УДК 004.986

С.Н. СКОРИК
Херсонский национальный технический университет

ФОРМАЛЬНАЯ МОДЕЛЬ СИТУАЦИИ УГРОЗЫ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СИСТЕМ

В статье рассмотрены вопросы информационной безопасности облачных систем. Предложены средства защиты виртуальных систем. Использование данных средств защиты позволяет избежать большинство угроз безопасности и одновременно повысить стабильность работы системы. Предложена формализация описания ситуаций при возникновении угроз безопасности. В результате получено исчисление, которое учитывает возможность возникновения множественных угроз.

Ключевые слова: Облачные вычисления, виртуальная система, безопасность, угроза, антивирусная защита.

С.М. СКОРИК
Херсонський національний технічний університет

ФОРМАЛЬНА МОДЕЛЬ СИТУАЦІЇ ЗАГРОЗИ БЕЗПЕКИ ХМАРНИХ СИСТЕМ

У статті розглянуті питання інформаційної безпеки хмарних систем. Запропоновано засоби захисту віртуальних систем. Використання даних засобів захисту дозволяє уникнути більшість загроз безпеки і одночасно підвищити стабільність роботи системи. Запропонована формалізація опису ситуацій при виникненні загроз безпеки. В результаті отримано обчислення, яке враховує можливість виникнення множинних загроз.

Ключові слова: Хмарні обчислення, віртуальна система, безпека, загроза, антивірусний захист.

S. SKORIK
Kherson National Technical University

FORMAL MODEL OF SITUATION SECURITY RISKS OF CLOUD SYSTEMS

The article discusses the information security of cloud systems. Proposed remedies virtual systems. Using data protection avoids most security threats while improving system stability. A formalization of describing a situation when threats arise is discussed. The result is a calculus that takes into account the possibility of multiple threats.

Keywords: Cloud computing, virtual system, security, threat, virus protection.

Постановка проблемы

Центр обработки данных (ЦОД) представляет собой совокупность серверов, размещенных на одной площадке с целью повышения эффективности и защищенности. Защита центров обработки данных представляет собой сетевую и физическую защиту, а также отказоустойчивость и надежное электропитание. В настоящее время на рынке представлен широкий спектр решений для защиты серверов и ЦОД от различных угроз. Их объединяет ориентированность на узкий спектр решаемых задач. Однако спектр этих задач подвергся некоторому расширению вследствие постепенного вытеснения классических аппаратных систем виртуальными платформами. К известным типам угроз (сетевые атаки, уязвимости в приложениях операционных систем, вредоносное программное обеспечение) добавились сложности, связанные с контролем среды (гипервизора), трафика между гостевыми машинами и разграничением прав доступа. Расширились внутренние вопросы и политики защиты ЦОД, требования внешних регуляторов. Работа современных ЦОД в ряде отраслей требует закрытия технических вопросов, а также вопросов связанных с их безопасностью. Финансовые институты (банки, процессинговые центры) подчинены ряду стандартов, выполнение которых заложено на уровне технических решений. Проникновение платформ виртуализации достигло того уровня, когда практически все компании, использующие эти системы, весьма серьезно занялись вопросами усиления безопасности в них.

В современных условиях становится все сложнее обеспечить защиту критически важных для бизнеса систем и приложений. Появление виртуализации стало актуальной причиной масштабной миграции большинства систем на виртуальные машины (ВМ), однако решение задач обеспечения безопасности, связанных с эксплуатацией приложений в новой среде, требует особого подхода. Многие типы угроз достаточно изучены и для них разработаны средства защиты, однако их еще нужно адаптировать для использования в облаке.

Анализ последних исследований и публикаций

Согласно результатам большинства опросов, именно безопасность является основной причиной, по которой руководители ИТ-компаний не решаются начать движение в сторону облачных решений. Один из

опросов на портале LinkedIn показал, что у 54% из более чем 7000 респондентов проблема безопасности вызывает наибольшую озабоченность, когда речь заходит о миграции в облако.

Как и в любом ИТ-сервисе, в облаке имеются уязвимости с точки зрения безопасности, которые пытаются обнаружить злоумышленники. Однако по мере роста осведомленности ИТ-специалистов об этих уязвимостях и о методах их устранения облачная среда становится все более безопасным местом. В действительности у тех, кто отважился совершить миграцию в облако, уровень безопасности повысился, о чем свидетельствуют голоса 57 % участников опроса, проведенного компанией Mimecast. Причина, по которой большинство участников этого исследования уверены в безопасности облачных вычислений, заключается в том, что люди понимают суть имеющихся угроз и научились минимизировать их.

