при выполнении условий, предусмотренных политиками безопасности (определяющими время и место подключения, тип устройства подключения и установленные на нем СЗИ, разрешенный набор и обновление ПО, каналы доступа).

Решение этих задач направлено на минимизацию вероятности таких ИБ-угроз, как несанкционированные действия с данными, атаки на канал передачи информации между централизованными ресурсами и конечной точкой, авторизация другого человека под именем легитимного пользователя. Используемые для этого средства защиты хорошо известны. Это антивирусы, средства аутентификации (скажем, электронная подпись), средства защиты канала (например, VPN). Для мобильных точек доступа дополнительно потребуется установить средства криптографической защиты данных, располагающихся на носителях информации (прежде всего на съемных — например, флэшках), и персональный межсетевой экран.

Как полагает специалист департамента внедрения и консалтинга компании LETA Максим Максимов, перед разработчиками ИБ-продуктов сегодня стоит задача перенести необходимый функциональный набор средств защиты информации, традиционный для стационарных точек доступа, на мобильные устройства. При этом подразделениям ИБ предстоит отыскать золотую середину между обеспечением ИБ и правом пользователя распоряжаться своим устройством как личным.

Руководитель отдела ИТ компании "Аладдин Р.Д." Леонид Корох предупреждает, что, если в компании реализуется программа BYOD, ее ИБ-служба должна учитывать, что некоторые административные полномочия по управлению устройством доступа могут быть возложены на пользователя. В этом случае ИБ-политики, регламентирующие эксплуатацию таких устройств, следует дополнять организационными требованиями к пользователю-администратору.

По мере все более широкого использования сотрудниками смартфонов и планшетов в бизнес-процессах своих компаний ИБ-службам нужно внимательнее рассматривать возможность внедрения у себя систем Mobile Device Management (MDM). Их функционал "заточен" под решение задач обеспечения безопасности при эксплуатации именно мобильных точек доступа. Количество предложений таких систем на рынке исчисляется сегодня десятками. Отрадно отметить, что наряду с зарубежными разработками появляются и конкурентоспособные отечественные. На эффективность таких систем благотворно влияет то, что разработчики операционных платформ для мобильных устройств охотнее стали публиковать используемые в их продуктах интерфейсы для программных приложений (API). Это облегчает распространение функционала MDM-систем на все более широкий спектр мобильных устройств доступа.

Несмотря на то, что для защиты конечных точек в корпоративной среде существует довольно большой набор продуктов и решений и к тому же среди них есть специализированные, ориентированные на эти задачи системы (такие, например, как упомянутые MDM, NAP, NAC, EPP), организация защиты конечных точек в каждой компании, подчеркивает инженер-консультант по информационной безопасности компании MONT Сергей Ласкин, имеет ярко выраженные индивидуальные особенности. Общим для таких проектов оказывается только цено-

ПРОДОЛЖЕНИЕ НА С. 19 ▸

Наши эксперты

АНДРЕЙ КОНУСОВ, *генеральный директор, "Аванпост"*

ЛЕОНИД КОРОХ, *руководитель отдела ИТ, "Аладдин Р.Д."*

СЕРГЕЙ ЛАСКИН, *инженер-консультант по ИБ, MONT*

СЕРГЕЙ ЛЫШЕНКО, *руководитель отдела специальных проектов, "Аквариус"*

МАКСИМ МАКСИМОВ, *специалист департамента внедрения и консалтинга, LETA*

ДЖАБРАИЛ МАТИЕВ, *руководитель группы по информационной безопасности, IBS Platformix*

ВЯЧЕСЛАВ МЕДВЕДЕВ, *аналитик, "Доктор Веб"*

ОЛЕГ САФРОШКИН, *менеджер по развитию бизнеса, "Информзащита"*

О самом важном из искусств

ВЯЧЕСЛАВ МЕДВЕДЕВ, АНАЛИТИК КОМПАНИИ "ДОКТОР ВЕБ"

— Хуже быть не может, — вздыхает пессимист.

