PCWEEK RUSSIAN EDITION REVIEW
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И РЕШЕНИЯ ДЛЯ БИЗНЕСА
ИТ-БЕЗОПАСНОСТЬ
МАЙ • 2012 • МОСКВА
http://www.pcweek.ru

Безопасность облачных сред

ВАЛЕРИЙ ВАСИЛЬЕВ

Проведенный компанией IDC в прошлом году международный опрос свидетельствует о том, что сегодня на традиционную модель использования ИТ тратится только половина ИТ-бюджетов, и за ближайшие два года эта доля сократится до 37%. Остальная часть средств, выделяемых на ИТ, предназначается для построения и поддержки облачных ИТ.

ОБЗОРЫ

Недавнее исследование, инициированное корпорацией Microsoft, показало, что больше половины отечественных владельцев среднего и малого бизнеса (СМБ) считают, что облачные технологии станут основой ИТ-инфраструктуры их компаний в самом ближайшем будущем. Однако при столь оптимистичных оценках перспектив развития облаков вопросы их безопасной эксплуатации по-прежнему вызывают беспокойство у пользователей.

В нашем обзоре мы рассмотрим специфику организации защиты облачной ИТ-инфраструктуры. Для этого мы дали слово экспертам — разработчикам ИБ-средств, специализирующимся в этой области интеграторам, представителям корпоративных ИТ-пользователей, имеющим опыт внедрения облачных решений.

Основные факторы влияния на ИБ облачных сред

Как отмечает Валерий Корниенко, руководитель по стратегическому развитию сервисного бизнеса, "IBM в России и СНГ", постепенно происходит смена концепции информационной безопасности от идеи защищенного периметра к облачной модели защиты приложений, данных и сервисов. На практике при миграции в облака потребуется найти баланс между централизованными мерами обеспечения ИБ, ответственность за которые несет поставщик инфраструктурных услуг, и локальными, обеспечиваемыми клиентом.

Соответственно первое, что нужно сделать при построении защиты облаков, это определить, кто и какие ресурсы облака контролирует. Это обусловлено самой организацией облаков, отмечает системный архитектор центра ИБ компании "Инфосистемы Джет" Юрий Сергеев. Задача провайдера, по его мнению, заключается в создании базовой защищенной среды, в которой данные разных клиентов услуг будут изолированы друг от друга, а также в обеспечении контроля действий своих системных администраторов.

Потребителю облачных ИТ-услуг, как предупреждает директор по ИБ "Microsoft в России" Владимир Мамыкин, по-прежнему нужна сильная собственная ИБ-команда, но с другими, нежели ранее, компетенциями и с более высоким статусом в компании. Она должна уметь управлять ИБ-рисками в условиях неполного контроля за процессами обработки информации, интегрировать ИБ-контроль во внутренние процессы провайдера и своей организации, взаимодействовать с провайдерами облаков на основе формальных контрактов.

В облаках, как отметил Евгений Царев, начальник отдела решений ИБ компании "Техносерв", архитектурные и технологические факторы влияния на ИБ уходят на второй план на фоне организационных. Большую роль начинают играть правовые аспекты и разделение ответственности между клиентом и провайдером облачных сервисов, что порождает множество вопросов, связанных с организацией процесса предоставления и потребления ИТ-услуг.

Оба — клиент и провайдер — заинтересованы, как подчеркивает ведущий инженер департамента информационной безопасности "Ай-Теко" Иван Бадеха, в максимальной детализации предоставляемых услуг и формальном закреплении ответственности. Грамотно составленные договор на оказание услуг и соглашение об уровне обслуживания (SLA), по его мнению, могут иметь решающее значение при возникновении спорных ситуаций.

Заместитель руководителя направления "Защита виртуальных инфраструктур" компании "Код Безопасности" Мария Сидорова отмечает, что больше всего споров вокруг аспектов облачной ИБ вызывает доверие к провайдеру услуг, с которым клиент разделяет ответственность за ИБ. Выделяя требования, которые следует предъявлять к облачным провайдерам, она ссылается на документы Cloud Computing Information Assurance Framework (ENISA), Security Recommendations for Cloud Computing Providers (BSI), The Cloud Security Alliance Consensus Assessments Initiative (Cloud Security Alliance) и Security Assessment Provider Requirements and Customer Responsibilities (NIST).