В данной статье кратко охарактеризованы некоторые из наиболее распространенных рисков с точки зрения безопасности, связанных с облачными вычислениями, а также приведены шаги, которые можно предпринять для уменьшения этих рисков.

Средства защиты в виртуальных системах

Первым шагом для реализации облачной безопасности является идентификация уровней окружения, нуждающихся в защите [1]. После того как определены границы безопасности, стоит обратить внимание на методы, направленные на выполнение мониторинга, анализ подозрительной активности и защиту от вредоносных программ. В этом помогают различные инструменты или конфигурационные опции. Стоит отметить, что одним из важнейших аспектов работы любой среды, не только облачной, является развитый план по поддержанию безопасности инфраструктуры. Очень часто его частью является регулярное обновление программного обеспечения и внесение исправлений, мониторинг компонентов безопасности, а также проведение тестов на определение уязвимостей. Эти нехитрые процедуры могут предотвратить многие проблемы.

Не стоит забывать и о том, что при переходе в облако клиент передает свои ресурсы на сторону хостинг-провайдера, тем самым попадая в зависимость от производительности и пропускной способности каналов связи. В идеале взаимодействие с облаком должно быть эффективным, а время отклика – минимальным. Применение различных механизмов шифрования и использование веб-интерфейса для доступа к приложениям порождают сложность классификации сетевого трафика [2,3].

Сегодня облачные сервисы все чаще становятся мишенью различных атак, включая DDoS. Согласно некоторым отчетам, масштаб крупнейших DDoS-атак за последнее десятилетие увеличился примерно в 50 раз. Компания Arbor Networks в одном из своих исследований, в котором приняло участие порядка 130 специалистов, показала, что 76% опрошенных столкнулись с DDoS-атаками, целью которых били клиенты, а 43% опрошенных зафиксировали частичную или полную потерю работоспособности облачных сервисов. Атаки зачастую направлены на ограничение пропускной способности, чтобы сделать передачу «полезного» трафика максимально ограниченной либо вовсе невозможной.

Для информационной безопасности (ИБ) серверов, расположенных на территории ЦОД, необходимо, использовать физическую и программную безопасность. Под физической безопасностью имеется в виду ограничение доступа обслуживающего персонала в помещения, где установлено оборудование с опечатыванием корпусов средств вычислительной техники, так и меры удаленного контроля – видеозапись. Программная безопасность — это весь комплекс средств защиты от несанкционированного доступа: обновляемая ОС, обновляемый антивирус, межсетевой экран, криптографию, контроль периферийных устройств и т.д. Работы по администрированию в общем случае не должны требовать наличие административных привилегий.

Все средства защиты от угроз в виртуальных (облачных) системах можно разделить на ряд типовых классов: антивирусная защита, системы обнаружения вторжений и межсетевого экранирования, системы контроля доступа [4 - 6]:

– Антивирусная защита. Традиционные средства защиты, например, использование агентских антивирусов, одновременный запуск которых может вызвать так называемый «антивирусный шторм», не всегда применимы в условиях виртуализации. Производители находят решение этой проблемы разными способами. Стоит выделить три основных подхода: новаторский, консервативный и гибридный. Новаторский подход состоит в том, что виртуальная среда предоставляет специальный программный интерфейс для контроля виртуальных машин через гипервизор, а антивирусное средство пользуется им, выводя всю защиту на специализированную ВМ. Это позволяет отказаться от использования антивирусных агентов на виртуальных машинах, но в силу выбранной архитектуры имеет ограничения по возможностям анализа работы оперативной памяти. Классический подход заключается в недоверии к новому интерфейсу и работе по старой схеме с использованием антивирусных агентов, которые нужно обновлять и настраивать. Но вместе с тем вендоры в своих решениях стараются предоставить новые возможности для оптимизации исполнения агентов в виртуальной среде. Гибридный подход состоит в том, чтобы не отказываться от агентов полностью, делать их максимально легковесными и простыми для исполнения, но в то же время большую часть аналитики реализовывать на «соседней» ВМ, выделенной для задач антивирусной защиты. Этот подход более универсален, но, как и всё универсальное, в частных задачах может уступать первым двум вариантам. В целом же его эффективность по сравнению с неадаптированными для виртуальной среды решениями вполне ощутима.

