УДК 004.056

Васильев В.Н.
студент 2 курса магистратуры
факультет «Информатика и системы управления»
МГТУ им. Н.Э. Баумана
научный руководитель: Галкин В.А., к.т.н.
доцент
Россия, г. Москва

БЕЗОПАСНОСТЬ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

Аннотация. Статья посвящена некоторым аспектам облачных вычислений. Обоснована необходимость применения эффективных мер безопасности. Приведены стандарты, используемые в облачных вычислениях. Угрозы, возникающие в облачных вычислениях. Меры необходимые для стабильного функционирования облака.

Ключевые слова: облачные вычисления**,** дата-центр, ИТ-структура**,** виртуальная машина, администратор виртуальной инфраструктуры.

Облачные технологии (облачные вычисления) – это, в большинстве своем, технологии обработки данных, в которых компьютерные ресурсы и мощности предоставляются пользователю как Интернет-сервис. Пользователь имеет доступ к собственным данным, но не может управлять и не должен заботиться об инфраструктуре, операционной системе и собственно программном обеспечении, с которым работает.

«Облако» - метафора удаленного вычислительного дата-центра, доступ к которому представляется после внесения денежных средств pay-as-you-go (оплата происходит за фактическое пользование вычислительными ресурсами). Программное обеспечение предоставляется пользователю как сервис. В этом случае пользователь не заботится об инфраструктуре, программном обеспечении и безопасности «облака».

В облачных технологиях используются вычислительные мощности, оборудование и дисковое пространство, расположенные не на территории офиса. Поэтому разрабатывать собственную ИТ-структуру не обязательно, так как облачные технологии обходятся менее затратно, чем разработка собственного программного обеспечения и содержание ИТ-службы.

Облачные вычисления становятся популярнее с каждым днем и вопрос применения эффективных мер безопасности крайне важен.

Считается, что облачные вычисления - безопасны, но уверенно говорить об этом достаточно сложно. К локальным облакам можно применять уже сложившиеся технологии, обеспечивающие безопасность, и в этом проблем почти нет. Но при работе с глобальными облаками сложность систем сильно возрастает, и требуются совершенно новые методы, гарантирующие их безопасность.

Существует много мнений, что достаточно просто похитить виртуальный сервер из облака и сделать это гораздо проще, чем вынести физический сервер из ЦОД. Завладеть правами администратора так же не

составит большой трудности, а дальше уже можно скопировать всю виртуальную машину вместе с данными и спрятать ее в том же облаке.

Авторитетные специалисты уверены в неизбежности перехода в облака. Уитфилд Диффи, создавший вместе с Мартином Хеллманом алгоритмические основы криптографии с открытым ключом, обрисовал ситуацию следующим образом: «Мы попадаем в зависимость от облачных вычислений так же, как в зависимость от общественного транспорта. Увы, со многими его особенностями придется смириться, но ведь, пользуясь самолетами, мы вынуждены доверять неподконтрольным нам организациям, к тому же навязывающим нам свои условия и принуждающим нас следовать их расписанию... Да, всего этого можно было бы избежать в том случае, если бы мы могли пользоваться личными самолетами, но экономические преимущества общественного транспорта настолько велики, что у нас не остается выбора». [1]

Часто компании опасаются, что при переходе в облака создастся прямая угроза безопасности конфиденциальных данных со стороны их целостности и защищенности. Опасения вызывают несколько аспектов:

- Технологические - классические методы защиты не работают, не ясен уровень потенциальной угрозы, отсутствуют общепринятые стандарты информационной безопасности.

- Юридические - размыта область ответственности, так как речь идет об инфраструктуре, динамически меняющей свой периметр, размер, структуру.

- Психологические - ИТ-аутсорсинг в России в целом пока еще не стал привычным общепринятым явлением.

Стандарты, используемые в облачных вычислениях

Security Guidance for Critical Areas of Focus in Cloud Computing: собрание наиболее удачных практик по обеспечению безопасности в «облачных» вычислениях.