— Ну что вы! Все гораздо хуже, чем вы думаете, — утешает реалист.

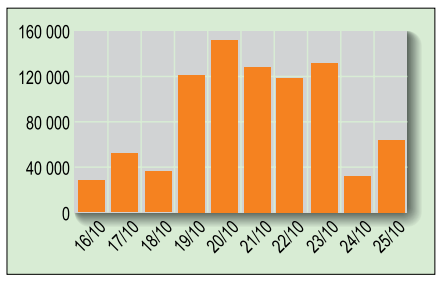
Модификация известного анекдота

В планах ИТ-служб по внедрению и совершенствованию сервисов услуги антивирусной защиты занимают отнюдь не первые строчки. Иногда они не входят даже в первую десятку. ИТ-службы активно интересуются "облачными" системами, защитой от утечек, контролем доступа, управлением правами… Но при этом практически каждая встреча с клиентами антивирусных компаний не обходится без жалоб на проблемы с вирусами и вызванные ими последствия. Почему многие ИТ-подразделения компаний бравурно отчитались перед своим руководством о создании систем защиты от вирусов, но на практике эти системы совсем не так уж надежны?

Причин тому много. Попробуем разобрать основные.

Есть мнение, что "все вирусы пишутся антивирусными компаниями, так как это им выгодно". Отсюда вытекает, что если "антивирусники халяву не давят", то они знают все вирусы всех типов. Все это, однако, далеко от правды.

Заглянув, скажем, на закладку Infected Objects ресурса Dr.Web Virus Analysts Web Site, расположенного по адресу http://live.drweb.com, можно увидеть, что 20 октября 2012 г. был побит очередной рекорд — на анализ поступило 150 тыс. неизвестных вирусов. За один день! И это, естественно, не всё, что было создано вирусописателями. Часть вредоносных файлов не попала в ловушки, так как была написана под конкретную жертву, часть не предназначалась для свободного распространения в сети Интернет и, например, выкладывалась на конкретные взломанные сайты. Причин много, вывод один: ни одна антивирусная компания не знает все угрозы на момент их появления.



Количество новых вирусов, зафиксированных в октябре 2012 г. (по данным Dr.Web Virus Analysts Web Site)

На это обычно возражают: "А эвристики? Мы тут читали тест…". Это подводит нас к иной проблеме. Раньше производителями потока вредоносных файлов были программисты-одиночки — исследователи и дилетанты, но одиночки. Теперь делом правит бизнес. Криминальные системы, занимающиеся вирусами, построены по принципу вполне легальных структур. Четкая организация позволила не только сократить издержки и обеспечить взрывной рост количества выпускаемых вирусов — с этим антивирусные компании могут справиться. Проблема в том, что тестирование выпускаемых вирусов на актуальных версиях антивирусов обеспечивает выпуск только образцов, не обнаруживаемых антивирусами, имеющимися у целевой группы жертв. Тесты эвристиков можно списывать в утиль. Их результаты только вводят в заблуждение — теперь не менее важна скорость реакции на поступающие образцы вирусов и наличие мощной разветвленной системы сбора образцов.

Итак, как минимум от момента поступления неизвестного вируса до момента получения обновления система с большой вероятностью будет заражена. По имеющимся оценкам, для кражи данных достаточно одной-трех минут, тогда как промежуток между обновлениями — порядка часа.

Проблема усугубляется тем, что для большинства компаний антивирусная защита является синонимом антивируса, причем установленного зачастую только на рабочие станции и иногда на файловые серверы. Риски защиты от неизвестных угроз практически неизвестны.