Среди факторов, затрудняющих защиту облачных сред, г-н Сергеев называет минимальный уровень ответственности по SLA со стороны провайдеров, а также: отсутствие:

- зрелых стандартов, классифицирующих облачные среды и регламентирующих их взаимодействие с другими системами;
- полнофункциональной защиты информации в интерфейсах прикладного программирования (API), предназначенных для взаимодействия с облаком, — аутентификации, авторизации, шифрования, аудита и мониторинга;
- устоявшейся практики реализации в облачных средах действующих ИБ-стандартов;
- интероперабельности различных облачных сервисов друг с другом;
- организационной и технической возможности контроля состояния защищенности информации у клиентов.

Критерии ИБ для облачных сервисов

Основные ИБ-критерии при использовании облаков, как считает вице-президент ассоциации RISSPA Денис Безкоровайный, различаются у разных компаний и для разной информации. Например, если компания использует сервис доставки контента для хранения и распространения рекламных видеороликов, задача по обеспечению конфиденциальности не стоит. Если же речь идет об облачном бухгалтерском учете, то необходимо не только защищать данные, которыми эти системы оперируют, но и выполнять нормы законодательства, относящиеся к их защите.

Г-н Бескоровайный напоминает, что на сегодняшний день наиболее полное описание основных мер и процессов ИБ, которые должны быть реализованы провайдером облачной услуги и клиентом, дано в документах организации Cloud Security Alliance — Cloud Control Matrix и Consensus Assessments Initiative Questionnaire (последний доступен на русском языке на сайте ассоциации RISSPA — российском отделении Cloud Security Alliance). В этом документе структурированы сведения о мерах защиты и процессах ИБ, затрагивающие основные области: физическую безопасность, управление доступом, проверку персонала, планирование аудита, программу управления ИБ, юридические вопросы, технические средства обеспечения ИБ и защиты данных, вопросы безопасной разработки приложений, обеспечение непрерывности бизнеса и др.

К основным ИБ-критериям, с которыми пользователям следует подходить к провайдерам облачных сервисов, г-н Сергеев относит:

- гарантию пропускной способности канала до облачного сервиса;
- изолированность модели предоставления услуг на уровнях сети, ОС, СУБД и приложений;
- обеспечение конфиденциальности данных с возможностью контроля состояния защиты со стороны клиента;
- гарантированное удаление данных без возможности их восстановления третьими лицами после передачи облачного ресурса от одного клиента другому;
- доверие к платформе исполнения с точки зрения ее защищенности в целом.

Поскольку, как полагает продакт-менеджер компании OCS Денис Дерюгин, для клиента облачных услуг прежде всего важно обезопасить свои данные, самым главным критерием он считает доверие к поставщику услуг, которое подкрепляется такими мерами, как шифрование и резервное копирование данных, обеспечение катастрофоустойчивости услуги, идентификация пользователей, защита данных при передаче (в том числе при передаче внутри облака), изоляция пользователей друг от друга, организация соответствия нормативным требованиям.

ИБ-риски и угрозы, специфичные для облачной архитектуры

Руководитель направления общесистемного ПО компании CPS Илья Коношевский, напоминает, что облако включает в себя облачные вычисления, облачные сервисы и виртуализацию, представляющую собой технологию, на которой во многом базируются облачные вычисления.

Если традиционные средства защиты работают на уровне операционных систем и аппаратной части ИТ-среды, то важнейший компонент облака — средства виртуализации — расположен между ними и, как напоминает г-н Бадеха, тоже требует защиты, в том числе от администраторов виртуальной инфраструктуры, от перегрузки аппаратных ресурсов, от некорректного обращения с данными разных клиентов при их совместном хранении.

Директор по развитию бизнеса компании "Информзащита" Андрей Степаненко указывает на то, что традиционными ИБ-средствами невозможно обнаружить нарушение прав доступа к средствам управления виртуальной инфраструктурой. Он также обращает внимание на появление в виртуализованных средах нового слоя привилегированных пользователей — системных администраторов поставщика услуг, которые имеют доступ к данным виртуальных машин.

По мнению г-на Безкоровайного, архитектура облачных сервисов, которая как раз и определяет возможные ИБ-риски и уязвимости, остается непрозрачной для тех, кто их защищает на стороне клиента. Он считает, что российским провайдерам облачных услуг сегодня не хватает мотивации для построения действительно надежных ИБ-систем, и если на развитых ИТ-рынках выстроенная и проверенная независимыми аудиторами ИБ-система для облачной услуги является необходимым атрибутом для привлечения клиентов, без которого провайдер не попадает в список поставщиков для крупных контрактов, то в России в силу неразвитости рынка облачных сервисов о безопасности часто не думают вообще — ни провайдеры, ни клиенты.

