Комплексная безопасность в облачных средах

Круглый стол. В обсуждении приняли участие: Мария Сидорова – заместитель руководителя направления "Защита виртуальных инфраструктур"компании "Код Безопасности", Михаил Чернышев – менеджер по продажам компании McAfee и представители корпорации Intel.

"Код Безопасности": вопрос обеспечения безопасности данных в облаке становится одним из самых важных вопросов для клиентов виртуализированного ЦОД

SN. Насколько вопросы обеспечения ИБ актуальны для ЦОД, построенных с использованием технологий виртуализации?

М.С. Появление центров обработки данных (ЦОД), построенных с использованием технологий виртуализации, это – устойчивая тенденция настоящего времени. В большинстве случаев ЦОД находится вне ИТ-инфраструктуры предприятия, а обеспечение безопасности данных, которые передают клиенты виртуализированного ЦОД поставщику услуг (провайдеру), – это один из наиболее остро волнующих вопросов для заказчиков услуг ЦОД. К задаче обеспечения безопасности данных добавляется также необходимость приведения информационных систем в соответствие с требованиями законодательства, отраслевых и международных стандартов на сторонней территории. Эти задачи в определенной пропорции делят и клиент, и провайдер, а, между тем, все эти процессы должны быть прозрачны для клиента ЦОД. Не стоит упоминать, что доверие клиентов – важный аспект работы для каждого ЦОД. Вот почему повышенная безопасность нередко предлагается клиентам ЦОД как дополнительная услуга.

SN. С какими трудностями сегодня сталкиваются владельцы коммерческих виртуализированных ЦОД?

М.С. Можно выделить три основные проблемы обеспечения безопасности данных в виртуализированных ЦОД. *Первая* – это неспособность традиционных средств защиты обеспечить защиту от новых угроз, специфичных для виртуальной среды, и выполнение требований по нормативному соответствию. С точки зрения серверной архитектуры, при переходе от физической среды к виртуальной появляются два новых компонента – гипервизор и сервер управления виртуальной инфраструктурой, которые являются потенциальными каналами утечки, посредством которых нарушитель может получить доступ к обрабатываемым на виртуальных машинах данным. Причем, важность этих компонентов для обеспечения информационной безопасности очень высока. Компрометация сервера виртуализации будет приводить к серьезному повышению риска компрометации всех виртуальных машин, размещенных на этом сервере, а захват централизованных средств управления виртуальной инфраструктуры, очевидно, – к компрометации всех виртуальных машин в рамках инфраструктуры. С помощью этих компонентов злоумышленник может перехватить потоки данных, идущие с виртуальных машин на устройства, или получить непосредственный доступ к дискам хранилища с файлами виртуальных машин. Причем, он может получить доступ к дискам хранилища даже в том случае, когда виртуальные машины выключены или не работают, без участия программного обеспечения этих виртуальных машин. В случае с приведением информационных систем в соответствие с требованиями законодательства или стандартов безопасности появляются новые проблемы. Например, для обеспечения контроля целостности конфигурации и доверенной загрузки обычно используются аппаратно-программные модули доверенной загрузки. Если для серверов виртуализации такой способ приемлем, то для виртуальных машин такие средства вряд ли применимы (по причине отсутствия аппаратного обеспечения).

Вторая проблема – это появление в виртуализированных ЦОД нового слоя привилегированных пользователей – администраторов виртуальной инфраструктуры, обладающих самыми широкими полномочиями по манипуляциям с данными клиентов. Виртуализация обеспечивает высокую консолидацию ресурсов, а утечка данных через администратора (умышленная или непредумышленная), по данным исследования агентства Forrester 2010 года, является самым дорогостоящим типом инцидента информационной безопасности. Именно поэтому крайне важно контролировать действия администраторов виртуализированной инфраструктуры ЦОД и, по возможности, ограничивать их полномочия. Надо заметить, что без использования специальных наложенных средств ИБ в виртуальной среде практически отсутствуют способы проактивного контроля над действиями "суперпользователей".

