персональные данные персональные данные персона № 3 (44), март 2012 данные
Информационно-аналитический журнал для операторов персональных данных

«Меры и средства защиты персональных данных»

Обеспечение защиты персональных данных программными средствами для «облачных» решений на базе мировых практик

В настоящее время идет много дискуссий вокруг практической реализации Федерального закона «О персональных данных» (далее – ФЗ-152, Закон). В этих дискуссиях рождается практика применения этого нормативного правового акта предприятиями и организациями, которые должны обеспечить сохранность и безопасность персональных данных своих клиентов.

Эти дискуссии активно продолжатся около двух лет, но ясного и точного понимания, как должны строиться информационные системы предприятий, чтобы удовлетворить требованиям вышеназванного закона и в тоже время обеспечить высокий уровень безопасности данных, пока нет. Еще больше вопросов возникает при реализации своих проектов информатизации инфраструктуры на базе «облачных» технологий. Хочется обратить внимание, что аналогичные законы и инструкции существуют во всех развитых странах мира уже достаточно долго, и за десятилетия их правоприменения сложилась устойчивая практика обеспечения требований к информационным системам по защите и безопасности хранящихся и обрабатываемых в них данных. Мы бы хотели поделиться реальным опытом обеспечения безопасности облачных структур наших клиентов, в тоим числе и с точки зрения законов США по защите персональных данных.

Законы США PII, PCI DSS, HIPAA , Sarbanes–Oxley Act и ряд других требуют от программных продуктов, используемых при обработке и хранении персональных данных, соблюдения следующих положений:

1. Обеспечение защиты персональных данных путем шифрования, контроля доступа и адекватной аутентификации пользователей.
2. Ведение расширенного журнала аутентификации для целей аудита в соответствии с Актом Sorbanes Oxley.
3. Защита финансовых транзакций в соответствии с PCI-DSS. В том числе: управление межсетевыми экранами, защита хранения данных, обеспечение работы и регулярного обновления антивирусной защиты, разграничение прав доступа, контроль и защита идентификаторов, инструменты контроля политики безопасности и ряд других требований.

В среде специалистов и консультантов IT, которые работают в России над проектами по реализации соответствия существующей и планируемой информационной инфраструктуры положениям закона «О персональных данных», сложилось мнение, что достаточно провести формальные мероприятия, которые позволят выполнить основные положения этого закона, такие как, например, сертификация программных и аппаратных продуктов в уполномоченных органах. Это требование, конечно, необходимое, но недостаточное для реального обеспечения защиты персональных данных. Поэтому при выборе продуктов, которые Вы планируете использовать, нужно отдавать приоритет тем, которые, помимо удовлетворения формальным требованиям закона, имеют механизмы, обеспечивающие полноценную защиту ПД клиентов. Практика правоприменения ФЗ-152, в том числе и негативная, накапливается годами, а решения по реализации проектов нужно принимать сегодня. Поэтому хотелось, чтобы операторы персональных данных понимали, что потеря конфиденциальности персональных данных чревата рисками исков потерпевшей стороны, чьи данные были раскрыты. Примером такого инцидента является дело Citigroup. В июне 2011 года банк признал, что неизвестные хакеры, сломав его систему безопасности, получили доступ к данным сотен тысяч кредитных карт клиентов в Северной Америке.

«Во время рутинного мониторинга мы обнаружили несанкционированный доступ к on-line счету Citi,- говорится в сообщении банка. – Мы оповестили клиентов, чьи данные были затронуты». По данным банка, примерно 1% или сотни тысяч держателей кредитных карт были затронуты, при общем количестве держателей карт около 21 миллиона, в соответствии с данными годового отчета за 2010 год. Были раскрыты имена, номера кредитных карт, домашние адреса и адреса электронной почты клиентов. Потери на восстановление защиты, замену карт, возмещение мошеннических платежей и урегулирование претензий составили много миллионов долларов.

Также широко известен инцидент с компанией Sony, которая призналась, что в период с 17 по 19 апреля 2011 года из базы данных PlayStation Network были украдены следующие данные пользователей: имя, почтовый адрес, адрес электронной почты, дата рождения, логин и пароль доступа в PlayStation Network/Qriocity, Handle/PSN online ID и, возможно, номер кредитной карты.