– Системы обнаружения вторжений и межсетевого экранирования. С появлением виртуальных сред появилась новая проблема – неконтролируемое сетевое взаимодействие между ВМ. Трафик между ВМ обычно не покидает виртуальной среды, как следствие, отследить его традиционными средствами защиты не представляется возможным. Стоит отметить, что каждая компания имеет свой взгляд на решение этой задачи. Некоторые всё так же полагаются на программный интерфейс гипервизора, другие реализуют ВМ, встраиваемую между виртуальными коммутаторами, третьи заменяют сами коммутаторы, встраивая свою программную реализацию с возможностями по защите информации. Особенно интересны средства защиты с реализацией vNetwork Distributed Switch. В целом для контроля сетевых взаимодействий в виртуальной среде лучше не полагаться целиком на программные решения, установленные в ней же, так как платформа Intel x86 имеет физические ограничения, устраняемые в аппаратных решениях специальными ASIC-процессорами. Решением будет контроль внешних подключений к среде виртуализации с помощью аппаратных решений, а внутренних – программными решениями, реализуя таким образом комбинированный подход.

– Системы управления состоянием защиты виртуальной среды. Виртуальная среда представляет собой динамическую и сложную инфраструктуру, контроль которой с точки зрения ИБ – непростая задача. Этот класс решений предназначен для управления конфигурацией виртуальной среды и мониторинга состояния информационной безопасности, что зачастую не реализуется обычными средствами управления, такими как VMware vCenter. К лидирующим продуктам здесь можно отнести Reflex VMC и Catbird vSecurity. Оба решения имеют центр правления и виртуальные устройства, размещаемые на серверах ESX/ESXi. Можно констатировать, что это комплексные многокомпонентные продукты, отличающиеся быстрым развертыванием за счет использования virtual appliance и требующие кропотливой работы по их настройке, так как они регламентируют работу среды в целом. Решения в том числе полезны для автоматизации операций по настройке компонентов среды и контроля этого процесса с точки зрения ИБ. На текущий момент не каждая компания готова к применению подобных решений, но интерес к ним, несомненно, повысится с общим развитием отрасли.

– Системы контроля доступа к виртуальной инфраструктуре. Один из лидеров этого рынка – решение HyTrust от одноименной компании. Как и многие средства защиты для виртуальных сред, оно представляет собой виртуальное устройство. Решение позволяет повысить безопасность виртуальной инфраструктуры за счет перехвата всех соединений пользователей с ней и разграничения доступа по ролям с применением меток безопасности. Продукт выгодно отличается стабильностью работы и невлиянием на работоспособность самой виртуальной инфраструктуры. HyTrust удобен для администраторов, так как при выполнении всех функций контроля доступа и журналирования действий, не зависимых от управляемой ими среды, они продолжают работать с теми же VMware vSphere Client и консолями SSH. Благодаря встроенным ролям и правилам доступа в решении реализована самозащита от выключения.

– Классические системы защиты. И, конечно, не стоит забывать о классических средствах защиты, таких как контроль защищенности, мониторинг и управление событиями, система обнаружения вторжений и межсетевое экранирование на входе в среду виртуализации, защита систем хранения данных и организация доступа к интерфейсам управления аппаратными ресурсами серверов (iLO/ILOM/DRAC и другие). Большинство средств защиты для виртуальных сред интегрируется в единую систему управления и имеет коннекторы для подключения к SIEM, что позволяет интегрировать их с общей системой обеспечения ИБ, действующей в физической среде.

Безопасность данных на примере технологии облачного хранилища данных Dropbox

Dropbox – это сервис, который позволяет хранить пользователям свои данные в облачном хранилище. Данный сервис обязан быть максимально защищенным от всех видов угроз, поскольку пользователи могут хранить в облаке конфиденциальную информацию и рассчитывают на полную безопасность. Для защиты от проникновения разработчик использует шифрование данных, загружаемых в облако, функцию двухэтапной авторизации, также используется защита от сетевых атак. Работу в области безопасности подтверждают сертификаты по информационной безопасности, которые компания получает за подход к вопросам безопасности, конфиденциальности, целостности и доступности данных.