В настоящее время активно ведется разработка новых стандартов:

- ISO 27017 (Security in cloud computing) - стандарт (ISO 27017) представляет собой дополнения и уточнения к ISO 27002 Code of Practice for Information Security Management (предшественником которого является стандарт ISO 17999 и на основе которого принят ГОСТ Р ИСО/МЭК 17799-2005«Практические правила управления информационной безопасностью»);

- ISO 27018 (Privacy in cloud computing) - является дополнением к ISO 27017 и рассматривает аспекты обеспечения конфиденциальности и персональных данных в «облаках»;

- ISO 27036-5 (Information security for supplier relationships — Cloud Computing) - является руководством по оценке и снижению рисков, связанных с потреблением сервисов, которые предоставляют сторонние организации (в текущей редакции пятая часть стандарта рассматривает отношения с поставщиками при «облачной» модели предоставления сервисов). [2]

В начале 2012 года американский Национальный институт стандартов и технологий опубликовал проект 4-й редакции Специальной публикации SP 800-53 «Меры обеспечения безопасности и защиты персональных данных в федеральных информационных системах и организациях» (Security and Privacy Controls for Federal Information Systems and Organizations).

В опубликованном на сайте NIST информационном сообщении отмечается - предлагаемые в новой редакции изменения непосредственно связаны с текущим состоянием угроз (т.е. с возможностями и намерениями противников, и выбором ими целей для атак). Они также опираются на собранные и проанализированные данные об атаках за продолжительный период времени. В число основных изменений входят:

- ряд новых и улучшения уже имевшихся мер обеспечения безопасности;
- более ясный язык при формулировке требований и спецификаций для мер обеспечения безопасности;
- новое руководство по индивидуализации и настройке мер безопасности, включая создание специализированных наборов мер безопасности (overlays);
- дополнительные вспомогательные указания по мерам безопасности и их усилению;
- новые меры защиты персональных данных и указания по их внедрению;
- обновленные базовые профили мер безопасности (security control baselines);
- новые, более удобные для использования сводные таблицы мер безопасности, а также
- пересмотренные меры обеспечения уверенности (designated assurance controls) и требования в отношении минимальных гарантий (minimum assurance). [3]

В настоящее время международная организация по стандартизации (International Organization for Standardization – ISO) разрабатывает специальный стандарт, который посвящен безопасности облачных вычислений. Основная направленность – решение организационных вопросов, связанных с облаками.

Ассоциация RISSPA и российское подразделение Cloud Security Alliance (Cloud Security Alliance Russian Chapter) представили в начале 2012 года первый официальный документ – «Опросник оценки состояния безопасности облачной среды». Опросник предназначен для сбора, классификации сведений о системах защиты и процессах управления информационной безопасностью, которые используют поставщики облачных услуг.

«Русифицированный опросник позволит всем, кто рассматривает возможность использования облачных сервисов, в первую очередь, публичных, систематизировать вопросы по безопасности и защите

клиентских данных к провайдеру, используя передовую практику Cloud Security Alliance. Эта информация необходима клиентам для выполнения анализа рисков и планирования процессов взаимодействия».[4]

Провайдеры с помощью опросника смогут оперативно помогать клиентам, оперативно принимать решения по предоставляемым сервисам и будет возможность делиться информацией. Всеобщий доступ к результатам уменьшат количество дублирующих обращений к провайдерам.

Документ предоставит заказчикам нужные данные по информационной безопасности и упростит механизм обмена информацией о безопасности и защите между заказчиками. [5]

Нельзя забывать и о выполнении законодательства о персональных данных в облаке.

Правовая сторона вопроса:

- пользователь является оператором;
- поручение обработки персональных данных провайдеру;
- согласие субъекта на передачу персональных данных третьим лицам.

Организационная сторона вопроса:

- кто допущен к управлению ВМ?
- как ограничен перечень администраторов ВИ?
- кто разрабатывает модель угроз?
- должен ли провайдер услуг предоставить полную информацию об инфраструктуре облака?