Ситуация требует кардинальной переоценки важности характеристик закупаемого антивируса. Если раньше оценивалась только его способность находить вирусы (а именно на это направлено большинство известных тестов), то сейчас не менее важны и другие качества. Используемое антивирусное решение должно иметь:

- систему самозащиты, не дающую неизвестной вредоносной программе возможность нарушить нормальную работу антивируса до поступления обновления, позволяющего лечить заражение;
- систему автоматического сбора информации для немедленной передачи в антивирусную лабораторию всех необходимых для решения проблемы данных;
- независимые от используемых в операционных системах механизмов средства управления и обновления антивирусного решения, исключающие возможность перехвата системы обновления вредоносной программой, обеспечивающие постоянное соединение защищаемых рабочих станций и серверов с сервером обновлений и максимально быстрое получение обновлений;
- функционал для блокирования не только поступающих (неактивных) вредоносных программ, но и, что гораздо важнее, уже запущенных;
- возможность применения дополнительных (кроме сигнатурных и эвристических) механизмов для обнаружения неизвестных вредоносных программ, в том числе за счет использования серверных систем защиты на уровне почтовых серверов и шлюзов.

Системные администраторы также должны учитывать риск неизвестной угрозы. А потому необходимо:

- исключить возможность работы с ресурсами сети Интернет с той же машины, с которой работают с сервисами компании (особенно с бухгалтерскими системами и системами "Банк — Клиент");
- перейти от защиты только рабочих компьютеров сотрудников к защите всех мест, где так или иначе сотрудники обрабатывают корпоративные данные (в том числе мобильных устройств и домашних компьютеров), и всех узлов сети, включая почтовые серверы и шлюзы. Так, например, внедрение защиты на уровне почтового сервера позволит не только более эффективно фильтровать почтовые сообщения, но и очищать почтовые базы от вирусов, неизвестных на момент заражения, что также исключает их случайную отправку получателю;
- использовать эффективные серверные системы фильтрации почтового и интернет-трафика. Так, защита почтовых серверов Microsoft Exchange должна дополняться проверкой на прокси-серверах, что обеспечивает переход от анализа по составляющим письма к комплексному анализу за счет реализации механизмов, невозможных на сервере Microsoft Exchange.

Только в случае реализации всех вышеописанных мер возможен перелом в борьбе с вирусами.

СПЕЦПРОЕКТ КОМПАНИИ "ДОКТОР ВЕБ"

Защита конечных...

◂ ПРОДОЛЖЕНИЕ СО С. 17

вой фактор: стоимость средств защиты, как он полагает, в любом случае должна быть не больше, чем стоимость информации, подлежащей защите. “Для защиты компьютеров, за которыми работают бухгалтеры, нужно использовать улучшенную аутентификацию, шифрование данных, хорошие антивирусные средства. Возможно, стоит вынести их в отдельную подсеть. Для сотрудников канцелярского отдела защита может быть и слабее — здесь бывает достаточно стандартного разграничения доступа к ресурсам и более дешевого антивируса”, — говорит он.

Характеризуя ситуацию с обеспечением корпоративной ИБ в целом, менеджер по развитию бизнеса компании “Информзащита” Олег Сафрошкин напоминает, что применение ИТ-решений должно быть нацелено на решение задач бизнеса. Обеспечение ИБ при этом отодвигается на второй план. Это должны учитывать также и ИБ-разработчики. Появление новых информационных технологий и включение их в бизнес-процессы предполагает возникновение и новых рисков для безопасности, поскольку средства защиты, ориентированные под эти технологии, выпускаются, как считает г-н Саврошкин, с опозданием. В результате тем, кто в числе первых внедряет новинки, зачастую приходится решать задачи ИБ с помощью подручных средств и прибегая к организационным мерам.

Основные проблемы

Если для конечных точек (ноутбуков, нетбуков, ультрабуков), унифицированных к настоящему времени по аппаратной архитектуре и операционной среде, проблем с выбором средств защиты, можно сказать, нет, то разнообразие и проприетарность (некоторых) платформ для смартфонов и планшетов требуют от разработчиков средств защиты специальных подходов практически для каждого типа этих устройств.

