УДК 004.056

М. В. Гладкий
Белорусский государственный технологический университет

БЕЗОПАСНОСТЬ ПРИЛОЖЕНИЙ НА ПЛАТФОРМАХ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Предмет исследования данной статьи – методы защиты информации в облачной инфраструктуре (на базе платформ Amazon Web Services и Microsoft Azure), а также методы обеспечения безопасности операционной системы хоста и клиента, в частности изоляция экземпляров виртуальных машин и приложений, разграничение прав доступа, аутентификация и авторизация пользователей, шифрование данных.

Рассмотрены наиболее известные типы угроз (сетевые атаки, уязвимости в приложениях операционных систем, вредоносное программное обеспечение, контроль среды гипервизора, мониторинг трафика между гостевыми машинами). Разработана классификация основных видов атак в зависимости от типа уязвимости (инъекции кода, межсайтовый скриптинг, перехват вебсессий, «человек посередине») и уровня воздействия (отказ в обслуживании, переполнения буфера гипервизора, повышение прав пользователя виртуальной машины), а также проанализированы решения по их устранению.

Выявлено, что появление новых типов угроз и атак, направленных на платформу виртуализации, требует внедрения ряда специализированных механизмов, которые условно подразделяются на два класса: средства защиты в виде готовых аппаратных решений или в виде виртуальных устройств и средства защиты виртуальных машин и контроля коммуникаций в виртуальной среде (на уровне гипервизора).

Ключевые слова: облачные вычисления, безопасность, сетевая атака, защита информации, виртуализация.

M. V. Gladkiy
Belarusian State Technological University

APPLICATION SECURITY ON THE CLOUD COMPUTING PLATFORMS

The information security methods in the cloud (on Amazon Web Services and Microsoft Azure platforms) and ensuring security methods of the host and client operating system (insulation copies of virtual machines and applications, permissions, authentication and authorization, data encryption) are the subjects of research in this article.

The most well-known types of threats (network attacks, vulnerabilities in applications, operating systems, malicious software, the control of the hypervisor environment, monitoring traffic between the guest machines) are analyzed. The classification of the main types of attacks, depending on the type of vulnerability (code injection, cross-site scripting, intercept web session, “a man in the middle”) and exposure (denial of service, buffer overflow in hypervisor, elevation user virtual machine). The solutions to estimate them and analyzed.

It is revealed that the emergence of new types of threats and attacks on the virtualization platform requires the implementation of a number of specialized mechanisms. These mechanisms are conventionally divided into two classes. The first class is hardware solutions or virtual devices. The second class is the means of protection of virtual machines and communications control in the virtual environment (at a hypervisor level).

Key words: cloud computing, security, network attack, protection of information, virtualization.

Введение. Облачные вычисления получили широкое распространение в различных областях науки и техники. С их помощью можно решить такие задачи, которые раньше казались либо очень трудными, либо неосуществимыми. Но одним из препятствий на пути использования облаков становятся вопросы безопасности. Опасения относительно сохранности конфиденциальных данных до сих пор остаются основным ограничением внедрения облачных технологий.

Кроме того, на данном этапе распространения облачных вычислений отсутствует полная классификация способов обнаружения угроз по сравнению с традиционной инфраструктурой. В научных работах и статьях авторы пытаются применять классические подходы, методы и технологии, не учитывая при этом особенностей виртуальной среды. Поэтому данная область требует детального изучения: необходимо рассмотреть различные виды угроз, которым могут подвергаться данные в облачной

инфраструктуре, а также уделить особое внимание средствам защиты информации, разработанным в ответ на существующие угрозы.

Основная часть. В настоящее время на рынке представлены различные способы защиты приложений в облачной инфраструктуре. Они ориентированы на узкий спектр решаемых задач. К известным типам угроз добавились сложности, связанные с контролем среды (гипервизора), трафика между гостевыми машинами и разграничением прав доступа.

