Комплексная защита данных в публичных облаках

Обзор последних анонсов решений компании Trend Micro, позволяющих максимально снизить риски информационной безопасности (от конечных устройств до обработки/хранения данных на стороне публичного сервис-провайдера) при развертывании корпоративных приложений в публичных облаках.

Денис Безкоровайный – технический консультант Trend Micro в России и СНГ.

Введение

Развитие рынка облачных сервисов, помимо преимуществ, связанных с этим видом ИТ-услуг, породило и большое количество проблем, прежде всего, в области информационной безопасности, что оказалось особенно чувствительным для корпоративного сектора. После ряда крупных скандалов в 2011 г. (например, в МО США) в связи с утечкой данных несколько крупных проектов по миграции приложений и данных в публичные облачные среды были приостановлены. По этой же причине внутренними регламентами многих западных банков также было запрещено развертывание каких-либо корпоративных сервисов (за исключением клиентских) в публичных облаках.

В качестве причин, значительно снижающих уровень ИБ при переходе развертывания корпоративных приложений от датацентров с охраняемым периметром к датацентрам, которые поддерживаются публичным провайдером услуг, можно выделить следующие:

- *снижение уровня защищенности данных и приложений при переходе от невиртуализованных к виртулизированным ИТ-инфраструктурам;*
- *обслуживание ресурсов, выделяемых для арендуемых ИТ-сервисов, недоверенным персоналом;*
- *доступ к приложениям/данным по общедоступным каналам связи;*
- *необходимость поддержания мобильных корпоративных и некорпоративных (концепция BYOD – bring your own device) устройств.*

Из-за снижения уровня ИБ на базе виртуализованных ИТ-инфраструктур к концу 2010 г. в США и Западной Европе были доработаны все основные документы – стандарты, рекомендации, связанные с обеспечением безопасности услуг/сервисов на базе ИТ. Это также затронуло и отраслевые стандарты, например: PCI DSS, HIPAA, SOX (GLBA), FISMA, ISO и др. В настоящее время решения для ИБ с учетом этих требований активно развиваются. По оценкам Gartner, к 2015 г. острота этой проблемы в большей степени должна быть снята.

Trend Micro входит в тройку ведущих поставщиков решений в области информационной безопасности в мире, и в своем отчете – "Угрозы для безопасности бизнеса, цифровых устройств и облачных технологий" (декабрь 2012 г.) – несанкционированный доступ к данным в облачных сервисах был назван в качестве одной из ключевых угроз в 2013 г.

После анонсирования в феврале 2013 г. доступности 9-й версии Deep Security, интегрированной с решением SecureCloud, а также расширения функционала Mobile Security для мобильных устройств на базе Android, Trend Micro представила законченный пакет решений для обеспечения интегрированного управления информационной безопасностью и соблюдения требований регуляторов в части ИБ для публичных/гибридных облаков как от внешних, так и от внутренних угроз.

В рассматриваемом обзоре обсуждаются программные решения, ориентированные на защиту данных и приложений, развертываемых в публичных/гибридных облачных средах с полным управлением, включая ключи шифрования, с клиентской стороны. В этом контексте задача защиты частных облаков – более простая.

SecureCloud – защита от внутренних угроз на стороне провайдера при обработке данных

Возможность доступа к данным в лице так называемого "суперпользователя" или администратора виртуальной инфраструктуры (или недоверенного сотрудника – с точки зрения клиента облачных ИТ-услуг) – одна из основных причин, сдерживающих распространение корпоративных облачных (публичных) сервисов. Необходимо отметить, что здесь речь идет о данных, которые обрабатываются на стороне провайдера. Защита от утечек только хранимой на стороне провайдера информации уже много лет достаточно эффективно решается за счет многоуровнего шифрования/дешифрования данных на стороне клиента. При этом без особых затруднений могут использоваться как российские, так и западные алгоритмы.

Сейчас уже многие провайдеры предлагают собственные интегрированные средства обеспечения безопасности пользовательских данных, и на рынке также представлены соответствующие решения ИБ от третьих фирм, однако проблема остается.

