Cyren Web Security – безопасность из облака

Обзор функциональности решения Cyren Web Security, используемого по модели "Security-as-a-service" и позволяющего осуществлять защиту персональных компьютеров и мобильных устройст при работе в публичном "облаке".

Михаил Рожнов – ведущий эксперт компании "Сертифицированные информационные системы".

Введение

Сегодня для каждой компании наличие интернет-соединения является настолько обязательным, что может быть сравнимо с необходимостью электричества в офисе. Отсутствие данного элемента блокирует работу компании целиком – нет доступа к почте, информационным ресурсам, порталам, рабочему месту, если вы находитесь вне офиса. Тем не менее, у этой бизнес функции есть две стороны: она может не только повысить производительность компании, но и остановить работу.

Любая интернет-атака – случайная ссылка или интересное вложение – парализует компанию и создает массу головоломок для отдела информационной безопасности. С появлением первых вирусов стали разрабатываться и средства для борьбы с ними. Усложнялось понятие вредоносного программного обеспечения, усложнялись и средства борьбы с ними, которые стали появляться как на границе периметра, так и на конечных рабочих станциях. Все это повлекло, в свою очередь, усложнение экосистемы в целом.

Эта тенденция продолжалась до момента старта облачных технологий. Все началось с того: «а зачем мне разворачивать это приложение у себя внутри компании, если я могу им воспользоваться как готовым сервисом»; или: «а зачем мне приобретать сервер для развертывания системы, если я могу взять его в аренду». Такие технологии, как IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service), SaaS (Software-as-a-Service) уже давно вошли в IT-обиход и имеют практическую реализацию. При этом они не исключают применение технологий и в сфере защиты информации. На российском рынке данное понятие пока новое, однако, на зарубежном рынке оно уже используется совместно с технологиями As-a-service. SECaaS (Security-as-a-service) – бизнес модель, в которой сервис-провайдер интегрирует свои услуги безопасности в корпоративной инфраструктуре на основе подписки. При этом достигаются такие показатели как:

- *реализация заявленных функций безопасности;*
- *повышение отказоустойчивости;*
- *снижение себестоимости владения (TCO);*
- *отсутствие необходимости проведения обучения на низком инженерном уровне;*
- *наличие только операционных затрат – OPEX модель.*

В совокупности это дает возможность осуществлять замену решений, требующих инсталляцию внутри компании.

Cyren Web Security – безопасность из облака

Одним из ведущих игроков на рынке облачных сервисов по информационной безопасности является компания CYREN – вендор, предоставляющий спектр сервисов под общим названием Web Security для организации безопасного серфинга в сети Интернет. В этот сервис включается URL-фильтрация (построение списка IP-репутаций), а также антивирусная защита конечных пользователей (контроль загружаемых объектов на наличие вредоносного кода или фильтрация по типу загружаемых файлов).

Архитектура решения настолько гибкая, что не требует внесения изменений в уже существующую архитектуру. Большая часть работы в интернете осуществляется через браузер. Для того чтобы субъект был привязан к некоторой политике, ограничивающей доступ к запрещенным сайтам, необходимо на рабочих станциях распространить конфигурационный файл прокси-сервера (PAC-файл) облачного сервис-провайдера. Скачав данный файл, его можно распространить на машинах через групповые политики, доступные в среде Microsoft Windows Server, для конфигурирования браузера Internet Explorer. Если в компании используется браузер Chrome, то, выставив настройки для Internet Explorer, их можно автоматически распространить и на Chrome. При условии использования браузера FireFox настройки задаются через указание URL-адреса PAC-файла.

Стоит также отметить, что решение умеет работать и с защищенным протоколом HTTPS. Многие веб-сайты используют данный протокол для предоставления защищенного механизма аутентификации и защиты от атак Man-in-the-middle. Решение предоставляет администраторам возможность активации контроля защищенного трафика. В случае отключения данной опции сервис будет инспектировать IP/домен, содержащийся в запросе, основываясь только на категоризации запроса к оригинальному сайту. Однако инспектирование самого контента осуществляться не будет. В случае же активации опции сервис будет работать в следующей последовательности:

- прерывать запрос на соединение;
- расшифровывать трафик;
- инспектировать для подтверждения соответствия требованиям установленных политик, в случае несоответствия – блокировать трафик;
- осуществлять повторное шифрование трафика и разрешать его для конечного пользователя – в случае соответствия URL-запроса политикам.