Мария Сидорова – заместитель руководителя направления "Защита виртуальных инфраструктур"компании "Код Безопасности".

Третьей проблемой является возможность совместного хранения ресурсов разных клиентов: их виртуальные машины могут выполняться на одном сервере виртуализации, а их диски – находиться в одном хранилище. Совместное хранение ресурсов разных клиентов – источник ряда проблем, таких как потенциальный ущерб для "соседей" в случае компрометации ресурсов хотя бы одного клиента, а также возможность несанкционированного доступа к ресурсам "соседа" со стороны пользователей клиента. Очевидно, что эти проблемы решит разграничение ресурсов разных клиентов, но в силу специфики самих технологий виртуализации сделать это не всегда просто.

SN. Для решения каждой из обозначенных Вами проблем требуется применять один, а то и несколько продуктов. Как в этом случае избежать "зоопарка" СЗИ, созданных разными производителями и зачастую плохо взаимодействующих, а иногда и конфликтующих между собой?

М.С. В этой ситуации целесообразно применять решения разработки одного производителя, который имеет максимально полную линейку СЗИ, способных нейтрализовать угрозы, специфичные для виртуализированного ЦОД. Соответственно, если в виртуализированном ЦОД обрабатывается информация ограниченного доступа (будь то персональные данные, коммерческая тайна, конфиденциальная информация и т.д.), такие решения также должны быть сертифицированы регуляторами. Полную линейку продуктов для защиты виртуализированного ЦОД, в том числе для построения защищенной VPN-сети, обнаружения/предотвращения вторжений, антивирусной защиты и защиты от вредоносных программ, предлагает компания "Код Безопасности".

Оптимальным решением для обеспечения полноценной защиты ресурсов клиентов виртуализированного ЦОД, приведения в соответствие нормативным требованиям и получения отчетов о состоянии параметров безопасности виртуальной инфраструктуры является продукт vGate R2. vGate R2 – это сертифицированное средство защиты от несанкционированного доступа и контроля выполнения ИБ-политик в виртуальных инфраструктурах, построенных на платформах компании VMware.

Для решения проблемы "суперпользователя" в vGate R2 реализовано разделение ролей администраторов и запрет доступа администраторов виртуальной инфраструктуры к данным виртуальных машин. При использовании vGate R2 администратор получает доступ к виртуальной инфраструктуре только после обязательной процедуры аутентификации на сервере авторизации. После этого все действия администратора по управлению виртуальной инфраструктурой, а значит, и доступ к ресурсам клиентов виртуализированного ЦОД, контролируются и фиксируются в журнале событий vGate R2. Кроме того, полномочия каждого администратора виртуальной инфраструктуры ограничены в соответствии с его задачами администратором безопасности (например, предоставлен доступ только к необходимым серверам, запрещена/разрешена возможность скачивания файлов виртуальных машин или создания назначенных заданий). Казалось бы, тут появляется другой "суперпользователь" в лице администратора информационной безопасности. Но этого не происходит, поскольку для этого пользователя ограничен доступ к виртуальной инфраструктуре и возможность самосанкционировать доступ к виртуальной инфраструктуре отсутствует.