Во-первых, это связано с тем, что, несмотря на подписание соответствующих соглашений с провайдером публичных ИТ-услуг, контроль за персоналом провайдера недоступен клиентам ИТ-услуг, что вызывает элемент беспокойства. *Во-вторых*, интеграция какого-либо дополнительного оборудования и/или ПО в инфраструктуру провайдера – это сложная процедура, требующая как временных, так и материальных затрат, и нередко добавить что-то по желанию клиента в типовую инфраструктуру провайдера просто невозможно.

Шифрование данных в облаке – один из основных защитных механизмов, снижающих риски компрометации данных, рекомендованных Cloud Security Alliance.

Решение SecureCloud, которое Trend Micro аносировала еще в марте 2011 г. (версия 1.1), при полной прозрачности для приложений и неизменности формата данных для приложений, а также каком-либо влиянии на инфраструктуру и ПО провайдера во многом позволяет снять остроту этой проблемы.

SecureCloud реализует полное шифрование устройства/диска (FDE – Full Disk Encryption) на уровне операционной системы как для физических, так и для виртуальных машин (ВМ) в облачной среде. Благодаря этому обеспечивается защита всех данных, метаданных и связанных структур без ограничения функциональности приложений. Криптографическое ядро продукта сертифицировано по FIPS 140-2.

В SecureCloud реализована простая система управления ключами, которая позволяет с помощью политик определять, когда и откуда можно получить доступ

к зашифрованным данным. Кроме того, к серверам, запрашивающим доступ к защищенным томам хранилища, применяются правила проверки подлинности и целостности. SecureCloud обеспечивает простую и безопасную передачу ключей шифрования разрешенным устройствам без необходимости выполнять развертывание всей файловой системы и инфраструктуры управления.

С помощью SecureCloud можно защитить конфиденциальную информацию, хранящуюся в "облачных" и виртуальных средах, от хищения, несанкционированного доступа и неутвержденного переноса в другие центры обработки данных. Такая защита помогает обеспечить соответствие внутренним правилам и нормативным документам, таким как HIPAA, HITECH, законы Сарбейнса-Оксли и Грэмма-Лича-Блайли, а также отвечает требованиям стандарта безопасности в области использования платежных карт (PCI DSS).

Продукт позволяет напрямую интегрироваться с несколькими основными распространенными платформами для создания и управления платформой облачных сервисов (IaaS) и виртуальной инфраструктурой: VMware vCloud Director 1.0/1.5, VMware vSphere 4/5 (ESX 4/5); Eucalyptus 1.6/2.0; Amazon EC2; RightScale; TCloud. Среди поддерживаемых ОС серверов: Windows 7, Windows Server 2003 R2 SP2 (32- и 64-разр.), Windows Server 2008 R2 SP2 (32- и 64-разр.), Windows Server 2008 SP2 (32- и 64-разр.), CentOS 5.5 (32- и 64-разр.), Red Hat Enterprise Linux 6 (32- и 64-разр.), Ubuntu 10.10 (32- и 64-разр.), SUSE Linux Enterprise Linux 11.4.

Разработчики в своем стремлении быть интероперабельными предлагают решения, позволяющие управлять гетерогенными ресурсами и объединять вычислительные мощности под контролем различных гипервизоров в единую облачную инфраструктуру. Например, платформа для создания IaaS-облаков от Eucalyptus поддерживает как гипервизоры VMware, так и open-source гипервизоры Xen и KVM. Поскольку SecureCloud работает с IaaS-платформой, защита будет одинаково эффективной для ВМ, работающих на любом из поддерживаемых облачной платформой гипервизоров.

SecureCloud имеет три основных компонента: агент, сервер управления ключами и консоль управления.

При загрузке операционной системы ВМ-агент SecureCloud формируется запрос на получение ключа расшифрования к серверу управления ключами. На сервере управления ключами выполняется обработка запроса – вручную администратором безопасности или автоматически на основе заранее настроенных политик. Политики определяют набор критериев, по которым одобряется или отвергается запрос на ключ. Например: кто запрашивает ключ; какая это виртуальная машина (имя, IP адрес и т.д.); когда она была запущена и где (в каком датацентре); можно ли выдавать ключ этой машине; установлен ли на ней антивирус с последней версией сигнатур; присутствуют ли на ней другие системы защиты; не нарушена ли целостность критичных файлов? Все это можно проверить либо напрямую агентом SecureCloud, либо с помощью глубокой интеграции с другим продуктом для защиты датацентров от Trend Micro – Deep Security (рис. 1), используя который заказчик уже может иметь настроенные профили защиты и правила контроля целостности.