Сервис использует самоподписанный корневой сертификат. Для каждого запроса, сделанного пользователем, порождаются две отдельные SSL-сессии: первая – между клиентом и сервисом Web Security, вторая – между прокси Web Security и сайтом назначения. Web Security сервис выполняет верификацию SSL-сертификата для проверки корректности всех сертификатов в цепочке. Данная проверка включает в себя:

- гарантию того, что нет несовпадений между корневым сертификатом и доменным именем обрабатываемого сайта;
- подтверждение того, что сертификат был издан доверенным удостоверяющим центром;
- проверку валидности срока действия сертификата;
- проверку, что сертификат не попадает в список отозванных;

– корневой SSL-сертификат должен быть распределен и импортирован на всех конечных узлах для корректной работы в браузере. Данная операция может быть выполнена либо вручную (конечный пользователь получает почтовое сообщение со ссылкой на импорт сертификата), либо за счет использования групповых политик.

Таким образом, применение сервиса позволит работать не только с открытым трафиком, но и трафиком, инкапсулированным в SSL, без потери свойств защиты данного протокола.

Также необходимо отметить, что решение позволяет осуществлять работу не только с персональными компьютерами, но и мобильными устройствами (рис. 1). Такие технологии как BYOD (Bring Your Own Device) и COPE (Corporate-Owned, Personally Enabled) уже не являются новинкой на рынке информационных технологий даже в корпоративном секторе. В связи с этим сервис уже поддерживает работу с платформами Android и iOS. При использовании мобильной платформы Android на устройство производится инсталляция программного модуля, обеспечивающего VPN-канал с сервис-провайдером. Таким образом, весь трафик «заворачивается» в туннель и проходит через прокси-сервис провайдера. При использовании мобильной платформы iOS конфигурирование осуществляется через настройку прокси-сервера. В обоих случаях конфигурирование должно осуществляться через MDM (Mobile Device Management).

Со стороны администратора настройка выглядит очень просто. Существует веб-консоль, которая позволяет заводить или синхронизировать из Active Directory пользователей, которые будут контролироваться политиками сервиса. Далее на основании предустановленных шаблонов осуществляется детальная настройка политик. После распространения файла с настройками прокси-сервера (вручную или через групповые политики) сервис готов к использованию. Теперь администратор только осуществляет контроль за действиями пользователей, получая наглядные отчеты в консоли управления.

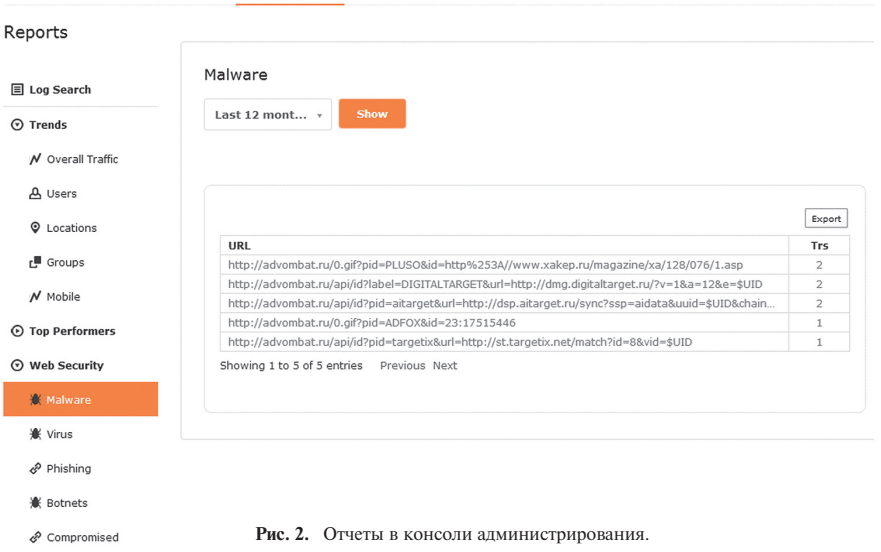

Рис. 2. Отчеты в консоли администрирования.