Консьюмеризация информационных технологий, по мнению г-на Лышенко, осложняет задачу производителям СЗИ, поскольку средства защиты должны теперь, с одной стороны, защищать устройство доступа как корпоративный ИТ-ресурс, а с другой — не должны вмешиваться в использование устройства как личного (к примеру, не лишать владельца возможности запускать игровые программы, скачивать и слушать музыку, смотреть фильмы…). Поэтому в СЗИ для мобильных устройств следует предусматривать возможность их эксплуатации в качестве как корпоративных, так и личных.

Сегодня, считает г-н Медведев, на рынке имеется достаточное количество достойных продуктов, с помощью которых можно обеспечить надежную защиту конечных точек от известных угроз (для защиты от неизвестных угроз он рекомендует использовать организационные меры). В то же время мобильные (и домашние) устройства доступа в большинстве своем он оценивает как незащищенные. На данный момент, по его оценкам, именно с них идет большой поток вирусов внутрь корпоративной ИТ-среды. Это указывает на то, что задача безопасного для компании использования мобильного устройства, изначально спроектированного как консьюмерское, последовательно или одновременно в корпоративной и вне корпоративной среды еще не имеет решения, адекватного требованиям корпоративной ИБ.

По мнению руководителя группы по информационной безопасности компании IBS Platformix Джабраила Матиева, разработчики промышленных ИБ-продуктов и ИБ-сервисов не успевают за процессами консьюмеризации корпоративных ИТ, причем их отставание он оценивает как огромное. В оправдание ИБ-вендоров, на его взгляд, можно сказать, что есть такие ИБ-задачи, которые для мобильных платформ пока решить технологически невозможно. Действительно, DLP-система, например, для смартфонов или планшетов все еще тяжела из-за требований к производительности и энергопотреблению устройств.

Защита конечных точек как услуга

Возможность организовать защиту конечных точек доступа как сервис, по мнению г-на Медведева, весьма актуальна, особенно для небольших компаний. Актуализирует сервисный подход в этой области, как он полагает, отсутствие возможности у ИБ-специалистов получать информацию, достаточную для принятия необходимых мер по защите, по причине дефицита таковой на рынке и из-за невысокой средней квалификации “безопасников” в стране, тем более на периферии. В этих условиях удаленно предоставляемые сервисы информационной безопасности, по его словам, нужны как воздух.

Вместе с тем разработчики средств защиты конечных точек, считает г-н Лышенко, должны учитывать то, что российские корпоративные заказчики пока не готовы к переходу на централизованные хранение и обработку информации, в том числе с использованием облачных решений. Поскольку корпоративные данные, которыми оперируют сотрудники, по-прежнему в массе своей хранятся на конечных устройствах, то и средства защиты тоже должны размещаться на устройствах доступа.

Со своей стороны, г-н Медведев приветствует этот консерватизм российских компаний. Он крайне низко оценивает нынешнюю безопасность облачных сервисов, называя ее мифом. По его мнению, перенося сервисы в облака, компании действительно могут улучшить их непрерывность и доступность, но во многих случаях существенно ухудшают при этом их безопасность. В целом, считает он, переход в облако, как правило, требует увеличения затрат на безопасность, чего в сегодняшней практике не наблюдается.

Большой вред корпоративной ИБ, по мнению г-на Медведева, наносят облачные ИБ-сервисы, использующие в своей работе репутационные оценки контента и зараженности интернет-ресурсов. Их сегодня предоставляют многие ИБ-провайдеры. “По сути эти сервисы работают по правилу “миллион леммингов не может ошибаться”. В результате даже если файл или иной ресурс оказывается заражен, а антивирусы еще не обнаружили это заражение, то на основании того, что этот зараженный ресурс используют многие (т. е. многие оказались зараженными, а такое может случиться, например, при взломе популярного информационного сайта), он получает репутацию надежного!” — говорит он.

