Гарантии информационной безопасности внешнего ЦОД

Обзор требований с точки зрения информационной безопасности (ИБ), которые следует предъявлять провайдеру облачных сервисов внешнего ЦОД при необходимости обеспечения корпоративного уровня ИБ.

Дмитрий Янченко – старший аналитик ИБ ЗАО "ЕВРААС.ИТ".

Растущие условия рынка заставляют бизнес добиваться все новых и новых показателей в области предоставления комплексности услуг, оперативности их оказания, прозрачности для инвесторов и регуляторов. Закономерно возрастает потребность и в вычислительных мощностях, и в серьезных процессных решениях и сервисах. Но зачастую стоимость владения такой системой и ее поддержка может превышать стоимость годового бюджета компании. В подобных случаях, как показывает практика, система собирается из "подручных" недорогих компонентов, которые кастомизируются собственными силами и объединяются всевозможными скриптами. И первый же внешний аудит информационной безопасности этой системы неприятно удивляет ее владельцев.

Для современных развивающихся компаний гораздо более приемлемым как в техническом, так и в финансовом аспекте, является другой путь – аутсорсинг готовых технологий, процессов и сервисов. Компания получает все и сразу и при этом за приемлемые деньги. В настоящее время доступны несколько вариантов интеграции внешних, облачных сервисов: SaaS, PaaS и IaaS. Первая модель – SaaS – облачное приложение в виде сервисов – организуется таким образом, что клиент получает доступ к приложениям, которые находятся в облачной инфраструктуре. Где и на каком оборудовании выполняется приложение, клиент может не знать. Второй вид облачных сервисов – платформа как сервис, PaaS. Клиент может устанавливать и разрабатывать свои приложения на предоставленной платформе. Клиент контролирует приложения, имеет частичный контроль над платформой, но не контролирует инфраструктуру. Третья модель – облачная инфраструктура как сервис, IaaS. Клиенту предоставляется виртуальная архитектура, состоящая из серверов, рабочих станций и сетевого оборудования, где клиент сам может разворачивать свои собственные операционные системы, базы данных и приложения.

Почему же такой удобный способ развития до сих пор не получил заметного распространения? Наиболее часто упоминаемая респондентами причина – потеря контроля над безопасностью данных. Действительно, чем глубже уровень аутсорсинга, тем ниже уровень контроля над информационными активами. При использовании SaaS-облака в распоряжение компании поступают тонкие терминальные клиенты, подключенные к некоему черному ящику, в котором циркулирует вся информация, включая коммерческую тайну. Как в таком случае можно управлять рисками и процессами обеспечения безопасности?

Кроме того, немаловажным фактором является необходимость соответствовать требованиям регуляторов, например ФСБ, ФСТЭК, РКН, PCI SSC, для чего в компании должны быть реализованы как специфические технические решения, так и ряд мер по управлению информационной безопасностью. В случае подключения к облаку очевидно, что большая часть этих требований может быть выполнена только провайдером облачных услуг (ЦОД) или при его непосредственном участии.

Итак, если принято решение использовать облачные сервисы, необходимо решить вопросы управления информационными и операционными рисками, а также вопросы соответствия нормативным требованиям и взаимодействия с регуляторами. И решить их нужно до начала взаимодействия с провайдером. Ключевым моментом здесь будет договор с ЦОД. В нем нужно учесть все законодательные требования, требования стандартов, процедуры управления и обеспечения безопасности, а также механизмы контроля их выполнения. Для составления такого договора, как правило, недостаточно привлечь юрисконсульта – необходимы знания и практический опыт реализации множества специфичных отраслевых стандартов и подзаконных актов. Наиболее правильным будет обратиться в организацию, имеющую соответствующую аккредитацию и опыт. Назовем ее "провайдер услуг информационной безопасности", или "ИБ-провайдер".

ИБ-провайдер предоставит услуги по определению стратегии обеспечения ИБ компании, а также по ее дальнейшей реализации, определив при этом, какие мероприятия необходимо провести внутри компании, а какие включить в договор с ЦОД, а также предложит варианты передачи некоторых процессов на аутсорсинг.