В России провайдеры воспринимают ИБ не как конкурентное преимущество, а как статью расходов, которой лучше избегать до появления более зрелых в вопросах ИБ клиентов. Исключение, по мнению г-на Безкоровайного, составляют частные облака и облака крупных интеграторов.

Хорошей отправной точкой подготовки к проведению анализа рисков для облачных сред г-н Безкоровайный считает документ Cloud Computing Security Risk Assessment. Benefits, risks and recommendations for information security, разработанный агентством European Network and Information Security Agency (ENISA), в котором систематизированы основные риски и уязвимости облачных сред с позиции клиента. В частности, к критическим там отнесены следующие риски:

- привязка к одному облачному провайдеру, без возможности легко его сменить;
- ошибки изоляции между ресурсами в облачной архитектуре, из-за чего возможны утечки данных;
- нарушения требований законодательства в связи с использованием облачных сред;
- действия злоумышленников из числа привилегированных сотрудников облачного провайдера;
- неполное удаление данных в облачной инфраструктуре.

Чтобы минимизировать ИБ-риски, пользователям облачных ИТ, по мнению г-на Бадехи, кроме основного договора на предоставление услуг следует продумывать и оформлять договоры об уровне услуг, соглашение о конфиденциальности, поручения на обработку персональных данных (ПДн), включающее требования к классу информационных систем ПДн, договориться с провайдером о предоставлении информации об архитектуре и других пользователях облака для составления модели угроз и оценки рисков, об основных механизмах организации ИБ на его стороне.

Помочь в снижении ИБ-рисков, с которыми сталкиваются пользователи облаков, могут ИБ-стандарты для облачных сред. Правда, как отмечает г-н Степаненко, они находятся в стадии разработки.

Наиболее уязвимые компоненты облачных сред

Как напоминает Святослав Редько, ведущий архитектор отдела инфраструктурных проектов компании HP, защищать следует

не компоненты облака, а информацию, обращающуюся в нем, при этом нужно учитывать, что разную информацию и защищать следует по-разному. Наиболее очевидным компонентом, требующим защиты во всех облачных моделях, эксперты считают защиту управляющих интерфейсов и API облачных сервисов.

По причине разнородности облачных сред однозначного ответа на вопрос, какие компоненты облачных сред являются наиболее уязвимыми и требуют первоочередного внимания со стороны обеспечения ИБ, по мнению г-на Сергеева, нет. Вместе с тем наиболее уязвимыми он считает сервисы, доступные из внешних сетей, особенно при слабой реализации ИБ в интерфейсе взаимодействия с облаком API. Целевым атакам, по его наблюдениям, подвергаются те сервисы, которые обеспечивают изоляцию между данными клиентов услуг облака: для SaaS — это сервер приложений; для PaaS — платформа, которая является средой разработки приложений для данного типа облаков; для IaaS — гипервизор и другие компоненты виртуальной инфраструктуры.

Наиболее актуальными для корпоративных клиентов облачных сервисов г-н Бадеха считает компрометацию клиентских устройств доступа в облако, перехват данных при передаче по незащищённым каналам связи и несанкционированный доступ к среде виртуализации.

Наиболее уязвимым звеном в предоставлении облачной услуги, по мнению г-на Дерюгина, является ее конечный пользователь. Он не сильно задумывается об ИБ-угрозах и нарушает ИБ-политику далеко не всегда по злому умыслу. Именно поэтому при переходе в облака контроль выполнения ИБ-политики становится особенно актуальным.

Заместитель генерального директора компании "Аладдин Р.Д." Алексей Сабанов рекомендует пользователям облачных сервисов для обеспечения конфиденциальности хранить в облаках обезличенную (зашифрованную) информацию, для обеспечения доступности наладить гарантированную строгую взаимную аутентификацию "пользователь — ресурс" а целостность информации поддерживать с помощью квалифицированных электронных подписей.

Алексей Петров, ИТ-директор "ИНФРА Инжиниринг", отмечает, что лицензирование ПО в облачной архитектуре тоже представляет собой существенную проблему как с фискальной точки зрения, так и с технической. Облачная архитектура предполагает динамическое перераспределение ресурсов, к которым относится и ПО. Потребитель облачных услуг должен иметь возможность динамически изменять количество лицензий ПО и платить за них соответственно потреблению. По его наблюдениям, далеко не все вендоры готовы предложить динамическое лицензирование своих программных продуктов, что снижает экономическую эффективность использования облаков.