Со стороны пользователей критических изменений также не происходит. Новые сервисы иногда пугают тем, что требуют проведения дополнительного обучения для персонала перед вводом системы в эксплуатацию. Здесь же для пользователя все прозрачно – получив ссылку на активацию сервиса для учетной записи, субъект определяет пароль и аутентифицируется для начала работы.

При использовании данного сервиса компания получает:

– *URL-filtering* – фильтрация URL-запросов по категориям на основании IP-адресов, доменных имен, контекста, содержащегося в запросе;
– *Anti-Malware Scanning* – фильтрация и блокировка веб-ресурсов, содержащих вредоносное программное обеспечение;
– *Web Security* – фильтрация веб-сайтов на принадлежность к одной из категорий: вредоносный сайт, фишинговый сайт, фрод-сайт, ботнет;
– *SafeSearch* – исключается «взрослый» контент при организации поиска в системах Google, YouTube, Yahoo, Bing и им подобным.

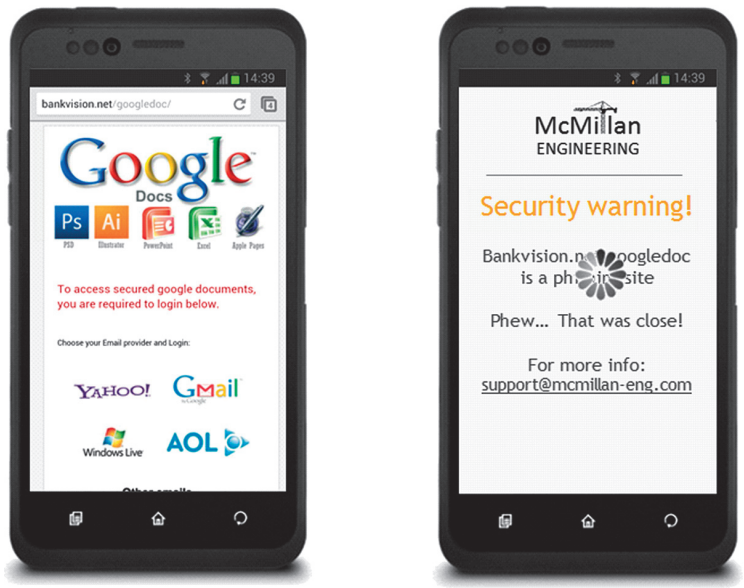

Рис. 1. Защита мобильных пользователей.

Заключение

SECaaS – это технология «завтрашнего» дня. Сервис по безопасности – это то, что позволяет сохранять высокий уровень защиты при условии минимальных вложений, высокий уровень отказоустойчивости при минимальных задержках с развертыванием. Это защита в один клик мышки, и мы надеемся, что российский рынок готов принять данную бизнес-модель уже сегодня.

Михаил Рожнов,
компания "Сертифицированные информационные системы".

Многофакторная аутентификация – теперь требование ФСТЭК

Июнь 2014 г. – В начале года ФСТЭК утвердила методический документ о мерах защиты информации в государственных информационных системах. Документ прояснил многие аспекты, касающиеся организационных и технических мер защиты информации, принимаемые в государственных информационных системах, в соответствии с утвержденным приказом ФСТЭК России от 11февраля 2013 г. No17.

ФСТЭК настоятельно рекомендует полностью отказаться от привычной аутентификации на основе статических паролей для всех пользователей без исключения и перейти к более надежной многофакторной аутентификации. Обязательными требованиями для многофакторной аутентификации являются использование аппаратных аутентификаторов и механизма одноразовых паролей при удаленном и локальном доступе.

Компания SafeNet – крупнейший производитель программного обеспечения средств защиты аутентификации имеет в своем арсенале такие продукты как SafeNet Authentication Manager и SafeNet Authentication Service, прошедшие сертификацию ФСТЭК. Эти решения дают возможность применить механизм двух-

(продолжение – стр. 8)