Рассмотрим, для примера, стратегию приведения компании в соответствие стандарту PCI DSS. Стандарт выбран не случайно, поскольку он включает требования как по техническим мерам обеспечения безопасности, так и по организационным. Требования Стандарта применяются ко всем "системным компонентам", то есть к сетевым устройствам, серверам и приложениям, которые входят в среду данных платежных карт, либо соединяются с ней. Но виртуальные и облачные технологии имеют ряд специфических особенностей

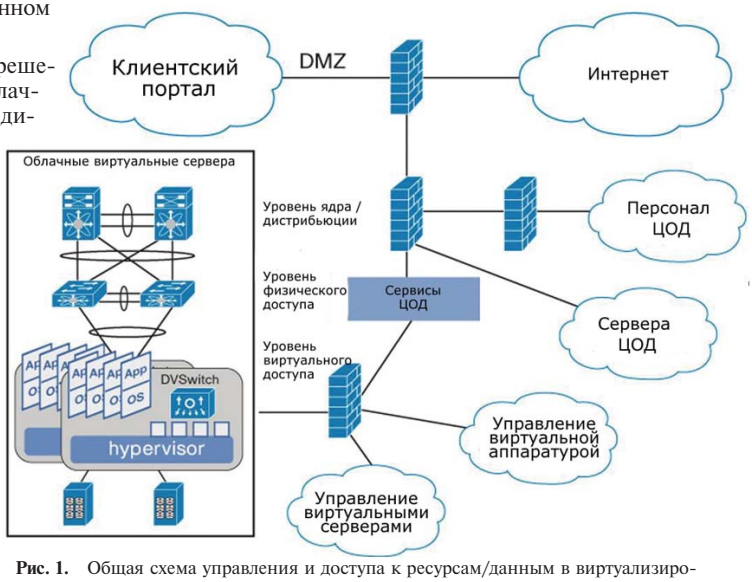

Рис. 1. Общая схема управления и доступа к ресурсам/данным в виртуализированном ЦОД.

в плане сегментации сети, хранения данных платежных карт, управления доступом, мониторинга и контроля.

В настоящее время большинство компаний аттестовано по версии Стандарта 1.2.1, в котором отсутствуют определения "виртуализация" и "облачные вычисления", и при сертификационном аудите виртуальные компоненты проверялись так же, как и физические, что иногда порождало спорные моменты. PCI DSS является одним из немногих регулирующих документов, которые регулярно пересматриваются с учетом реального практического опыта, и уже во второй версии Стандарта появились термины "гипервизор", виртуальные машины (ВМ), виртуальные приложения, виртуальные коммутаторы, маршрутизаторы и сети (рис. 1). Особенностью обеспечения безопасности виртуальной среды является наличие гипервизора и гостевых ВМ, сущности обоих типов следует защищать отдельно друг от друга и рассматривать как независимые операционные системы, к которым применимы все соответствующие требования PCI DSS. Помимо этого, необходимым является выполнение требования к гипервизору по разграничению доступа к общим ресурсам между ВМ, особенно, если речь идет о компании – поставщике хостинговых услуг, предоставляющей своим клиентам виртуальные серверы.

Пусть в рассматриваемом примере компания использует облачный сервис в качестве площадки для электронной коммерции. Компания размещает свой интернет-магазин в облаке, предоставляемом провайдером, и в этом случае, в терминологии PCI DSS, она является "мерчантом". При этом все оборудование принадлежит провайдеру, и управляется, и обслуживается им же, а облако – виртуальный ЦОД – передается в пользование мерчанту. Исходя из принципов экономии, мерчант размещает свои ресурсы, не относящиеся к обработке данных платежных карт, в том же облаке.

Облачная среда управляется совместно мерчантом и провайдером. Мерчанту, посредством клиентского портала, предоставлен ограниченный набор действий по управлению своими виртуальными компонентами. Провайдер предоставляет набор различных опций и уровней сервиса, вплоть до отдельных SLA по сетевым подключениям, безопасности, вычислительной производительности, резервированию, качеству сервиса и т.п.

Выделим и проанализируем основные риски информационной безопасности. Во-первых, нужно учесть риск привязки к провайдеру. Риск ведет к финансовым потерям вследствие повышения стоимости оплаты услуг или сложности миграции на другой ЦОД. Также следует учесть такой риск, как банкротство или поглощение провайдера, что может привести к остановке предоставления сервиса или изменению предоставляемых услуг. Следующий организационный риск состоит в потере бизнес-репутации компании-клиента, вызванный тем, что вредоносная деятельность одного из арендаторов может сказаться и на других арендаторах через блокировку ip-адресов, если производится спам-рассылка или конфискация ресурсов, если есть соответствующее постановление суда. Также существует риск потери управления, который может привести к невозможности соблюдения требований безопасности, а также ухудшению производительности и качества обслуживания.