Техническая сторона вопроса:

- реализация требований к подсистемам СЗПДн на уровне ВМ;
- обеспечение физических мер защиты провайдером;
- защита от специфических угроз ВИ.

Факторы, препятствующие использованию облачных вычислений

Усиление защищенности данных. Защита данных в традиционных ЦОД строится на основе физической защиты доступа к аппаратным или программным ресурсам, но в облаке все расставленные по периметру барьеры теряют смысл. Чтобы сохранить защищенность, соответствующие методы должны стать информационно-центричными (information-centric). Такого рода секретность предполагает перенос методов защиты непосредственно к данным – доступ может получить только тот, кто обладает нужными правами, в нужное время и в нужном месте.

В распределенных средах, обладающих качествами multi-tenancy (коммунальности, несколько пользователей независимо друг от друга разделяют один и тот же ресурс) и multi-instancy (индивидуальности, каждый пользователь владеет частью облака для выполнения своих приложений), данные защищаются с максимальной возможностью; это делается для исключения доступа различных пользователей к одним информационным ресурсам.

Если сравнивать Infrastructure as a Service (предоставление

унифицированных аппаратных и программных ресурсов в виде сервиса), Platform as a Service (предоставление в виде сервиса платформы для разработки) и Software as a Service (предоставление по запросу готового специализированного ПО). В случае IaaS изолировать данные проще, так как меньше границ соприкосновения. Обеспечение защиты и аутентификации нужно нацеливать на более мелкие порции данных и меньшие по размерам группы пользователей.

При обмене данными между теми, кто в облаке и вне облака, может потребоваться согласованная защищенность данных, различная для разных групп пользователей. Распределение грифов секретности должно выстраиваться таким образом, чтобы не снижалась общая производительность, для этого нужно ранжировать данные по степени их важности и величине рисков. IRM обычно распространяют только на управление идентификацией и доступом, но в облачном случае права должны быть доведены до уровня данных.

Способы решения информационной безопасности в частных облаках

Для частных облаков проблема безопасности - это проблема защиты от инсайдеров. Ее можно контролировать за счет:

- тщательного подбора персонала;
- физического контроля доступа к аппаратным средствам;
- использования дополнительных программно-аппаратных решений для шифрования/дешифрования баз данных при обработке, а также для разделения функций администрирования и доступа к данным. Все перечисленные функции клиент может контролировать самостоятельно. Это значит, что клиент должен полностью доверять сервис провайдеру, от которого он получает ИТ-услуги, если он заботится о безопасности своих данных.

Как показывает ряд исследований, проблема ИБ в публичных облаках в ближайшие годы останется актуальной. Так, компания Gartner в 2010 г. провела первое исследование, связанное с безопасностью виртуализации ("Addressing the Most Common Security Risks in Data Center Virtualization Projects", январь 2010 г.). В соответствии с ним к 2012 г. 60% виртуализированных серверов будут менее защищены, чем физические серверы, которые они заменяют. Но к 2015 г., как отмечает Gartner, эта величина снизится до 30%. [6]

Способы решения информационной безопасности в публичных облаках

Проблема информационной безопасности в публичных облаках в настоящее время решается несколькими способами:

1. За счет максимального использования частных облаков и развития виртуализации в существующих традиционных дата-центрах.
2. За счет перехода на аутсорсинг и колокацию ИТ-услуг, где вопросы

контроля доступа к данным можно жестко контролировать, одновременно добиваясь снижения стоимости капитальных и эксплуатационных затрат ИТ-услуг (например, за счет все той же виртуализации).

3. За счет передачи в публичные облака только тех ИТ- сервисов, для которых:

- утечка данных не является критичной для компании;

- утечка данных затруднена из-за того, что они всегда зашифрованы (дополнительные резервные копии), дешифрование которых происходит только на стороне клиента.

4. Решением для некоторых была бы возможность онлайновой криптографии при обработке только наиболее критичных данных: данный подход в настоящее время достаточно сложен для массового использования.