Рис. 1. Защита данных в облаке – интегрированные решения на базе SecureCloud и Deep Security 9.

В случае одобрения запроса на выдачу ключа, агент получает ключ по защищенному каналу и осуществляет расшифровку и подключение защищенного диска к уже работающей ВМ. После этого зашифрованный диск становится прозрачно доступным для ОС и приложений, например, СУБД или веб-серверу.

Для расположения сервера управления ключами используется ЦОД компании Trend Micro – высоконадежный и внешнеаудируемый, сертифицированный по ISO 27001.

В первом случае клиенты получают возможность управлять ключами шифрования с помощью внешней услуги SecureCloud от Trend Micro.

Поддержка в SecureCloud протокола KMIP позволяет использовать внешний аппаратный HSM (Hardware Security Module) для еще большей надежности хранения ключей.

При интеграции в приложение дополнительных операций по шифрованию/дешифрованию данных всегда встает вопрос о накладных затратах на процессор. Тестирование показывает, что накладные расходы при использовании продукта SecureCloud не превышают 3–7% от базового уровня.

Система шифрования и управления ключами Trend Micro™ SecureCloud позволяет:

- сделать все защищаемые данные клиента, украденные у сервис-провайдера, нечитаемыми и бесполезными для нарушителя;
- предотвращать несанкционированный доступ к данным клиента в облачном датацентре провайдера;
- контролировать ключи шифрования заказчиком и отделять функцию защиты данных от облачного провайдера;
- авторизовывать запросы на ключи вручную и автоматически на основе политик;
- гарантировать невозможность доступа других клиентов провайдера к защищаемым данным компании при повторном использовании жестких дисков в облачной среде;
- поддерживать масштабируемость для множества ВМ;
- поддерживать независимость от технологии облачного провайдера (снижение lock-in риска);
- обеспечивать контроль доступа к данным в облаке при ограниченных возможностях аудита облачного провайдера;
- обеспечивать контроль данных в облаке при смене провайдера или его закрытии;
- обеспечивать защиту данных при краже всей машины или ее виртуальных дисков.

В декабре 2012 г. решение SecureCloud получило награду "Best Cloud Security Product" престижного конкурса V3 Technology Awards 2012.

Deep Security – защита облачных серверов и приложений от внешних угроз

Решение Deep Security обеспечивает защиту виртуальных серверов и приложений, разворачиваемых на них, от внешних угроз, которые могут поступать по публичным каналам доступа к ресурсам. В интеграции с SecureCloud данное решение обеспечивает “круговую оборону” инфраструктуры и данных клиента на стороне провайдера.

В решении Deep Security реализованы функции обнаружения и предотвращения атак, брандмауэра, контроля целостности и проверки журнала – в едином программном агенте с централизованным управлением. Решение также обеспечивает защиту от вредоносных программ без использования агента, что позволяет повысить уровень защиты и плотность размещения виртуальных машин в виртуализированном ЦОД. Deep Security может использоваться в виде программного обеспечения, виртуального устройства или их комбинации.

Последняя – 9 версия – стала доступна с февраля 2013 г. и обеспечила следующие новые возможности по сравнению с предыдущей реализацией:

- *интеграцию с vCloud Director, Amazon Web Services.* Унифицированная консоль администрирования обеспечивает единую среду для управления защитой данных в ЦОД, а также в общедоступных средах на основе VMware vCloud® и Amazon;
- *поддержку новейших продуктов VMware: vSphere 5.1 и vCloud Networking and Security 5.1 (vCNS);*
- *улучшенную защиту без использования агента.* Функции кэширования и дедупликации на уровне VMware ESX® повышают производительность, а технология сканирования для получения рекомендаций упрощает настройку политик безопасности;
- *функцию контроля целостности,* которая повышает уровень защищенности виртуализованных систем и степень их соответствия нормативным требованиям. Используя технологию Intel TPM/TXT, Deep Security 9 может отслеживать любые неавторизованные изменения в гипервизоре, помогая обеспечить соответствие новейшим нормативным требованиям, таким как, например, рекомендации по виртуализации PCI DSS;
- *гибкую многопользовательскую архитектуру для центров обработки данных и поставщиков услуг.* Deep Security 9 поддерживает логическое разделение политик и данных подписчиков, возможность делегирования полномочий

и самообслуживания, а также эластичное масштабирование облачных сервисов путем автоматического развертывания и запуска компонентов Deep Security. Управление с помощью RESTful API упрощает масштабирование и интеграцию в облачную инфраструктуру.