Готовность ИБ-индустрии к защите облачных ИТ-сред

Наши эксперты считают, что традиционные средства защиты информации недостаточно эффективны против новых, специфичных для облаков, ИБ-угроз. Оптимальным вариантом они считают комбинацию из традиционных и специально предназначенных для облаков средств защиты. При этом, как утверждают некоторые эксперты, далеко не все облачные ИБ-продукты проработаны не только как методы, но даже как идеи. Нужны доверенные операционные системы, компонентные среды, гипервизоры, средства защиты для систем виртуализации, нужны технологии организации доверенных сеансов доступа для массовых облачных пользователей.

Вместе с тем есть и более оптимистичные оценки. Как отметил Валерий Корниенко, платформы для построения решений на основе виртуальных сред переместились из категории уникальных внутренних и специализированных инфраструктур в категорию продуктов и предложений для открытого рынка и обеспечение ИБ таких сред перестало быть задачей, решаемой при каждом внедрении индивидуально. Необходимые для этого продукты уже представлены на рынке.

Г-н Царев также отмечает, что на рынке уже есть комплексные решения, которые позволяют не только обеспечить защиту информационных активов в облачной инфраструктуре, но и сделать эту защиту гибкой, адаптивной и эффективной, в том числе и по затратам, — дело упирается в квалификацию специалистов, реализующих систему защиты.

Согласно наблюдениям г-жи Сидоровой, на российском ИБ-рынке уже существуют проверенные на практике многими российскими компаниями решения, способные не только нейтрализовать специфические облачные угрозы, но и обеспечить соответствие мировым и отечественным стандартам и практикам, а также российскому законодательству.

Г-н Степаненко тоже уверен, что у ИБ-производителей есть широкий спектр готовых продуктов, которые разрабатывались специально для облаков и учитывают угрозы, появившиеся с новыми технологиями. Основное препятствие их распространения — незначительный опыт эксплуатации из-за малого числа внедрений.

По наблюдениям г-на Бадехи, за последние два года ИБ-индустрия сумела предложить рынку ряд конкурирующих ИБ-решений для облаков. Обеспечение безопасности облачных сред перестало быть задачей, решаемой при каждом внедрении индивидуально. Из принципиально новых ИБ-технологий, по его мнению, следует ожидать в будущем реализации разграничения доступа к аппаратным ресурсам на уровне среды виртуализации и гомеоморфного шифрования, позволяющего серверную обработку данных производить в зашифрованном виде, а открытую информацию предъявлять только ее владельцу.

Влияние и готовность регулятивной базы к переводу ИТ в облака

Поскольку, как отмечает г-н Мамыкин, технологии развиваются быстрее законодательных процессов, то во всех странах сегодня пока нет документов, регламентирующих использование облаков, прежде всего в области, связанной с критической инфраструктурой стран. Он рассматривает отставание законодательства от технологий как благо, так как это не дает законодательным инициативам превращаться в тормоз технологического прогресса — законы должны поддерживать уже фактически воспринятые обществом технологии.

По мнению г-на Сабанова, отсутствие нормативной базы и ИБ-стандартов для облачных вычислений переводит сегодня использование облачных сервисов в разряд наиболее рискованных. Вместе с этим он оптимистично оценивает ближайшие перспективы регулирования ИБ в нашей стране. Он надеется, что вскоре появятся нормативные документы, в которых будут должным образом оценены риски и выданы рекомендации по защите интересов государства, бизнеса и граждан.

Как действующий практик, г-н Петров считает, что во многом вопросы обеспечения ИБ в облаках закроет сертификация вендорских облачных платформ и построенных облаков провайдеров. Однако сам процесс такой сертификации представляется отдельной большой проблемой.

Защита информации в community-облаках для enterprise-сектора

*Облачные технологии становятся все более востребованными крупными компаниями со сложнораспределенной инфраструктурой, стремящимися перейти к более эффективному предоставлению ИТ-услуг. Есть три классические категории облаков: инфраструктура как сервис (IaaS), платформа как сервис (PaaS), приложение как сервис (SaaS). Причем в крупных компаниях, оптимизирующих использование аппаратных ресурсов, сегодня наиболее уверенно растет интерес именно к IaaS. О том, как подготовить инфраструктуру к созданию облака и обеспечить необходимый уровень безопасности в облачной архитектуре, рассказывает **Юрий Сергеев**, системный архитектор Центра информационной безопасности компании “Инфосистемы Джет”.*

Юрий Сергеев

Сформулируйте, пожалуйста, основные причины повышения роли ИБ в облачных средах.