Кроме *организационных*, при использовании облачных сервисов также возникает ряд *технических* рисков. К ним можно отнести сбои на стороне провайдера, последствием которых может стать остановка предоставления сервиса и потеря информации, что необходимо учесть при выборе ЦОД, а также определить требования и санкции в SLA. Нужно учесть, что частным случаем предыдущего риска является истощение ресурсов, к которому могут привести уязвимости в алгоритмах распределения ресурсов, атаки типа "отказ в обслуживании". Риск потери связи с провайдером грозит остановкой бизнес-процессов, поэтому плюсом будет наличие реплицируемых датацентров провайдера в нескольких регионах, резервные каналы связи, в том числе спутниковые, наличие резервной копии критичных систем в частном облаке. Для обработки риска перехвата информации при передаче необходимо использовать криптографию, а также контролировать исполнение пользователями правил безопасности. Риск невозможности уничтожения информации может привести к утечкам информации и санкциям со стороны регуляторов. Наконец, злоумышленники могут взломать непосредственно интерфейс управления, ведь каждая облачная архитектура зависит от программного обеспечения, которое может содержать критические уязвимости, например, в гипервизоре.

Помимо обработки перечисленных бизнес-рисков, для приведения компании в соответствие стандарту PCI DSS необходимо организовать **процессы** обеспечения и управления информационной безопасностью.

В качестве критериев оценки полноты и качества процесса **обеспечения защиты** данных могут использоваться свидетельства, подтверждающие и описывающие:

- методы и средства разделения данных разных клиентов;
- характеристики системы хранения данных;
- средства обеспечения конфиденциальности, целостности и доступности;
- механизмы контроля доступа и контроля утечек данных;
- средства защиты данных между клиентом и провайдером, а также между площадками провайдера.

Для организации процесса **управления уязвимостями** необходимо регламентировать процедуры внешнего и внутреннего сканирования сети и приложений, а также определить ответственность за устранение уязвимостей. Для оценки полноты функций **мониторинга и регистрации** необходимо проверить задействованные системы, объемы и сроки хранения логов, а также рассмотреть возможности хранения логов во внешнем хранилище.

Немаловажным является и процесс **управления идентификацией**. Необходимо проработать возможности интеграции каталогов учетных записей ЦОД и заказчика, выяснить вопросы защиты и управления базой учетных записей провайдера, рассмотреть варианты использования SSO.

Физическая безопасность – отдельное требование PCI DSS, поэтому необходимо убедиться, что контроль доступа в помещениях ЦОД осуществляется в режиме 24x7, при этом доступ персонала к данным клиентов регистрируется. Также нелишним будет узнать об инфраструктуре ЦОД – выделенная она или разделяемая с другими компаниями, а также про порядок набора персонала в штат.

Для обеспечения **безопасности приложений** необходимо использовать рекомендации OWASP при разработке, проводить процедуры тестирования как внешних приложений, так и собственного исходного кода. Также в качестве мер защиты необходимо использовать web-application firewall и проводить регулярный аудит баз данных.

При построении процесса **управления инцидентами** необходимо проверить наличие и выполняемость плана реагирования на инциденты в ЦОД, после чего доработать или создать собственный план, обеспечив взаимосвязь механизмов управления инцидентами. Помимо этого, необходимо убедиться в наличии и актуальности Плана обеспечения непрерывности бизнеса и восстановления после катастроф, изучить характеристики резервных площадок и каналов связи.

Обозначенные процессы – необходимое условие соответствия стандарту PCI DSS. Понятие "процесс" подчеркивает тот факт, что приведение в соответствие – не разовая процедура, а переход компании на новый уровень менеджмента ИБ. И на этом уровне логично выделяются два вида сервисов – сервисы обеспечения ИБ и сервисы управления ИБ. Задачи обеспечения ИБ в техническом плане сводятся к установке, настройке и обслуживанию средств защиты информации. Данные работы могут быть выполнены совместно ЦОД и заказчиком, причем не исключено, что и ЦОД, и заказчик для этих целей могут привлекать специализированную компанию на аутсорсинг.

Но для решения задач управления информационной безопасностью, реализующих функции контроля полноты и качества сервисов обеспечения ИБ, привлечение внешнего ИБ-провайдера является обязательным условием. Мировой опыт, лучшие практики и стандарты однозначно заявляют, что функции исполнителя и контролера не должны совмещаться в одном лице, и это правило работает в любой сфере, не только в информационной безопасности. На самом деле, подразделения, в чьи функции входит обслуживание и сопровождение технических средств не мотивированы на тщательный контроль эффективности защиты, и не способны на объективный анализ своих действий. По материалам Forrester Research, наиболее часто на аутсорсинг ИБ передают следующие задачи: мониторинг событий ИБ, управление логами, управление уязвимостями, обеспечение безопасности приложений, управление инцидентами, обеспечение безопасности контента, управление политиками и соответствием регулирующим требованиям.