Deep Security строится по модульному принципу, позволяя выбирать только требующуюся функциональность из следующего списка (рис. 2):

– *защита от вредоносных программ*. Модуль интегрируется с программными интерфейсами VMware vShield Endpoint, обеспечивая защиту виртуальных машин VMware от вредоносных программ без использования агента, не снижая производительность и не требуя дополнительных ресурсов. Он помогает избегать "антивирусных штормов", которые часто наблюдаются при полной проверке системы и обновлении антивирусных баз данных. Кроме того, доступны средства защиты от вредоносных программ с использованием агентов для физических серверов, виртуальных серверов на основе Hyper-V и Xen, "облачных" серверов общего доступа и виртуальных компьютеров в локальном режиме. Модуль обеспечивает согласованные меры безопасности с использованием агентов и без них для адаптивной защиты виртуальных серверов при их перемещении между центром обработки данных и общедоступным "облаком";

– *Web Reputation*. Модуль интегрируется со средствами оценки веб-репутации Trend Micro™ Smart Protection Network™, защищая пользователей и приложения путем блокирования доступа к вредоносным URL-адресам. Он обеспечивает такие же возможности в виртуальных средах в режиме без агентов с помощью того же виртуального устройства, которое также позволяет использовать технологии защиты без агентов, не требующие дополнительных ресурсов;

– *контроль целостности* – отслеживание любых неавторизованных изменений в гипервизоре на основе технологии Intel TPM/TXT;

– *обнаружение и предотвращение вторжений*. Модуль обеспечивает своевременную защиту от известных угроз и атак "нулевого дня". Правила защиты уязвимостей изолируют бреши в защите (например, указанные в ежемесячном бюллетене Майкрософт) от неограниченного количества угроз. Предоставляются встроенные функции защиты уязвимых мест более чем 100 приложений, включая базы данных, веб-серверы, а также почтовые и FTP-серверы. Правила, блокирующие недавно обнаруженные уязвимости, автоматически загружаются в течение нескольких часов и могут быть за считанные минуты развернуты на тысячах серверов без перезагрузки системы.

Модуль обеспечивает соответствие требованию 6.6 стандарта PCI для защиты веб-приложений и обрабатываемых ими данных. Он защищает системы от атак, связанных с внедрением SQL-кода и межсайтовым выполнением сценариев, а также блокирует уязвимости веб-приложений. Уязвимые места будут защищены до выпуска необходимых исправлений;

– *брандмауэр*. Модуль обеспечивает централизованное управление политикой брандмауэра сервера с использованием двунаправленного потокового брандмауэра. Он поддерживает зонирование виртуальных машин и предотвращает атаки типа "отказ в обслуживании". Кроме того, он обеспечивает эффективную защиту всех IP-протоколов и типов фреймов, а также детальную фильтрацию портов, IP- и MAC-адресов;

– *проверка журналов*. Модуль выявляет важные события, относящиеся к системе безопасности, в многочисленных записях журналов в масштабе центра обработки данных и передает сведения о подозрительных событиях в систему SIEM или на централизованный сервер регистрации для сопоставления, формирования отчетов и архивации. Он использует синтаксис программного обеспечения с открытым исходным кодом системы OSSEC.