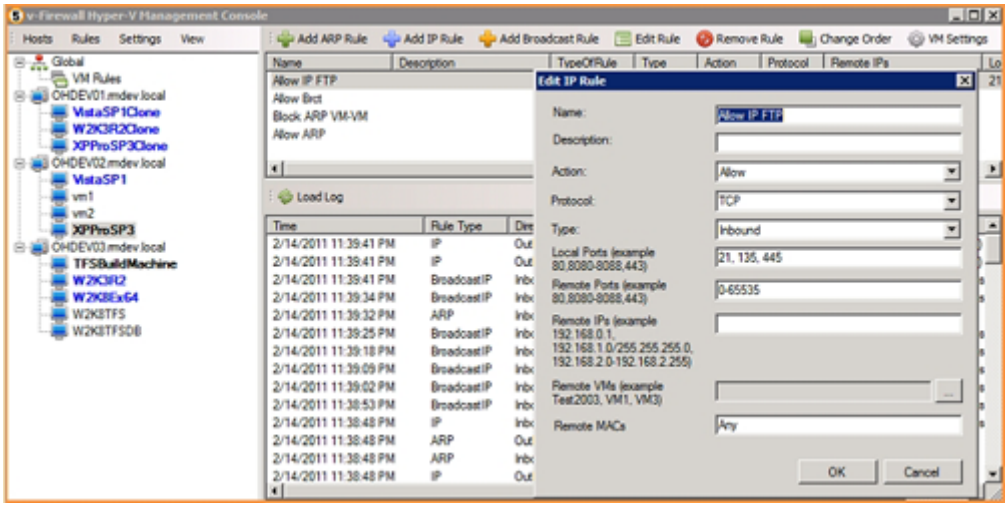
В общей сложности были похищены данные 77 миллионов пользователей. Чтобы устранить нарушения в системе безопасности, Sony пришлось отключить сеть, через которую клиенты играли, скачивали фильмы, телешоу и музыку, за что платили $49 в год. «Пользователям PlayStation Network должна быть обеспечена защита финансовых данных, включая свободный доступ к информации по операции с их кредитными картами на два года. Расходы по оказанию этой услуги должна взять на себя Sony», - написал бывший генеральный прокурор Коннектикута.

Sony в результате скандала может потерять до $1,5 млрд. В этой сумме эксперты учитывают не только выплаты по многочисленным возможным искам, но и остановку работы сети, ежегодно приносящей компании около $500 млн. дохода, а также потенциальное падение продаж консолей японской компании. Акции Sony упали в цене на Токийской фондовой бирже на 2,3%, в то время как индекс Nikkei 225 вырос на 1,4%.

У нас пока таких прецедентов нет, но это связано с тем, что законодательная база не доработана, а юристы только вырабатывают механизмы обеспечения прав своих клиентов на охрану их персональных данных. Очевидно, что риск таких исков есть и у нас, и это нужно учитывать сегодня, когда Вы планируете свой бюджет на информатизацию с учетом требований закона «О персональных данных». При закупках мы рекомендуем отдавать приоритет продуктам, которые не только имеют необходимые сертификаты соответствия, но и имеют действенные механизмы, проверенные и одобренные мировой практикой по обеспечению защиты персональных данных.

Поскольку современные информационные структуры проектируются с использование преимущественно «облачных» технологий, примером таких продуктов, обеспечивающих информационную безопасность, являются Deep Security от Trend Micro , vGate R2 от «Кода безопасности» для VMware Sphere и 5nine Virtual Firewall для Microsoft Hyper-V. Сейчас на долю Microsoft и VMware приходится по оценкам аналитиков более 70% рынка виртуализации. Нужно сразу отметить, что общее количество доступных продуктов по обеспечению безопасности «облачных» сред невелико. Это несколько решений под VM Ware Sphere и единственное программное решение под Microsoft Server 2008 R2 - 5nine Virtual Firewall, которое обеспечивает программное управление безопасностью виртуальной среды Hyper-V, на базисе каждой отдельной виртуальной машины.

5nine Virtual Firewall - это продукт для обеспечения безопасности виртуальных машин в среде Hyper-V , который позволяет программно управлять сетевой безопасностью виртуальной инфраструктуры на основе управления каждой ВМ, определяя правила сетевого трафика для каждой ВМ и таким образом увеличивая ее безопасность.



Virtual Firewall позволяет просматривать и анализировать журналы сетевого трафика, собирать статистику событий для каждой из ВМ, что является одним из основных требований к такого рода продуктам в США. Наконец, 5 nine Virtual Firewall предоставляет возможность регулировать использование полосы пропуска внешнего сетевого трафика для каждой виртуальной машины в инфраструктуре, предотвращая отказ в обслуживании критически важных приложений из-за перегрузки внешнего канала.