Основой обеспечения безопасности является строгий контроль физического доступа к серверам и сетевой инфраструктуре. В отличие от физической безопасности, сетевая безопасность представляет собой построение надежной модели угроз, включающей в себя защиту от вторжений и применения межсетевых экранов с целью разграничения внутренней сети центра обработки данных (ЦОД) на подсети с разным уровнем доверия [1].

Следует обратить особое внимание на механизмы регулирования подключений к облаку. Это может быть контроль доступа с определенных IP-адресов или обязательное подключение через VPN (virtual private network). Доступ также может регулироваться с помощью специализированных устройств – шлюзов безопасности, которые играют роль посредников между клиентами и облачными платформами [2].

Далее в статье приводится классификация существующих угроз облачных вычислений с учетом особенностей виртуальной среды.

Динамичность виртуальных машин. Виртуальные машины могут быть перемещены между физическими серверами. Такая изменчивость влияет на целостность всей системы безопасности. Однако уязвимости операционной системы или приложений в виртуальной среде распространяются бесконтрольно и часто проявляются после произвольного промежутка времени. Поэтому очень важно надежно зафиксировать состояние защиты системы независимо от ее местоположения.

Разграничение сети и защита периметра. При использовании облачных вычислений периметр сети размывается или исчезает. Это приводит к тому, что защита более уязвимой части облака определяет общий уровень защищенности. Для разграничения сегментов с разными уровнями доверия виртуальные машины должны сами обеспечивать себя защитой, перемещая сетевой периметр к самой виртуальной машине.

Уязвимости внутри гипервизора. Серверы облачных вычислений и локальные серверы используют одни и те же операционные системы и приложения. Для программного обеспечения (ПО) на облачных платформах очень высока угроза удаленного взлома или заражения. Вызвать переполнение буфера и инициировать запуск произвольного кода могут определенные ошибки в гипервизоре. Ошибки могут содержаться как на стороне управления виртуальной инфраструктурой, когда их эксплуатация проводится снаружи, так и со стороны виртуальных машин [1].

Защищенность данных и приложений. В традиционной инфраструктуре защита данных строится на основе физической защиты доступа к программно-аппаратным ресурсам. В облачной среде такой подход теряет смысл, так как методы защиты должны представлять собой единое целое. Доступ может получить только тот, кто обладает нужными правами в нужное время и в нужном месте. Предприятия должны обладать возможностью проверить, что ресурсам не нанесен вред и системы не скомпрометированы, особенно в ситуации, когда они размещаются в разделяемой физической среде.

Доступ системных администраторов к серверам и приложениям. Одна из основных характеристик облачных платформ – самообслуживание. Каждый пользователь может получить доступ через Интернет к управлению вычислительной мощностью. В традиционных ЦОД доступ инженеров к серверам контролируется на физическом уровне, в облачных средах они работают через Интернет. Критически важными становятся строгий контроль доступа для администраторов, а также обеспечение контроля и прозрачности изменений на системном уровне.

Защита бездействующих виртуальных машин. При выключении виртуальной машины существует возможность ее компрометации и заражения. Для этого достаточно получить доступ к хранилищу образов через сеть. Более того, на выключенной виртуальной машине отсутствует возможность запустить защитное программное обеспечение. В настоящее время уже созданы программные комплексы (например, Deep Security), где реализована защита не только внутри каждой виртуальной машины (ВМ), но и на уровне гипервизора [1].

Влияние традиционной безопасности на производительность. Большинство существующих решений безопасности создавалось для внутренней инфраструктуры и проектировалось без учета работы в виртуальной среде. В облачной системе, где виртуальные машины разделяют общие программно-аппаратные ресурсы, единовременный запуск приведет к катастрофическому снижению производительности.

В настоящее время облачные услуги по защите информации предлагает большое число

компаний, но лишь некоторые из них обеспечивают достаточно эффективную защиту, позволяющую в полном объеме обезопасить приложения от всех возможных типов атак [3].