Облачные сервисы, безусловно, приносят ряд положительных эффектов. Например, позволяют значительно повысить плотность размещения систем или упростить их масштабируемость. Но облачные сервисы строятся по принципам, отличным от классических, с использованием большого числа взаимосвязанного с точки зрения ИБ программного обеспечения. Добавление компонентов приводит к тому, что возникают новые проблемы. Обычно большая часть этих компонентов имеет широкие полномочия в создаваемой системе. В случае успешной реализации атак на них защищенность информации, обрабатываемой в облаке, может оказаться под угрозой. Но кроме неопределённого внешнего злоумышленника нужно оценивать провайдера услуги и других её пользователей, которые работают на базе тех же вычислительных ресурсов и потенциально имеют большие возможности для несанкционированного доступа к доверенной оператору информации.

Какие компоненты IaaS-облака являются наиболее уязвимыми и требуют первоочередного внимания с целью обеспечения ИБ?

Однозначного ответа на этот вопрос пока не существует. Традиционно более уязвимы те сервисы, доступ к которым возможен из внешних сетей. Также под угрозой могут оказаться сервисы, которые обеспечивают изоляцию между данными подписчиков услуг облака. Применительно к IaaS это гипервизор и другие компоненты виртуальной инфраструктуры. Так, добавление элемента в систему управления виртуальными инфраструктурами приведёт к тому, что, взломав эту систему, злоумышленник получит доступ ко всей циркулирующей в виртуальной среде информации. Кроме того, взлом конкретного сетевого узла одного подписчика может привести не только к его компрометации. Последствием могут стать локальные escape-атаки на другие узлы прочих пользователей облака, направленные на преодоление изоляции гипервизора. Таким образом, не стоит забывать о безопасности самой платформы виртуализации, которая также неидеальна. И наконец, нельзя забывать о системах, обеспечивающих работу самой виртуальной инфраструктуры: коммутаторах, системах хранения данных, средствах управления. Все эти компоненты таят в себе угрозы нарушения конфиденциальности доверенной оператору информации, от которых, безусловно, необходимо защищаться.

Если говорить о community-облаках, какие из обозначенных вами уязвимостей сохраняют свою актуальность?

Зачастую в community-облаке доверие к оператору несколько выше, чем в публичном, так как за его реализацию обычно отвечает родственная специализированная компания. Например, головная структура или выделенная под ИТ-задачи организация, обслуживающая все компании холдинга, позволяя последним концентрироваться на выполнении бизнес-задач без оглядки на поддержку инфраструктуры. Аналогичным образом строятся и отношения с “соседями” по облаку — субъективно их редко воспринимают как нарушителей. Тем не менее построение системы защиты, в которой во главу угла ставится субъективное отношение к нарушителю, выглядит опрометчивым шагом. Обязательно нужно учитывать его потенциальные возможности в случае отсутствия ограничительных контрмер. В любом случае сложность и взаимосвязанность компонентов IaaS-облака порождает большое количество ошибок не только на этапе установки и конфигурирования, но иногда и на этапе их разработки. Поэтому главная наша задача — создать такую прозрачную защиту, которая работает незаметно для пользователя, обеспечивает изоляцию между подписчиками услуги и удобна для последних. И в этом случае особенно актуальной становится специализация на сервисной модели обеспечения информационной безопасности.

Каким образом строится защита в community-облаке с учетом обозначенных вами уязвимостей?

Мы всегда рекомендуем комплексный подход к защите, в том числе и для community-облаков. В первую очередь необходимо продумать модель разделения ответственности. Дело в том, что число администраторов может быть значительным. Более того — они могут быть территориально разобщены и действовать независимо, обладая разными мотивациями. Эта модель должна быть донесена до лица, принимающего решения о подключении к облаку, что повышает прозрачность и увеличивает доверие к поставщику услуги. И вне зависимости от места нахождения каждого конкретного администратора нужно обеспечивать контроль его действий: соответствуют ли действия политике, могут ли администраторы получить доступ к защищаемым сведениям, содержащимся в виртуальной среде. Сейчас, например, для виртуальных сред на базе VMware есть решения, позволяющие обеспечить разделение обязанностей (separation of duties) в виртуальной среде и исключить ситуацию, когда кто-либо наделяется правами суперпользователя и получает все полномочия на управление виртуальной инфраструктурой. Эта задача выглядит актуальной, особенно с учетом того, что построение community-облаков IaaS часто реализуется с применением решений VMware.