Однако несмотря на все примененные меры безопасности, в 2011 году в результате программного сбоя любой пользователь мог получить доступ к чужим данным с помощью произвольного пароля. Несмотря на заверения компании, что все данные зашифрованы, на самом деле сотрудникам компании всего лишь запрещается просто так просматривать пользовательские данные, а по соответствующему запросу из правоохранительных органов Dropbox готов предоставить любые файлы любого пользователя. Поэтому более надежный способ обезопасить данные - это лично зашифровывать файлы перед отправкой их в облачное хранилище.

Формализация описания ситуаций при возникновении угрозы безопасности

В соответствии со сценарно-прецедентным подходом в основу системы управления безопасностью облачных геолокационных систем могут быть положены следующие понятия: позиция, время, действие, сценарий, план, прецедент, проблемная ситуация [7].

Позиция описывает местонахождение объекта (субъекта) в заданной двух(трех)-мерной системе координат, и представляется в форме пары (тройки) вида $p=(\xi,\chi)$, где ξ, χ – координаты по

соответствующим осям.

Время задается отсчетами t относительно начального значения t_0 на заданной временной шкале T, упорядоченной по $<_T$.

Пусть заданы множество угроз Ψ, множество субъектов обеспечения безопасности (СОБ) $Z = \{A, B, D, F\}$ и множество допустимых действий СОБ U. Каждый из СОБ $z \in Z$ в момент времени t выполняет некоторое действие $a_{z(t)} \in U$.

Триадой назовем кортеж вида $\langle p, t, a_{z(t)} \rangle$.

Триада является элементарным фрагментом планов и сценариев противодействия угрозам, триадой также может быть задана цель сценария (цель может состоять в достижении позиции p к моменту t, тогда $a_{z(t)}$ может быть нулевым).

Активность СОБ $z \in Z$ представлена его выполняемым сценарием Σ_z.

Сценарий Σ_z СОБ z представляет собой кортеж вида

$$\Sigma_z = \langle t_s, t_r, [..., \langle t_i, p_i, a_i \rangle, ...], g \rangle, \tag{1}$$

где $[..., \langle t_i, p_i, a_i \rangle, ...]$ – упорядоченная последовательность триад, такая что $t_i <_T t_{i+1}$;

t_s – момент запуска выполнения сценария;

t_r – планируемый момент запуска;

$g = \langle t_e, p_e, a_e \rangle$ – конечная цель выполнения сценария,

t_e – конечный момент времени;

p_e – конечная позиция;

a_e – действие, выполняемое по достижению конечной позиции $\langle t_e, p_e \rangle$.

Соответственно, для каждого СОБ $z \in Z$ в любой момент времени $t \in T$ можно получить его местоположение $p_{z(t)}$, выполняемый им сценарий Σ_z и, зная t_s, конкретное выполняемое действие $a_{z(t)}$.

Представленный способ формализации позволяет корректировать назначенную любому из СОБ $z \in Z$ цель g_z и/или выполняемый сценарий Σ_z «на лету», без перезапуска цикла функционирования информационной системы обнаружения и предотвращения вторжения (ИСОПВ).

Угроза $\psi \in \Psi$ может быть представлена классом K_ψ и множеством нарушителей L, для каждого из которых $l \in L$ в любой момент времени $t \in T$ известно его местоположение $p_{l(t)}$

$$\psi_t = \langle K_\psi, \{(l, p_{l(t)}), ...\} \rangle \ \forall l \in L. \tag{2}$$

Позиционный контекст угрозы ψ_p описывается перечислением множества текущих позиций нарушителей $\psi_p = \{(l, p_l), ...\} \ \forall l \in L$.

Каждой тактической операции Ω, выполняемой в ответ на угрозу $\psi \in \Psi$, соответствует множество участвующих в ней СОБ $Z_\Omega \subseteq Z$ и *план* мероприятий Π_Ω, представляющий собой кортеж вида

$$\Pi_\Omega = \langle \psi, Z_\Omega, \{..., (z(k), \Sigma_{z(k)}), ...\} \rangle, \tag{3}$$

где $\{..., (z(k), \Sigma_{z(k)}), ...\}$ – множество выполняемых сценариев $\Sigma_{z(k)}$ для каждого СОБ $z(k) \in Z_\Omega$.