Для управления доступом администраторов и разделения ресурсов разных клиентов в vGate R2 реализовано мандатное управление доступом на основе меток конфиденциальности. Пометив ресурсы разных клиентов метками разных цветов, можно гарантировать логическое отделение ресурсов одних клиентов от ресурсов других. И хотя физически эти ресурсы могут находиться на одном сервере или в одном хранилище, такое логическое разделение гарантирует, что сотрудники одной организации не получат доступа к ресурсам другой. Также будет невозможен вариант использования ресурсами одной организации ресурсов другой организации. С помощью меток конфиденциальности можно также разграничить доступ администраторов к ресурсам клиентов: администратор, не получивший права, то есть "метку", не сможет получить доступ к этим ресурсам. Мандатное управление доступом на основе меток конфиденциальности, реализованное в vGate R2, определяет не только доступ администратора к объектам, но и условия выполнения основных операций с ними. Примечательно, что для серверов виртуализации и виртуальных машин метки конфиденциальности выполняют двойную роль: не только являются базой для мандатного управления доступом, но и дают возможность назначать этим объектам политики безопасности. Далее, для конкретной метки индивидуально настраиваются политики безопасности. После чего при назначении метки объекту (серверу виртуализации или виртуальной машине) набор политик начинает действовать для него. Наборы политик могут создаваться специально на основе заданных параметров, а могут использоваться готовые наборы, так называемые шаблоны, встроенные в vGate R2. vGate R2 включает в себя несколько шаблонов по приведению в соответствие требованиям №152-ФЗ, СТО БР ИББС, PCI DSS, VMware Security Hardening Guide, CIS ESX Server Benchmark.

У провайдера, использующего vGate R2, появляется дополнительная возможность для устранения беспокойства клиента о сохранности ресурсов. Провайдер может регулярно предоставлять клиенту отчеты о состоянии настроек безопасности, соответствии политик безопасности отраслевым стандартам, а также отчеты об изменениях конфигурации и произошедших событиях информационной безопасности. vGate R2 позволяет подготовить широкий набор различных отчетов по запросу или автоматически по расписанию. К примеру, можно ежемесячно отправлять клиенту отчет о соответствии политик безопасности требованиям стандарта PCI DSS. После несложной настройки vGate R2 будет создавать такой отчет автоматически, на фирменном бланке с логотипом клиента.

vGate R2 имеет сертификат ФСТЭК России и позволяет защитить информационные системы обработки персональных данных до класса К1 включительно. vGate R2 также содержит инструменты для обеспечения полноценной защиты гипервизора и средств управления виртуальной инфраструктурой от утечки информации по каналам, специфичным для виртуальной среды. Применение vGate R2 совместно с другими продуктами разработки "Кода Безопасности" позволяет построить комплексную систему защиты конфиденциальной информации и персональных данных при их обработке в виртуальной среде. Для обеспечения контроля целостности и доверенной загрузки серверов виртуализации, сервера управления и сервера авторизации vGate R2 рекомендуется устанавливать на каждый из этих серверов аппаратно-программный модуль доверенной загрузки ПАК "Соболь". Для обеспечения защиты сетевого доступа к виртуальным машинам и контроля трафика между виртуальными машинами на одном сервере виртуализации рекомендуется применять распределенный межсетевой экран высокого класса защиты TrustAccess. Применение TrustAccess для сегментирования информационных систем обработки персональных данных позволяет отнести отдельные сегменты к более низкому классу и добиться снижения затрат на защиту. Для защиты каждой виртуальной машины от несанкционированного доступа рекомендуется использовать средство защиты информации Secret Net, которое обеспечивает разграничение доступа, доверенную информационную среду, а также защиту информации в процессе хранения. Применение сертифицированного ФСТЭК и ФСБ России аппаратно-программного комплекса шифрования "Континент" обеспечит возможность построения защищенной VPN-сети и безопасного доступа клиентов к ресурсам ЦОД. В свою очередь, для построения надежной системы обнаружения/предотвращения вторжений (IPS/IDS) стоит применять программные продукты: Honeypot Manager, основанный на имитации данных и анализе обращений пользователей к ним, и Security Studio Endpoint Protection (SSEP), обеспечивающий антивирусную защиту и защиту от вредоносных программ.

Intel: решение проблемы возрастающих угроз ИБ – погружение функциональности ИБ на уровень чипов

Современная ИТ-индустрия стремительно движется в направлении развития облачных ИТ-инфраструктур и облачных ИТ-сервисов. Это, с одной стороны, существенно повышает доступность и простоту получения ИТ-услуг конечными потребителями, но, с другой, увеличивает и риски, связанные с возможными утечками информации, вследствие того, что все ИТ-операции осуществляются в распределенных средах по общедоступным каналам связи с использованием множества различных мобильных устройств.