Следующим шагом становится рассмотрение каналов возможных атак. Наиболее специфичными угрозами для облачной архитектуры являются DoS-атаки из-за зависимости от сетевой инфраструктуры между облаком и подписчиком услуг и перехват аутентификационных данных для доступа к облаку через его API, а также перехват данных, отправляемых и получаемых из облака, нарушение изоляции среды, переданной подписчику в рамках облачной среды, и атаки на браузеры и другие средства доступа к облаку.

Какие средства целесообразно выбрать для защиты облачной среды?

Сегодня рынок средств защиты облачных инфраструктур бурно развивается, а его лидеры создают новые продукты и адаптируют уже имеющиеся. Уже сейчас на рынке представлены успешные продукты для защиты облачных сред компаний Symantec, Trend Micro, VMware, HyTrust, Cisco, StoneSoft и др.

Защита виртуальных сред включает две основные задачи: контроль внешнего и внутреннего периметров. А в качестве ключевых можно выделить такие направления, как управление доступом к среде виртуализации, двухфакторная аутентификация пользователей, мониторинг действий администраторов и контроль изменения конфигурации. Также к ключевым задачам следует отнести обеспечение базовых сервисов защиты виртуальных машин, погружаемых в среду с использованием специализированных средств защиты: межсетевого экранирования, антивирусной защиты, обнаружения вторжений, контроля целостности и др.

Как вы оцениваете готовность enterprise-сектора к переходу на community-облака?

Мы видим, что некоторые наши заказчики уже начали реализовывать эту концепцию у себя. И понимаем, что операционные выгоды от такой трансформации предоставления услуг сильно перевешивают все препятствия для начала этой большой работы. В свою очередь, для реализации community-облаков существует ряд решений по ИБ, позволяющих не только обеспечить уровень защиты, адекватный текущему способу оказания ИТ-услуг, но и повысить его за счет новых технических возможностей. Думаю, что после нескольких реализаций и накопления “историй успеха” первопроходцами будет наблюдаться бурный рост активности enterprise-сектора в этом направлении.

Создание защищенного частного облака

Несмотря на прогнозы Gartner о снижении объема рынка услуг в секторе облачных вычислений, в России эта тема актуальна и переживает бурный рост. Все большее число крупных и средних компаний задумывается о создании своей облачной инфраструктуры, а некоторые уже предприняли ряд серьезных шагов в этом направлении. Это не случайно: развитие рынка требует постоянного улучшения качества предоставляемых сервисов и оптимизации затрат, в том числе и на информационные технологии (ИТ). Переход на облачную платформу позволяет решить данные проблемы.

Однако перенос в облако существующей ИТ-инфраструктуры у многих до сих пор вызывает сомнения. Это связано с рисками компрометации или потери данных, несанкционированного доступа к ним и вероятных ошибок при переносе информации. Важно понимать, что из-за особенностей облачной архитектуры реализация угроз информационной безопасности (ИБ) может привести к более тяжелым последствиям, чем обычно. Например, в связи с тем, что облако представляет собой единое хранилище информации, скорость вирусного заражения и компрометации данных внутри него при отсутствии необходимых мер защиты будет существенно выше, чем в традиционной инфраструктуре. Чтобы максимально снизить значимость возможных рисков, необходимо тщательно проработать вопросы обеспечения ИБ.

В случае размещения информации в публичных облаках обеспечение ИБ осуществляет провайдер облачных услуг, а в случае частных — сам владелец ресурсов. Данная статья относится ко второму варианту, встречающемуся в России наиболее часто. Обычно процесс создания частного облака проводится в шесть этапов: оценка, консолидация, виртуализация, миграция, автоматизация и оптимизация. Для создания надежной системы защиты важно на каждом из них предпринять ряд шагов, которые позволят минимизировать значения рисков.

Оценка. На первом этапе проводится анализ потребностей бизнеса, возможных путей достижения поставленных целей, а также сравнение комплексных решений, обеспечивающих их выполнение. Основными параметрами сравнения являются производительность, отказоустойчивость, масштабируемость ИТ-инфраструктуры, надежность средств защиты. Немаловажны также стоимость внедряемых ИТ- и ИБ-решений, совокупная стоимость владения ими (TCO), скорость окупаемости (ROI).

В результате такого анализа разрабатывается стратегия развития ИТ- и ИБ-инфраструктуры, в которой определяются необходимость создания частного облака, потенциальные угрозы и нарушители, общие требования к ИТ- и ИБ-архитектуре облака.