В результате исследования проблем безопасности приложений на платформах облачных вычислений была разработана классификация основных типов атак с учетом особенностей виртуальной среды.

Традиционные атаки на ПО. К данному классу атак относят уязвимости операционных систем, модульных компонентов, сетевых протоколов. Для защиты от таких угроз достаточно установить межсетевой экран, антивирус, систему предотвращения вторжений (Intrusion Prevention System – IPS). При этом важно, чтобы данные средства защиты могли эффективно работать в виртуальных средах.

Функциональные атаки на элементы облака. Этот тип атак связан с многослойностью облака. Для защиты от данного класса атак необходимо использовать следующие средства защиты: для прокси – эффективную защиту от DoS-атак (отказ в обслуживании), для вебсервера – контроль целостности страниц, для сервера приложений – экран уровня приложений, для СУБД (система управления базами данных) – защиту от SQL-инъекций, для системы хранения данных – резервное копирование.

Атаки на клиента. Концепция облачных технологий позволяет получить пользователю доступ к ресурсам через браузер. Здесь стоит обратить внимание на такие типы атак, как межсайтовый скриптинг, расщепление запросов клиента, модификация данных кэша сервера-посредника, «угон» паролей, перехват вебсессий, «человек посередине» и многие другие. На текущий момент наиболее эффективной защитой от данного вида атак является правильная аутентификация и использование шифрованного соединения с взаимной аутентификацией.

Атаки на гипервизор. Гипервизор является одним из ключевых элементов виртуальной системы. Основная его функция – разделение ресурсов между виртуальными машинами. Атака на гипервизор может привести к тому, что одна виртуальная машина сможет получить доступ к ресурсам другой. В качестве стандартных методов защиты необходимо применять специализированные продукты для виртуальных сред, интеграцию хост-серверов со службой каталога Active Directory [3].

Атака на виртуальные машины при их переносе с одного узла на другой. Виртуальная машина представляет собой файл, который может быть запущен в разных узлах облачной инфраструктуры. В системах управления виртуальными машинами предусмотрены механизмы переноса машин с одного узла на другой. Однако существует вероятность кражи файла виртуальной машины по сети с последующей попыткой его запуска за пределами облака.

Атаки на системы управления. Большое количество виртуальных машин, используемых в облачной инфраструктуре, требуют наличия систем управления, способных надежно контролировать создание, перенос и удаление виртуальных машин. Вмешательство в систему управления может привести к появлению новых невидимых виртуальных машин, способных блокировать одни виртуальные машины и подставлять другие.

Следует отметить, что появление новых угроз и методов атак, направленных непосредственно на платформу виртуализации, требует внедрения ряда специализированных защитных механизмов, которые не могут быть обеспечены классическими средствами защиты. В настоящее время такие средства защиты можно разделить на два класса [3].

К первому относятся системы, поставляемые в виде готовых аппаратных решений или в виде виртуальных устройств. Преимущество такого подхода – быстрая скорость развертывания и ввода в эксплуатацию, использование существующих аппаратных мощностей заказчика, экономия ресурсов.

Второй класс образуют средства, предназначенные для защиты непосредственно виртуальных машин и контроля коммуникаций в виртуальной среде (на уровне гипервизора) [1].

Межсетевые экраны. Основной задачей данной подсистемы является контроль доступа программных модулей. ПО содержит типовые шаблоны, обеспечивающие следующие возможности: изоляцию виртуальной машины внутри определенного сегмента, фильтрацию трафика, анализ протоколов, внедрение политики безопасности, сканирование сетевого окружения.

Средства обнаружения и предотвращения вторжений. Данная подсистема обеспечивает экранирование уязвимостей операционной системы (ОС) и приложений до момента, когда будут установлены важные обновления. Такие системы внедряются в виде программного агента, что позволяет экранировать уязвимости, обнаруженные в ОС и приложениях: защита от любых атак на известные уязвимости без установки критических обновлений; блокировка атак типа XSS (Cross Site Scripting) и SQL-Injection.