Из-за нерешенности многих проблем в области ИБ при переходе на полностью виртуализированные ИТ-инфраструктуры сдерживалось и их использование для развертывания корпоративных облачных ИТ-сервисов. Поворотным моментом в этой связи явилась середина 2010 г., когда были приняты законодательные и регламентирующие акты, устанавливающие дополнительные требования ИБ. Например, последняя версия стандарта PCI-DSS – Payment Card Industry Data Security Standard – устанавливает необходимость шифрования данных кредитных карт при проведении каких-либо транзакций с ними. Акт HiTECH 2010 г. также требует шифрования чувствительных данных, когда они передаются по публичным сетям типа Интернет.

Корпорация Intel поддержала концепцию облачных сервисов рядом совместных разработок со своими ключевыми партнерами, а также предложила собственные технологии на базе чипов, которые позво-

ляют не только решить проблему ИБ в распределенных средах, но и сделать доступным современный уровень защищенности информации массовому потребителю ИТ-услуг/сервисов.

Корпорация Intel развивает функционал обеспечения информационной безопасности в трех направлениях:

– процессоры x86 (Intel Core i3, i5, i7) были расширены дополнительным набором команд акселерации шифрования – Advanced Encryption Standard New Instruction (AES-NI), которые в настоящее время доступны в большинстве Intel® XEON® 5600 процессоров. Процессоры с данной опцией уже официально поставляются в Россию в соответствии с полным удовлетворением законодательных требований. Данная поддержка алгоритмов криптографии, на порядок повышая производительность программных решений шифрования, позволяет совершенно по-новому строить ИБ в современных облачных ИТ-инфраструктурах, защищая данные на всех уровнях, где они хранятся, обрабатываются, передаются;

– на завершившимся в сентябре форуме разработчиков IDF 2011, Intel и McAfee был сделан совместный анонс технологии DeepSAFE (это часть т.н. многоаспектного совместного проекта Patmos между McAfee и Intel.), который даст возможность вывести защиту от различных руткитов на качественно новый – надОС-ый уровень. Технология DeepSAFE будет поддерживаться процессорами Intel Core i3, i5, i7;

– McAfee и Intel совместно разрабатывают решение Anti-Theft ("анти-кража") для ультрабуков, которое включает уникальную технологию на уровне чипа, способную защитить устройство и данные в случае потери или хищения. Она включает блокировку устройства, шифрование данных и возможность установления местоположения потерянного устройства. McAfee будет привилегированным независимым поставщиком этой технологии Intel для производителей ПО, ретэйлерам, телекоммуникационным провайдерам и другим.

Отдельно хотелось бы остановить внимание на технологии DeepSAFE. Сегодня нельзя не отметить растущую сложность и изощренность атак на самые разные вычислительные устройства. Скрытые атаки совершаются каждую секунду, новые модификации вредоносного ПО появляются каждый день, и для того чтобы обеспечить возможность продуктивной работы для пользователей, необходимо использование средств защиты. Современные средства антивирусной защиты работают в рамках операционной системы, ведя наблюдение за происходящей активностью и пытаясь обнаружить известные атаки. Однако существуют варианты взлома, которые ставят своей целью захват управления на более низком, более привилегированном уровне, чем на том, где работает антивирусное ПО. В случае взлома обнаружение подобного рода атак сильно затруднено. В этой связи, технология McAfee DeepSAFE, анонсированная на Форуме для разработчиков Intel, поможет открыть новое направление на рынке систем защиты. Разработанная совместными усилиями Intel и McAfee технология McAfee DeepSAFE использует аппаратную технологию процессоров Intel VT-x, позволяя защититься от угроз за пределами операционной системы. Это делает возможным заблаговременно блокировать действия вредоносного кода и скрытых атак, использующих уязвимости операционной системы. Кроме того, благодаря реализации на аппаратном уровне, блокировка будет происходить если не мгновенно, то, по крайней мере, на порядок быстрее по сравнению с другими современными решениями. Технология McAfee DeepSAFE является отправной точкой для средств защиты нового поколения и станет основой целого ряда продуктов McAfee, которые будут использовать аппаратные возможности процессоров Intel для улучшенной защиты от известных и неизвестных угроз.