Консолидация. На следующем этапе определяются последовательность и объем работ, необходимых для перехода на облачную платформу, а также их бюджет. Работы направлены на создание единой точки обработки данных, виртуализацию инфраструктуры, автоматизацию процессов управления и контроля и защиту платформы. Комплекс работ по обеспечению безопасности включает в себя:

- защиту каналов связи;
- шифрование данных;
- идентификацию и аутентификацию пользователей;
- контроль целостности файлов и настроек;
- управление доступом к данным и элементам инфраструктуры;
- усиленную защиту инфраструктуры виртуальных рабочих столов;
- эшелонированную антивирусную защиту;
- защиту от DDoS;
- автоматическое резервное копирование;
- защиту рабочих мест пользователей и т. д.

Также на этапе консолидации начинают разработку (или актуализацию) нормативных документов в области ИБ, связанных с дальнейшим функционированием облачной платформы. Нормативные документы должны включать вопросы обеспечения технической поддержки и защиты, распределения обязанностей, ответственности, повышения осведомленности пользователей и т. д.

Виртуализация. Следующим шагом в создании частного облака является виртуализация сетевой инфраструктуры и средств защиты. С точки зрения ИБ на данном этапе необходимо:

- ограничить полномочия администраторов виртуальной инфраструктуры;
- обеспечить надежную защиту гипервизора и средств управления инфраструктурой виртуализации;
- настроить платформу виртуализации в соответствии с существующими политиками ИБ.

Миграция в облако. На данном этапе осуществляется непосредственный перенос приложений, их настроек и данных на облачную платформу. Корректное определение способа переноса данных и их состава крайне важны с точки зрения ИБ. Поэтому прежде всего, выявляют типы обрабатываемых данных и проводят их классификацию с точки зрения критичности для бизнеса. А затем определяют безопасный способ переноса данных и их допустимый объем.

Автоматизация. На пятом этапе осуществляется автоматизация процессов управления, которые в том числе включают в себя самомасштабирование и восстановление приложений после сбоев. Автоматизировать необходимо не только бизнес-приложения, но и приложения, обеспечивающие безопасность. Также следует уделить внимание построению процессов контроля, аудита, резервного копирования и восстановления данных, мониторинга и реагирования на инциденты в области ИТ и ИБ.

Оптимизация. Это заключительный этап, на котором подводятся промежуточные итоги: оцениваются показатели эффективности и проверяется степень достижения поставленных целей. По результатам устраняются все выявленные недостатки. В целях дальнейшего совершенствования рекомендуется проводить периодический анализ уязвимостей, актуализировать модель угроз и нарушителей, нормативные документы, а также модернизировать средства защиты в соответствии с тенденциями в области ИБ.

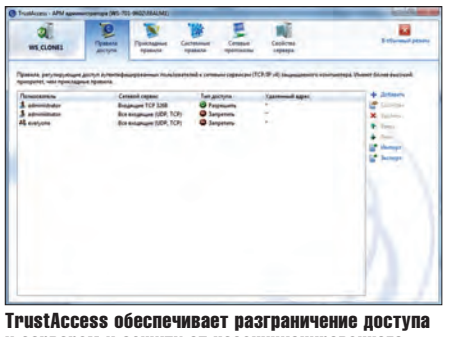
Таким образом, проблема обеспечения ИБ частного облака, несмотря на ряд особенностей, не является серьезным препятствием для перехода на облачную платформу. Более того, ее решение позволяет повысить эффективность проекта в целом. Выполнение предложенных рекомендаций к обеспечению безопасности на каждом из этапов создания облака позволит лучше управлять рисками и контролировать решение поставленных задач. Как следствие, будут минимизированы возможные финансовые и репутационные потери, связанные с компрометацией, потерей данных, их несанкционированным раскрытием, приостановкой работы внутренних и внешних сервисов и т. д.

Защита ключевых ресурсов в частном облаке

Облачные вычисления как наиболее перспективная технология, позволяющая экономить ресурсы и оптимизировать расходы на информационные технологии, вызывает большой интерес у представителей бизнеса. Крупные и средние предприятия предпочитают строить частные облака, которые зачастую работают в их собственных ЦОДах. Предприятия не очень доверяют сторонним провайдерам и, как следствие, не заинтересованы в аренде услуг публичных облаков. Но вопросы информационной безопасности стоят на первом плане при использовании и частных облаков. Уязвимость серверов, где разворачиваются облачные платформы, — серьезная проблема, с которой сталкиваются компании, внедряя облачные технологии. Помимо всего прочего характерными задачами защиты частных облаков являются угрозы инсайдерских атак, разграничение доступа на уровне ролей и должностных обязанностей, гибкость настроек и управления, соответствие законодательным стандартам. Отметим, что для публичных облаков наряду с хакерскими и DDOS-атаками также критична проблема доступа привилегированных пользователей к данным. В привычной физической среде защита организовывается путем использования периметрового межсетевого экрана, но облачные вычисления диктуют свои правила и требования — в облаке сложно выявить привычный периметр защиты.