При переносе обработки конфиденциальных данных в виртуальную среду проблема утечки конфиденциальной информации резко возрастает, в основном, из-за наличия “суперпользователя” в лице администратора виртуальной инфраструктуры (АВИ).

Основная проблема в том, что АВИ могут получить доступ к обрабатываемым конфиденциальным данным внутри виртуальных машин (ВМ) даже при выключенных ВМ. При этом все можно все сделать по сети, без физического доступа к инфраструктуре виртуализации. Любые системы защиты, находящиеся внутри операционной системы ВМ, в этот момент выключены, следовательно, суперпользователь может замести следы, очистив логи системы виртуализации, получив доступ к информации и скрыв следы преступления.

Угрозы, возникающие в облачных вычислениях:

- Несанкционированное взаимодействие между виртуальными машинами и хостами

Теоретически инфраструктура облака должна исключать любое взаимодействие между отдельными виртуальными машинами или виртуальными машинами и физическими машинами, на которых они работают. Однако подобного рода взаимодействие возможно через общие или распределенные области обмена данными (shared clipboard), оставляющие лазейку для распространения паразитных кодов. Примерно такую же возможность создают технологии виртуализации, использующие общий для всего хоста буфер хранения введенных с клавиатуры символов. Иногда считается, что в случае, когда виртуальная машина и хост работают под управлением разных операционных систем, утечка такого рода невозможна, но это утверждение доказательства еще не получило.

- «Побег» виртуальной шины

При плохой изоляции от хоста специально созданная виртуальная машина может «совершить побег» (VM Escape) – то есть она проходит сквозь гипервизор и захватывает управление хостом. Если целью побега является захват других виртуальных машин, это явление называют «перескакиванием» (VM Hopping).

- Слежение со стороны хоста

Виртуальная машина работает на хосте и под его управлением, если не будут созданы специальные барьеры, то хост может получить доступ к данным виртуальных машин. Данная ситуация недопустима, создаются условия для тотальной слежки в облаке.

- Слежение со стороны виртуальной машины

Процессоры и гипервизоры со встроенной защитой памяти исключают взаимное наблюдение между виртуальными машинами, но изолированность может быть нарушена на уровне сетевого трафика, при использовании машинами «виртуального коммутатора». В этом случае возможна кража или переадресация передаваемых пакетов данных.

- Атаки в облаке

При недостаточной изоляции в облаке может быть создана DoS-атака, выводящая из строя все облако, или локальная атака одной виртуальной машины на другую.

- Внешние модификации

Целью внешних атак может быть изменение кодов гипервизора и приложений, работающих на виртуальных машинах.

Перечисленные выше угрозы раньше не возникали, в связи с этим их невозможно устранить существующими технологиями.

Меры, необходимые для стабильного функционирования облака

- Физическая защита.

Оборудование должно быть обеспечено бесперебойным питанием и находиться под климат-контролем, обязательно должны быть предприняты противопожарные меры.

- Безопасность сети и логическое разделение.

Обязательным для облака является использование виртуальных версий файрволов и IDS. Должны быть изолированы те части облака, в которых хранится критическая информация. Проверки системы должны проводиться регулярно с использованием различных признанных стандартов и методов.

- Проверка

На шлюзах должны быть установлены антивирусные приложения и фильтрация контента. При проверке критических данных (персональные данные, интеллектуальная собственность) в дополнение к проверке необходимо применять меры по предотвращению потери данных.

- Администрирование

Облачным гипервизорам и серверам, на которых работают многие операционные системы, необходимо уделить особое внимание, они обеспечивают возможность управления всем облаком. Для обеспечения разделения обязанностей и усиления уровней безопасности требуется наличие разных сетей и администраторов. Ограничение доступа к управлению облачной средой, в том числе заблокированы и отключены API приложения.

- Всесторонний мониторинг и регистрация

Все стандарты безопасности требуют наблюдения и контроля доступа к сетям, системам, приложениям и данным, то же правило применимо и к облакам.