Позиционный контекст ситуации s_p содержит занимаемые СОБ $z \in Z$ позиции:

$$s_p = \{..., (z_i, p_{z_i}), ...\} \ \forall z_i \in Z. \tag{4}$$

Операционный контекст ситуации s_Ω содержит множество выполняемых операций $\{\Omega_j\}$, планов выполняемых операций $\{\Pi_{\Omega(j)}\}$, множество участвующих СОБ $z(k_j) \in Z_{\Omega(j)}$ и соответствующих сценариев

$\Sigma_{k(j)}$ для каждого из них [7]:

$$s_\Omega = \left\langle \{\Omega_j\}, \{\Pi_{\Omega(j)}\}, \{Z_{\Omega(j)}\}, \{\Sigma_{k(j)}\} \right\rangle \ \forall z(k_j) \in Z_{\Omega(j)}. \quad (5)$$

Ограничением является то, что каждый из СОБ $z_k \in Z$ в любой момент времени t может выполнять один и только один сценарий Σ_{kj}, соответствующий плану Π_{Ω_j} операции $\Omega_j \in \Omega$, такой что $z(k_j) \in Z_{\Omega(j)}$. В случае, если в момент времени t СОБ $z(m) \in Z$ не участвует ни в одной из операций $\Omega_j \in \Omega$, т.е. $\forall j \ z(m_j) \notin Z_{\Omega(j)}$, считаем, что $z(m)$ выполняет заданный штатный сценарий $\Sigma_{z(m0)}$.

Тогда текущая *ситуация* s_t описывается конфигурацией угроз, текущими позиционным и операционным контекстами:

$$s_t = \left\langle s_{p(t)}, s_{\Omega(t)}, \{\psi_{m(t)}\} \right\rangle \ \forall \psi_m \in \Psi. \quad (6)$$

Представленный формализм описания ситуаций учитывает возможность возникновения множественных угроз, т.к. конфигурация угроз и операционный контекст описывают множества угроз и, соответственно, выполняемых операций противодействия.

В момент возникновения угрозы для облачных систем складывается *проблемная ситуация*, требующая своего разрешения путем выполнения операций предупреждения или противодействия.

Управление безопасностью облачной системы в проблемной ситуации возлагается на сценарно-прецедентную интеллектуальную систему.

Основные результаты и выводы

В статье проведен анализ опросов, проведенных различными компаниями. Согласно этим опросам, безопасность является главной причиной, по которой специалисты откладывают переход на облачные технологии. Приведена структура облачных систем.

Описаны средства защиты в виртуальных системах. Таким образом, используя перечисленные в статье средства защиты, можно обезопасить систему от ряда угроз. В соответствии со сценарно-прецедентным подходом предложена формализация описания ситуаций при возникновении угроз безопасности, которая может быть использована для анализа, противодействия и предотвращения проблемных ситуаций в информационной системе обнаружения и предотвращения вторжений.

Список использованной литературы

1. Янюшкин В.В. Программные компоненты и архитектурные решения распределенных информационных систем на основе применения технологий cloud computing и WCF / В.В. Янюшкин // Перспективы развития средств и комплексов связи. Подготовка специалистов связи: мат. межвуз. научн.-техн. конф. – Новочеркасск: НВВКУС, 2009. – С.239-241.
2. Гультяев А.К. Виртуальные машины: несколько компьютеров в одном / А.К. Гультяев. – СПб.: Питер, 2006. – 224 с.
3. Коваленко О.С. Обзор проблем и состояний облачных вычислений и сервисов / О.С. Коваленко, В.М. Курейчик // Известия ЮФУ. Технические науки. – 2012. – №7. – С.146-153.
4. Бережной А. Sun VirtualBox как персональная система виртуализации. // ≪Системный администратор≫, №12, 2009 г.-С. 61-65.
5. Фингар П. DOT.CLOUD Облачные вычисления – бизнес платформа XXI века; пер. с англ. Захаров А.В. – М.: Аквамариновая Книга, 2011. – 256 с.
6. Ермаков Д. Г. Экспериментальная среда облачных вычислений в институте математики и механики УрО РАН / Д. Г. Ермаков, Д. А. Усталов // Программные продукты и системы: науч.- практ. изд. - 2012. - N 4. - С. 110-115.
7. Медведев А. А. Облачные технологии: тенденции развития, примеры исполнения / А. Медведев // Современные технологии автоматизации. - 2013. - N 2. - С. 6-9.