В случае использования облачных технологий необходим подход, позволяющий защитить данные и ограничить доступ к ним неавторизованным лицам. Понятно, что традиционные межсетевые экраны не способны в полной мере справиться с данной задачей. В этом случае стоит обратить внимание на решение TrustAccess российского разработчика "Код Безопасности".

TrustAccess представляет собой распределенный межсетевой экран высокого класса защиты, предназначенный для защиты



TrustAccess обеспечивает разграничение доступа к серверам и защиту от несанкционированного доступа на сетевом уровне

ключевых ресурсов сети (серверов и АРМ) от несанкционированного доступа (НСД), а также для разграничения доступа к информационным системам. Помимо фильтрации трафика по параметрам, присущим большинству межсетевых экранов, TrustAccess обеспечивает двустороннюю сетевую идентификацию и аутентификацию пользователей и компьютеров. Решение имеет в своем арсенале механизмы защиты сетевых соединений, средства централизованного управления, возможности регистрации и учета событий информационной безопасности. Обладая широким диапазоном настроек, TrustAccess обеспечивает разграничение доступа к серверам и защиту от несанкционированного доступа на сетевом уровне.

На современном этапе основным фундаментом для организации облаков является технология виртуализации. И тут традиционные средства защиты неэффективны в борьбе со специфичными угрозами информационной безопасности в виртуальной среде. На российском рынке представлено не так много средств защиты, способных одинаково эффективно работать как в физической, так и в виртуальной средах. TrustAccess можно использовать в обеих средах. Его применение в качестве межсетевого экрана внутри сервера виртуализации позволяет контролировать сетевой трафик виртуальных машин. Контролируются как внешние соединения, так и соединения между виртуальными машинами. Благодаря защитным механизмам TrustAccess, которые нечувствительны к атакам типа подмена MAC- или IP-адресов, межсетевой экран эффективен в виртуальной среде. Он позволяет создать защиту виртуальных серверов и рабочих мест. Совместимость продукта с платформами VMware подтверждена логотипом VMware Ready.

Кроме того, для обеспечения защиты информации в частных облаках, построенных на технологии виртуализации, не обойтись без использования специализированных средств защиты, которые оградили бы от специфичных угроз среды. Доказано, что получить доступ к данным в виртуальной среде проще, чем в физической. Администратор обладает неограниченными полномочиями и доступом к пользовательским данным, скомпрометировать которые не составляет труда. Именно на решение этих задач направлен разработанный компанией "Код Безопасности" продукт под названием vGate R2. Для решения проблемы привилегированного пользователя в vGate R2 реализовано разделение ролей администраторов и введен запрет на доступ 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. Кроме того, vGate R2 позволяет создать индивидуальный шаблон безопасности на основе принятых в компании регламентов информационной безопасности.

Также не теряют актуальности требования, связанные с защитой персональных данных, которые компаниям приходится соблюдать и в корпоративном облаке. Решение TrustAccess имеет сертификаты ФСТЭК России на соответствие уровням МЭ 2 и НДВ 4, что дает возможность использовать продукт для защиты конфиденциальной информации до класса 1Г включительно и всех классов информационных систем персональных данных (ИСПДн классов К1, К2, К3). Применение же TrustAccess для сегментирования информационных систем обработки персональных данных позволяет отнести отдельные сегменты к более низкому классу и добиться снижения затрат на защиту. Решение vGate R2 имеет сертификат ФСТЭК России (СВТ 5, НДВ 4), который позволяет применять продукт в автоматизированных системах уровня защищенности до класса 1Г включительно и в информационных системах персональных данных (ИСПДн) до класса К1 включительно.

Отдельно стоит отметить, что vGate R2 включает в себя несколько шаблонов по приведению в соответствие с требованиями Федерального закона № 152-ФЗ, СТО БР ИББС, PCI DSS, VMware Security Hardening Guide, CIS ESX Server Benchmark.

Возможности TrustAccess

- Аутентификация субъектов доступа — пользователей и компьютеров.
- Фильтрация сетевых соединений с широким диапазоном настроек.
- Защита сетевых соединений.
- Гибкая настройка уровня защищенности и производительности сети.
- Регистрация событий, связанных с информационной безопасностью.
- Контроль целостности и защита от НСД компонентов СЗИ.
- Централизованное управление.