Встроенный брандмауэр Windows защищает физический Hyper-V сервер, но не сможет этого сделать для каждой ВМ на нем. 5nine Virtual Firewall - это единственный Firewall для ВМ под Hyper-V.

Правила фильтрации пакетов Firewall позволяют разрешить или запретить разные виды входящего/исходящего трафика. При увеличении числа критических приложений и ВМ, работающих в Hyper-V, становится более важным защитить их от вредоносных атак, а также недобросовестных конечных пользователей.

С помощью нескольких щелчков мыши или простой команды PowerCLI можно использовать V-Firewall для создания и изменения правил брандмауэра. Эти правила позволяют ограничить различные типы сетевого трафика: входящего из внешней сети для Hyper-V ВМ, или исходящего из виртуальной машины к внешней сети, или между виртуальными машинами на частной виртуальной сети. Таким образом, V-Firewall позволяет защитить вашу виртуальную инфраструктуру «снаружи» и «внутри» от сетевых атак.

5nine Virtual Firewall также имеет «интеллектуальную» защиту против вредоносного сканирования, который позволяет избежать снижения производительности ВМ и хостов из-за вирусной или другой вредоносной активности, в тоже время, препятствуя проникновению различных троянов, руткитов и вирусов.

Правила межсетевого экрана можно легко создать на одной или нескольких виртуальных машинах в инфраструктуре Hyper-V при помощи простого, интуитивно понятного интерфейса. Создание правила брандмауэра сводится к заполнению строк в окне протоколами и номерами портов.

Как и в традиционных правилах брандмауэра, правила V-Firewall основаны на исходящем и конечном IP-адресах. Однако, в отличие от традиционных брандмауэров, с V-Firewall можно создавать правила, для конкретных Hyper-V виртуальных машин и применять эти правила к ряду ВМ. Администратор может быстро использовать правила по умолчанию: например, разрешить весь исходящий трафик во внешнюю сеть и принимать входящий трафик в ответ на внешний запрос (с помощью функции брандмауэра с отслеживанием состояния V-Firewall).

V-Firewall дает возможность подтвердить соответствие стандартам безопасности своей виртуальной инфраструктуры, так как это единственный инструмент такого рода, который может мониторить, давать отчеты, фильтровать виртуальной сетевой трафик, а также вести журналы транзакций, которые необходимы для проведения аудита соответствия законам о ПД и обнаружения хакерских атак. Даже если информационные системы клиента не попадают под юридическое или публичное регулирование, Virtual

Firewall все равно нужен для обеспечения регистрации и отчетности по трафику виртуальной сети.

5nine V-Firewall обычно используется для блокировки Hyper-V ВМ во всех направлениях и протоколирует трафик, который был разрешен или запрещен. Кроме того, V-Firewall обычно используется для выполнения регулировки пропускной способности на отдельных виртуальных машинах или группах виртуальных машин.

Мощная функция V-Firewall HEARTBEAT SERVICE непрерывно проверяет, применяются ли правила сетевого трафика.

В настоящее время компания 5nine работает над сертификацией VF по требованиям ФСТЭК России.

Trend Micro Deep Security 8 и 5nine V-Firewall широко применяются для обеспечения безопасности виртуальных сред за рубежом, где контроль обеспечения защиты персональных данных очень высок и достаточно жесткая конкуренция на рынке информационной безопасности. Поэтому эти продукты при удовлетворении требованиям ФСТЭК России могут быть рекомендованы большинству клиентов, работающих над проектами своих «облачных» платформ, удовлетворяющих требованиям закона «О персональных данных» и подзаконных актов.

Российский продукт vGate R2 от компании «Код Безопасности» специально разрабатывался для применения в государственных и иных учреждениях, в которых предполагается высокий уровень защиты информации и позволяет защитить информацию до уровня «совершенно секретно» от несанкционированного доступа.

Также хотелось бы обратить внимание отечественных разработчиков на то, что в ближайшем будущем при увеличении доли облачных технологий в информационных структурах российских предприятий и организаций повысится спрос на решения по обеспечению их безопасности. При разработке таких решений особенное внимание должно быть уделено соответствию Федеральному закону «О персональных данных» и, естественно, лучшим мировым практикам в области защиты информации.

Юрий Бражников,
Директор представительства 5nine Software в СНГ/Вост. Европе
Тел.: +7 (495) 777-32-82
www.5nine.ru