McAfee: в современной реальности мы говорим о 360 градусах защиты

Концепция информационной безопасности эволюционирует вместе с угрозами, которые современный мир предлагает в качестве испытания на прочность для компаний, корпораций и даже целых государств. Примеры: "Операция Аврора",

Михаил Чернышев – менеджер по продажам компании McAfee.

Stuxnet, Night Dragon наглядно иллюстрируют цели и средства их достижения.

В связи с этим, недостаточно иметь защищенным какой-либо один из объектов: к примеру, поставить самый мощный в индустрии межсетевой экран или систему защиты АСУТП (как могло бы показаться логичным в случае с Stuxnet).

В современной реальности мы говорим о 360 градусах защиты. Защита сети, защита мобильных устройств, классические настольные антивирусы и сопутствующее ПО, защита шлюзов почты и веб, защита данных от утечки. Достаточно просто взглянуть на сайт производителя *(www.mcafee.com),* для того чтобы убедиться в полномасштабности средств защиты информации от современных угроз.

Все более частое распространение получает облачная модель обеспечения безопасности в компаниях малого и среднего масштаба. Вместо того чтобы содержать дорогостоящую серверную, укомплектованную разносортными средствами безопасности, сейчас достаточно перейти в соответствующий раздел сайта производителя и выбрать себе защиту: конечных точек, безопасного серфинга веб, защиты электронной почты от вирусов и спама и даже архивирование почты. Облачные сервисы McAfee полностью удовлетворяют единой концепции Security Connected, в которой и управление, и мониторинг осуществляются полностью централизованно (аналогично тому, как в модели управления продуктами McAfee главную роль играет для всех без исключения продуктов центральная консоль McAfee ePolicy Orchestrator). Более того, интересным симбиозом облачной и настольной защиты является использование и продуктов на SaaS модели, и решений, не являющихся облачными – в этом случае производится интеграция двух решений в единое под управлением все того же McAfee ePolicy Orchestrator. На выходе мы получаем полностью реализованный подход 360 градусов безопасности, соединенных между собой общими управлением и стратегией (Security Connected).

Но, как можно справедливо заметить, с момента слияния Intel и McAfee прошло уже достаточно много времени и появилось минимум пресс-релизов о новых и перспективных направлениях защиты, разрабатываемых совместно. В октябре 2011 г. состоится конференция Focus 11 *(Лас Вегас 18-20 октября 2011 г.)*, на которой запланированы официальные релизы результатов совместных разработок. До текущего момента распространение любой информации о готовящихся к релизу продуктах и технологиях будет несколько преждевременным. Но с уверенностью можно сказать, что к привычным слоям защиты будет добавлен принципиально новый, находящийся "до" операционной системы, что только лишь усиливает концепцию безопасности Security Connected. С нетерпением ждем новостей из Вегаса!

Infinera: платформа для мультитерабитных транспортных сетей

Сентябрь 2011 г. – Компания Infinera (NASDAQ: INFN) представила DTN-X, первую мультитерабитную платформу для пакетных оптических транспортных сетей (P-OTN) на основе передовых фотонных интегральных схем (PIC) производительностью 500 Гбит/с. Новая платформа создана для крупных операторов, чьи сети нуждаются в увеличении пропускной способности ввиду развития видео-, мобильных и облачных сервисов. Решение DTN-X специально создано для интеграции коммутации и транспорта (DWDM) без потери производительности. Архитектура DTN-X объединяет простоту и надежность успешной платформы DTN от Infinera в новой мультитерабитной платформе, способной масштабироваться, простой в управлении и существенно снижающей количество элементов сети.