Средства контроля целостности. Контроль целостности ОС и приложений позволяет выявить опасные изменения, которые являются следствием компрометации системы хакером или вредоносным кодом. Эта подсистема

выполняет проверку по запросу или расписанию, а также осуществляет контроль свойств файлов, включая их атрибуты.

Средства защиты от вредоносных программ, учитывающие виртуализацию. Данный тип защиты учитывает специальные программные интерфейсы, которые предоставляет гипервизор. Защита включает сканирование виртуальных машин в режиме реального времени, что обеспечивается антивирусным агентом внутри каждой ВМ.

Средства контроля политик безопасности. Главная задача данного типа защиты заключается в сборе и просмотре журналов работы ОС и приложений на предмет выявления событий безопасности. Правила анализа журналов позволяют выявить значимые события в огромном массиве записей: обнаружение подозрительного поведения, сбор действий администратора, сквозной сбор событий со всех частей ЦОД (физических, виртуальных и облачных серверов).

Самозащищенные данные. Данный тип защиты использует зашифрованные данные, в которые интегрирован механизм обеспечения безопасности. Такой механизм включает в себя набор правил, которым должна удовлетворять среда, где находятся самозащищенные данные. При попытке доступа к этим данным механизм проверяет среду на безопасность и раскрывает их, только если среда является безопасной [1].

Доверенный монитор. Данное программное обеспечение устанавливается на сервер провайдера облачных вычислений. Оно позволяет наблюдать за действиями провайдера и передавать результаты пользователю, который может убедиться в том, что компания действует в соответствии с принятым регламентом.

Основным преимуществом этих средств является специализация на защите виртуальных сред и коммуникаций в них. Среди производителей таких систем можно отметить следующие компании: Trend Micro, StoneSoft, Symantec, Reflex Systems, CheckPoint, StoneSoft, «Код Безопасности» [3].

Заключение. В данной статье рассмотрены основные типы угроз, классифицированы основные виды атак в зависимости от типа уязвимости и уровня воздействия, а также проанализированы решения по их устранению. Все рассмотренные методы защиты имеют свои достоинства и недостатки. Зашифровав только одну часть облака, не предоставляется возможность защитить конфиденциальную информацию. Соответственно, для защиты данных на платформах облачных вычислений нужен комплексный подход, совмещающий использование шифрования с другими средствами защиты, включающими в себя программную реализацию межсетевого экрана, обнаружения и предотвращения вторжений, контроля целостности, защиты от вредоносного кода и анализа журналов.

Литература

1. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. М.: ДМК Пресс, 2012. С. 254−259.

2. Степаненко В. Облачная обработка данных – миф или реальность? М.: Сети и бизнес, 2010. С. 14−15.

3. Риз Д. Облачные вычисления. СПб.: БХВ-Петербург, 2011. С. 99−105.

References

1. Shan’gin V. F. *Zashchita informatsii v komp’yuternykh sistemakh i setyakn* [Protection of information in computer systems and networks]. Moscow, DMK Press Publ., 2012, pp. 254−259.

2. Stepanenko V. *Oblachnaya obrabotka dannykh – mif ili real’nost’?* [Is cloud computing myth or reality?] Moscow, Seti i biznes Publ., 2010, pp. 14−15.

3. Riz D. *Oblachnyye vychisleniya* [Cloud application architectures]. St. Petersburg, BHV-Peterburg Publ., 2011, pp. 99−105.

Информация об авторе

Гладкий Максим Валерьевич – ассистент кафедры информационных систем и технологий. Белорусский государственный технологический университет (220006, г. Минск, ул. Свердлова, 13а, Республика Беларусь). E-mail: MaksHladki@gmail.com

Information about the author

Gladkiy Maksim Valer’yevich − assistant, the Department of Information Systems and Technologies. Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: MaksHladki@gmail.com

Поступила 14.03.2015