В качестве примера можно рассмотреть некоторые услуги, предоставляемые нашей компанией в данном направлении.

Автоматический аудит безопасности сети

ИБ-провайдер предоставляет технологии обнаружения и исследования угроз для повышения безопасности сети и передачи актуальных данных о защищенности клиентам. Данная услуга предоставляется на базе решения McAfee Risk Advisor. Передовой механизм определения обнаруживает

узлы, сервисы и устройства в сети и проверяет эту инфраструктуру каждый день для поиска последних уязвимостей, которые могут быть использованы киберпреступниками. Свыше 400 исследователей угроз McAfee Labs непрерывно обновляют все расширяющуюся базу данных уязвимых мест в интернете, электронной почте, системе, сети и технологиях данных. Простые отчеты дают возможность исправить любые недостатки, в том числе выявленные уязвимости, предоставляя прямые ссылки на необходимые обновления и помогая с правильной конфигурацией. Между проверками служба предупреждений уведомляет клиентов о новых угрозах. Благодаря глобальной системе оперативного оповещения об угрозах (Global Threat Intelligence), пробелы в защите заполняются максимально быстро. Несмотря на эффективность, обработка уязвимостей – простой в использовании процесс: трудозатраты на установку или поддержание в работоспособном состоянии программного или аппаратного обеспечения минимальны. Централизованный портал обеспечивает ролевой доступ к информации о детальной ревизии уязвимостей. Обширный инструментарий предоставляет возможности выполнять проверки, изучать данные об уязвимостях, строить графики, иметь доступ к обновлениям, настраивать предупреждения, генерировать настраиваемые отчеты и т.д. Сервис включает поддержку пользователей онлайн, по электронной почте, по телефону со стороны сертифицированных специалистов по безопасности.

Безопасность веб-приложений

Данная услуга не требует установки аппаратного обеспечения и является легкой в применении. Весь веб-трафик маршрутизируется через ЦОД, где информация проверяется с помощью современных технологий безопасности с целью обеспечения всесторонней защиты. Отсутствие задержки и неограниченная масштабируемость в пределах предприятия позволяют обеспечивать производительность и надежность, достаточную для защиты даже самых распределенных организаций. Если в организации уже используется фильтрация веб-содержимого, данный сервис добавляет к ней дополнительные уровни защиты и обеспечивает защиту филиалов и мобильных пользователей. При обеспечении услуги используются сложные технологии анализа характера, намерения и поведения активного содержимого веб-страницы, обеспечивая упреждающую защиту от неизвестных вредоносных программ, смешанных угроз, поддельных сайтов и направленных атак. Наличие более сотни категорий фильтрации веб-содержимого обеспечивают гибкость с точностью и безопасностью, категории настраиваются индивидуально, в зависимости от рода деятельности организации.

Безопасность серверов и рабочих станций

ИБ-провайдер обеспечивает необходимую защиту от вирусов, шпионских программ, интернет-угроз и хакерских атак и предоставляет совершенные средства защиты сетевого трафика и электронной почты. В качестве такого средства может использоваться McAfee Total Protection – единое интегрированное решение, защищающее системы и данные от изощренных вредоносных программ, атак "нулевого дня" и от несанкционированных устройств. Данный сервис автоматизирует интерактивные средства защиты, позволяет сократить издержки и оптимизировать развертывание элементов систем безопасности, установку обновлений, проведение модификаций и управление. Единственное интегрированное решение исключает необходимость использования множества продуктов обеспечения безопасности. Список поддерживаемых платформ довольно обширен:

- Windows Server 2008/2003, Hyper-V, Core, Datacenter, Storage Server, Cluster Server, Small Business Server;
- Windows Server 2000, Advanced Server, Small Business Server;
- VMware ESX, ESXi;
- Citrix XenDesktop и XenServer;
- HP-UX 11.0, 11i, 11i v2/v3;
- IBM AIX 5.2, 5.3, 6.1;
- Linux Kernel 2.4 (32-разрядная версия) и 2.6 (64-разрядная версия);
- Solaris 8, 9, 10 (32- и 64-разр. версии);
- поддержка для Citrix MetaFrame 1.8 и XP;
- файловый сервер EMC Celerra.