Тенденции

Г-н Лышенко считает, что популярность движения BYOD стимулировала появление на рынке интересных решений в области защиты информации, в числе которых он называет экосистемы СЗИ (т. е. СЗИ одного семейства, работающие на различных платформах и в гетерогенных сетях); межсетевые экраны нового поколения (предоставляющие возможности глубокого контроля сетевого трафика на уровне приложений и объединяющие с функциями сетевого экранирования функции систем обнаружения вторжений и DLP-систем); системы обнаружения вторжений, способные проводить отложенный анализ действий, осуществляемых с мобильными устройствами; встраиваемые в SIM-карты смартфонов средства криптозащиты.

Защита мобильных устройств, по мнению г-на Короха, останется доминирующим направлением в области обеспечения ИБ конечных точек, предназначенных для доступа к корпоративным ресурсам наряду с интеграцией мобильных устройств с инфраструктурой Virtual Desktop Infrastructure и решениями типа XenClient в целях распространения виртуализации на конечные устройства (что особенно актуально при использовании ноутбуков по программе BYOD). По оценкам г-на Конусова, в 2013—2014 гг. это направление перейдет из фазы первичного ознакомления и анализа возможных вариантов в фазу массовых промышленных внедрений.

Актуальной задачей для обеспечения безопасности конечных точек доступа, полагает г-н Конусов, является контроль и фильтрация исходящего из корпоративной сети голосового трафика. Он отмечает, что на рынке уже появляются первые технологические предложения для этого, и уверен, что в ближайшие годы популярность таких систем и спрос на них будут возрастать.

Как отметил г-н Сафрошкин, разработчики пока не предлагают единого решения, позволяющего одновременно обеспечивать безопасность и централизованно управлять всеми типами точек доступа в компании (т. е. как мобильными устройствами, так и традиционными точками доступа — настольными рабочими станциями и ноутбуками). Однако, по его наблюдениям, работы в этом направлении идут полным ходом, а значит, подобные продукты появятся на рынке в ближайшем будущем.

К важным тенденциям в области защиты конечных точек Джабраил Матиев относит стремление ИБ-вендоров консолидировать ИБ-функционал по возможности в одном решении (например, реализовать в одном программном агенте, устанавливаемом на конечную точку, сразу несколько функций защиты). Кроме того, он также обращает внимание на то, что современные ИБ-решения учитывают рост популярности систем виртуализации и технологий виртуальных рабочих столов (например, их разрабатывают с таким расчетом, чтобы они функционировали на уровне гипервизора, а не на уровне рабочих станций).

В консолидации средств защиты конечных точек и централизации управления ими г-н Конусов усматривает противоречие между целями, которые преследуют с одной стороны вендоры, а с другой — заказчики. Если первые стремятся к реализации у заказчика модели “все из рук одного поставщика”, то в среде заказчиков, по его наблюдениям, мало кто готов и хочет перевести свою инфраструктуру защиты конечных точек на моновендорную платформу. В связи с этим, считает он, вполне вероятно появление в ближайшие годы универсальных консолей управления, позволяющих организовать контроль продуктов защиты конечных точек, предлагаемых разными разработчиками.

Среди нерешенных на сегодняшний день проблем в области защиты конечных точек доступа г-н Лышенко выделяет проблемы сертификации. “Раньше средства защиты создавались с расчетом их эксплуатации на протяжении нескольких лет, и никого особенно не волновала длительность процесса их сертификации. Сегодня же за время, пока новый ИБ-продукт проходит сертификацию, платформа, для которой он предназначался, успевает морально устареть. Это неизбежно стимулирует ускорение процессов сертификации, что является, с одной стороны, позитивной тенденцией. С другой стороны, это ускорение может отрицательно повлиять на качество сертифицируемых решений”, — отмечает он.