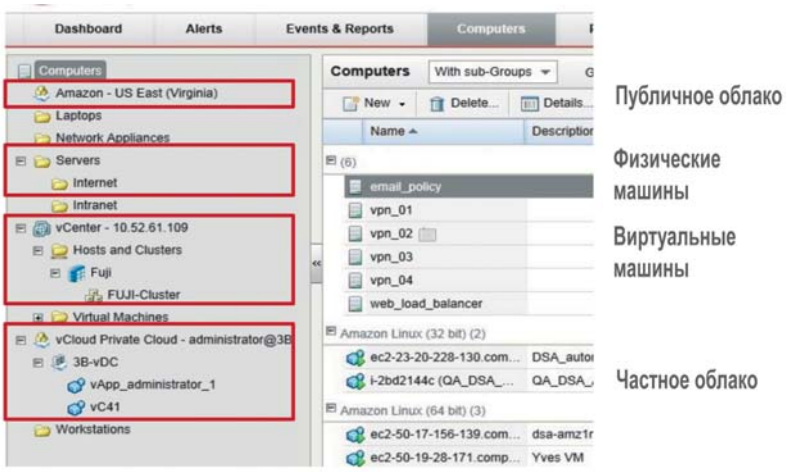

Рис. 3. Управление всеми активами/серверами в Deep Security осуществляется с одной консоли.

Управление всеми активами в Deep Security осуществляется с одной консоли (рис. 3) и в интеграции с SecureCloud позволяет превратить ядро облачной виртуальной инфраструктуры в полноценный защищенный датацентр с полным набором функциональности, присущей невиртуализованным датацентрам с охраняемым периметром.

Функциональность Deep Security может использоваться как провайдером услуг через SaaS-сервис, так и потребителем облачных услуг, значительно расширяя и упрощая (в последнем случае) возможности по управлению политиками безопасности и регламентными требованиями, связанными с ними в гибридных многооблачных средах.

Mobile Security – защита от утечек данных на мобильных устройствах

Мобильные устройства стали неотъемлемой компонентой облачной инфраструктуры для доступа к данным/приложениям и одновременно одним из самых уязвимых мест с точки зрения утечки данных как от инсайдерских, так и от внешних угроз.

Согласно оценкам компании Trend Micro, в 2013 г. число вредоносных и потенциально опасных приложений для Android™ вырастет на 185% и достигнет 1 млн. Согласно выводам отчета 2012 Mobile Threat and Security Roundup ("Обзор угроз для безопасности мобильных приложений и устройств – 2012"), главным трендом в 2013 г. станет рост числа вредоносных приложений, особенно рекламного ПО и программ для кражи информации. Агрессивные рекламные приложения будут способны не только "действовать нам на нервы", но и создавать реальные риски для конфиденциальности данных, например, выманивая данные с помощью мошеннических текстовых сообщений.

Следуя вызовам времени, в феврале 2013 г. Trend Micro представила обновленную платформу Trend Micro™ Mobile Security 8.0.

Mobile Security – это интегрированное решение управления мобильными уст-

Рис. 2. Архитектура Deep Security строится по модульному принципу.

ройствами, безопасностью и приложениями для мобильных устройств в рамках единой системы, позволяющей компаниям управлять безопасностью ПК и мобильных устройств с одной консоли.

Обеспечивая прозрачность и контроль за мобильными устройствами, Mobile Security позволяет руководителям ИТ-служб применять подход BYOD, при котором используются собственные устройства сотрудников и который повышает производительность и гибкость работы персонала, снижая затраты на ИТ-систему. Mobile Security распространяет действие защиты не только на традиционные ПК, позволяя компаниям контролировать и защищать мобильные устройства и хранящиеся на них данные с помощью паролей и шифрования, а также дистанционного уничтожения данных с утерянных или похищенных устройств.

Личная жизнь и работа переплетаются все теснее, поэтому сотрудники предприятий используют собственные ПК, планшеты и смартфоны в деловых целях. В последнее время обозначилась тенденция под названием "ориентированность ИТ-инфраструктуры на пользователя". Она вынуждает организации не только разрешать, но и поддерживать использование сотрудниками личных мобильных устройств, которые, как правило, бывают достаточно мощными и высокотехнологичными.

Ориентированность на пользователя ставит перед ИТ-специалистами серьезные вопросы:

– как организовать техническую поддержку устройств, о которых ничего не известно;

– как обеспечить максимальную прозрачность;

– как защитить корпоративную сеть и данные, если невозможно контролировать устройства;

– как различить личные и корпоративные данные на персональных устройствах, с которых сотрудники входят в сеть предприятия.

Mobile Security предлагает средства управления и обеспечения безопасности для крупных и средних предприятий, которые хотят использовать возможности ориентированности на пользователя, не подвергая риску ИТ-инфраструктуру.