- Безопасность системы

Виртуальные машины обязательно защищаются специальными облачными брандмауэрами, антивирусными и IPS приложениями. Также последовательно и постоянно внедряются патчи.

- Безопасность приложений и данных

Доступ к базам данных через приложения должен быть строго ограничен, приложения должны использовать только выделенные базы данных. Большое количество стандартов безопасности требуют проведения мониторинга и регистрации приложений и соответствующих баз данных.

- Аутентификация и авторизация

Двухфакторная аутентификация обязательна при удаленном и любом другом привилегированном доступе и должна применяться при введении имени и пароля пользователя. Роль аутентифицированного пользователя должна быть четко определена и минимизирована для выполнения определенного задания. Обязательным является шифрование паролей. Пакеты аутентификации, авторизации и учета использования ресурсов не должны быть сильно кастомизированные, поскольку это обычно ведет к уязвимостям.

- Управление уязвимостями

Приложения, находящиеся в облаке, должны постоянно обновляться, проходить независимые тесты на безопасность, сканироваться на уязвимости и непрерывно отслеживаться.

- Хранение данных

Организация должна быть осведомлена о хранимой в облаке информации, при необходимости она сортируется. Для проведения изменений должно быть известно физическое и логическое расположение данных.

- Управление изменениями

Избежать потерь при изменении может помочь аккуратно и понятно задокументированная политика управления изменениями для сети, систем, приложений и администраторов.

- Шифрование

Многие стандарты содержат требования для шифрования данных в момент передачи и хранения. Шифрование данных в облаке – достаточно сложный процесс, который требует особого внимания.

- Повышение надежности идентификации

В облачных условиях актуально направление управлением идентификацией и доступом (Identity Management, IM) и решения обеспечения безопасности на основе контроля за идентификацией (Identity-Based Security, IBS). Ключевыми моментами облачной безопасности должны стать следующие компоненты:

- федеративная проверка идентичности;
- аутентификация услуг, предлагаемых третьей стороной;
- обеспечение сквозных (end-to-end) процедур управления идентификацией.

Целостность и конфиденциальность данных позволяют сохранить решения категории IBS, при этом допускается возможность доступа к ним со стороны множества пользователей и приложений. Данный класс технологий базируется на технологиях сильной аутентификации (strong authentication):

- многофакторная аутентификация;
- однократные пароли;
- аутентификация на основе рисков (risk-based authentication), учитывающая предшествующую историю, текущий контекст и другие факторы риска, сопровождающие тот или иной запрос к данным.

Аутентификация должна делиться на уровни, предусмотренные в соглашении об уровне обслуживания, а процедуры авторизации (наделение правами), должны стать более гранулированными (granular authorization) – полномочия должны даваться только в ограниченных пределах, задаваемых выполняемыми ролями и функциями.

Необходимо развитие технологий: управление доступом на основе ролей (Role Based Access Control, RBAC), управление правами на информацию (Information Rights Management, IRM), избирательное управление доступом (Discretionary Access Control, DAC).

При переходе к облачным вычислениям компании скорее повышают свой уровень безопасности, а не понижают; провайдеры, предоставляющие ИТ-услуги, уделяют много внимания вопросам защиты данных и вкладывают большие денежные суммы в разработку эффективной и надежной системы защиты.

Часто на вопросах безопасности полностью базируется маркетинговая политика провайдера, для которого потеря репутации надежного партнера чревата полным крахом и уходом с рынка.

При выборе провайдера необходимо четко понимать, каким именно требованиям в области безопасности должна соответствовать предоставляемая им платформа.

Использованные источники:

1. http://www.osp.ru/os/2010/01/13000673
2. http://www.aladdin-rd.ru/company/pressroom/articles/34002/?print=Y
3. http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf
4. http://blog.i-oblako.ru/20120201archive.html
5. http://www.risspa.ru/csa
6. http://www.securitycode.ru/_upload/editor_files/pressa/IZ_44-3.pdf