Контроль целостности

ИБ-провайдер использует технологию непрерывного контроля целостности файлов, которая определяет все изменения в режиме реального времени при чрезвычайно малом влиянии на производительность системы. Тот факт, что контроль целостности файлов производится непрерывно, позволяет избежать процедур многократного ресурсоемкого сканирования всех системных компонент, а также позволяет выявлять такие случаи, когда конфигурационный файл был изменен злоумышленником, а затем возвращен в исходное состояние.

Непрерывный мониторинг

ИБ-провайдер управляет журналами протоколирования событий серверов, баз данных и сетевых устройств и хранит их в центральной базе данных. Базу данных можно защитить для предотвращения доступа привилегированных пользователей, включая администраторов, к конфиденциальным приложениям и данным, выходящим за пределы их полномочий.

Контроль конфигураций

Данный сервис позволяет организациям создавать стандарты конфигурации для сетевых устройств и обеспечивает возможность контроля за соблюдением установленных правил в режиме реального времени. Все изменения конфигурации отслеживаются с поддержкой версионности для удовлетворения требований раздела 10 стандарта PCI DSS, предъявляемым к журналам протоколирования событий. Также предоставляется возможность создавать политики отката к "надежной конфигурации устройства" при обнаружении любого несанкционированного изменения конфигурации. Решение предотвращает внесение несанкционированных изменений в критически важные системы и настройки систем. Оно защищает критичные файлы и параметры систем как от несанкционированного чтения, так и от записи. Данный сервис гарантирует, что вноситься в систему будут только санкционированные изменения с помощью централизованного процесса рассмотрения и утверждения. Ограниченное количество изменений, вносимых по факту, повышает доступность услуги и обеспечивает постоянное соответствие для критически важных серверов.

Единый портал управления

Единая централизованная консоль снижает стоимость владения за счет предоставления единого интерфейса управления соответствием и подготовкой отчетности. Используя данную платформу, ИТ-подразделения значительно сократят расходы на аппаратное обеспечение, обучение, а также снизят эксплуатационные издержки, получив при этом унифицированный контроль над политиками и защитой систем предприятия. Сотрудники, работающие над обеспечением соответствия, и аудиторы могут воспользоваться преимуществами данной платформы для подготовки собственных отчетов, проведения оценки или адаптации отраслевых норм соответствия без привлечения ИТ-ресурсов или выполнения задач в ручном режиме.

Итак, для того, чтобы деятельность рассматриваемой в нашем примере компании соответствовала стандарту PCI DSS, ей необходимо организовать описанные выше процессы управления безопасностью, при участии и поддержке ИБ-провайдера. Сложность здесь заключается в том, что указанные процессы должны одновременно охватывать и саму компанию, и ЦОД. Возможна ситуация, когда ЦОД уже имеет доверенного ИБ-провайдера, реализующего функции внешнего контроля. В таком случае лучшим вариантом было бы привлечь данного ИБ-провайдера и для приведения самой компании мерчанта в соответствие с требованиями стандарта PCI DSS, это обеспечило бы максимальную полноту и объективность оценки состояния ИБ. Но, если мерчант и ЦОД обслуживаются у разных ИБ-провайдеров, это тоже вполне нормальная ситуация. Главное – скрепить обязательства и ответственность договором.

В договор необходимо включить определение требований и контроль их исполнения, закрепить цели и показатели качества сервиса, а также штрафные санкции. Не следует забывать про интеллектуальную собственность – в договоре необходимо определить, кому принадлежат права на информацию, переданную облачному провайдеру, в том числе на резервные копии, на реплицированные данные и даже на логи. Нельзя допускать, чтобы контракт приводил к потере прав на информацию и иные ресурсы, переданные провайдеру. И еще один важный момент договора – процедура завершения контракта. Здесь определяется, как будут возвращаться данные, в каком формате, в какие сроки, как будут уничтожены все резервные и иные копии.

В качестве резюме хотелось бы отметить, что переход на использование облачных сервисов – это не просто шаг, это новая модель ведения бизнеса. При этом качественно меняется вся стратегия безопасности компании – происходит пересмотр "периметра ИБ", рисков, угроз и требований по безопасности. Облачные технологии изначально строятся в расчете на более высокий уровень отказоустойчивости и надежности. И тенденции таковы, что обеспечить безопасность в облаке будет в ряде случаев и проще, и эффективнее.

Дмитрий Янченко,
старший аналитик ИБ ЗАО "ЕВРААС.ИТ"