Платформа Mobile Security, защищающая различные мобильные устройства пользовательского класса, такие как iPhone, iPad, Android- и Blackberry-устройства, интегрирует средства управления ими и позволяет осуществлять предотвращение атак, защиту данных и управление приложениями из одной точки. Благодаря этому компании могут обеспечивать прозрачность и контроль, давая сотрудникам возможность свободно обмениваться данными в физической, виртуальной и "облачной" средах. Среди поддерживаемых платформ мобильного клиента: Android 2.1-4.0, iOS 4-5.1, BB (которые поддерживает Blackberry Enterprise 5.0 и более поздние версии), Symbian S60 (3 и 5 выпуски), Windows Mobile 5-6.5.

Среди основных характеристик Mobile Security следующие (рис. 4):

– мгновенный просмотр сводных данных о соответствии требованиям, количестве, защите и состоянии устройств и создание соответствующих отчетов;

– возможность управления безопасностью и конфигурацией ПК и мобильных устройств с единой консоли: интеграция с ведущим в отрасли решением OfficeScan для компьютеров от Trend Micro;

– разрешение или блокировка функций камеры, интерфейса Bluetooth® и устройства чтения SD-карт мобильных устройств;

– избирательное удаление данных с устройства – удаление только сообщений электронной почты, контактных данных, календаря и заданных значков Webclip;

– уведомления о взломе или расшифровке устройств;

– применение собственного шифрования и оповещение о несоответствии;

– обнаружение и блокирование вредоносных приложений и файлов данных;

– предотвращение доступа к вредоносным сайтам и веб-содержимому – служба Web Reputation;

– защита устройств от несанкционированного доступа с помощью брандмауэра;

– функция фильтрации и регистрации звонков и сообщений отслеживает, блокирует и регистрирует входящие и исходящие звонки, SMS и WAP-сообщения на основании пользовательской политики;

– принудительное применение паролей и шифрования для защиты от несанкционированного доступа; контроль продолжительности и результата;

– дистанционная блокировка в случае угрозы или утери телефона;

– определение местонахождения устройства при помощи встроенной функции поиска устройств;

– дистанционное удаление всех данных и настроек;

– ведение черного списка приложений;

– ведение белого списка приложений;

– установка приложений на устройства с помощью Webclip. Установка "необязательных" и "обязательных" настроек;

– прозрачность учета устройств и составления отчетов по устройствам, группам и для всей компании;

– дистанционная блокировка, удаление и выборочное удаление данных и принудительная защита паролем при включении питания обеспечивают защиту корпоративных данных на смартфонах и планшетных ПК в случае утери или хищения;

– расширенные возможности управления мобильными устройствами (MDM) позволяют организациям предоставлять и ограничивать доступ для корпоративных и собственных смартфонов и планшетных ПК сотрудников;

– предоставление полной информации об устройствах и их состоянии, включая настройки пароля и шифрования смартфонов и планшетных ПК, что позволяет администраторам ИТ-инфраструктур принимать упреждающие меры и сокращать расходы на техническую поддержку;

– централизованная регистрация устройств, а также предоставление или ограничение доступа к сети и приложениям, в том числе: настройки VPN, Exchange ActiveSync и Wi-Fi®.

Среди основных преимуществ использования Mobile Security:

– обеспечение прозрачности и контроля;

– сокращение эксплуатационных расходов;

– повышение производительности и гибкости персонала;

– ограничение потерь данных;

– снижение рисков безопасности.

Дополняющими продуктами Mobile Security могут служить: Endpoint Encryption – для более углубленной защиты данных от утечек и Data Loss Prevention – для более контролируемой работы с корпоративным контентом и защиты от утечек.

Рис. 4. Функциональность Mobile Security 8.0.

Заключение

Скорейшее внедрение законченных решений информационной безопасности для облачных сред, включая публичные и гибридные облака, позволит в значительной степени снизить риски утечки данных и в максимальной степени приблизить соответствие ИТ-инфраструктур к требованиям регуляторов, что, в свою очередь, позволит корпоративному бизнесу в полной мере воспользоваться всеми преимуществами облачных сервисов.

Денис Безкоровайный,
компания Trend Micro