ОСНОВНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ВИРТУАЛЬНЫХ СРЕДАХ И ОБЛАЧНЫХ ПЛАТФОРМАХ

***Зубарев Игорь Витальевич**, кандидат технических наук, доцент*
Радин Павел Константинович

Рассмотрены основные угрозы безопасности информации в виртуальных средах и облачных платформах. Рассмотрены проблемные вопросы защиты гипервизора, сервера управления, виртуальной машины и приложений, безопасности сетевого взаимодействия. Предложены меры по организации защиты информации в виртуальных средах и облачных платформах.

***Ключевые слова**: облачные вычисления, виртуализация, средства защиты информации*

THE BASIC INFORMATION SECURITY THREATS IN THE VIRTUAL ENVIRONMENTS AND CLOUD PLATFORMS

***Igor Zubarev**, Ph.D., Associate Professor*
Pavel Radin

The main threats to the security of information in virtual environments and cloud platforms are shown. Problem questions of protection of the hypervisor management server, virtual machine and application, security, networking is proposed. The arrangements for the protection of information in virtual environments and cloud platforms are considered.

***Keywords**: cloud computing, virtualization, information security tools*

Введение

В настоящее время одним из перспективных направлений совершенствования информационно-вычислительных ресурсов является внедрение технологии облачных вычислений [1, 2].

Под облачными вычислениями (cloud computing) понимают модель обеспечения глобального и комфортного сетевого доступа по требованию к совместно используемому пулу конфигурируемых вычислительных ресурсов (например, серверам, сетям передачи данных, системам хранения данных, программным приложениям и сервисам – как совместно, так и локально), которые могут быть оперативно выделены и освобождены с минимальными эксплуатационными затратами[1].

Для обеспечения согласованной работы узлов вычислительной сети, реализованной на облачной платформе, используется специализированное промежуточное программное обеспечение, обеспечивающее мониторинг состояния оборудования и программ, балансировку нагрузки, обеспечение ресурсов для решения задачи.

Одним из основных решений для сглаживания неравномерности нагрузки на вычислительные ресурсы является размещения слоя серверной виртуализации между слоем программных услуг и аппаратным обеспечением. В условиях виртуализации балансировка нагрузки может осуществляться посредством программного распределения виртуальных серверов по реальным серверам, перенос виртуальных серверов происходит посредством живой миграции.

Следует признать, что технология виртуализации имеет множество преимуществ, например: удобство управления виртуальной средой; высокая скорость разворачивания новых серверов; оперативность создания резервных копий, тестирования обновлений и нового функционала на

1 NIST SP 800-145. Definition of Cloud Computing.

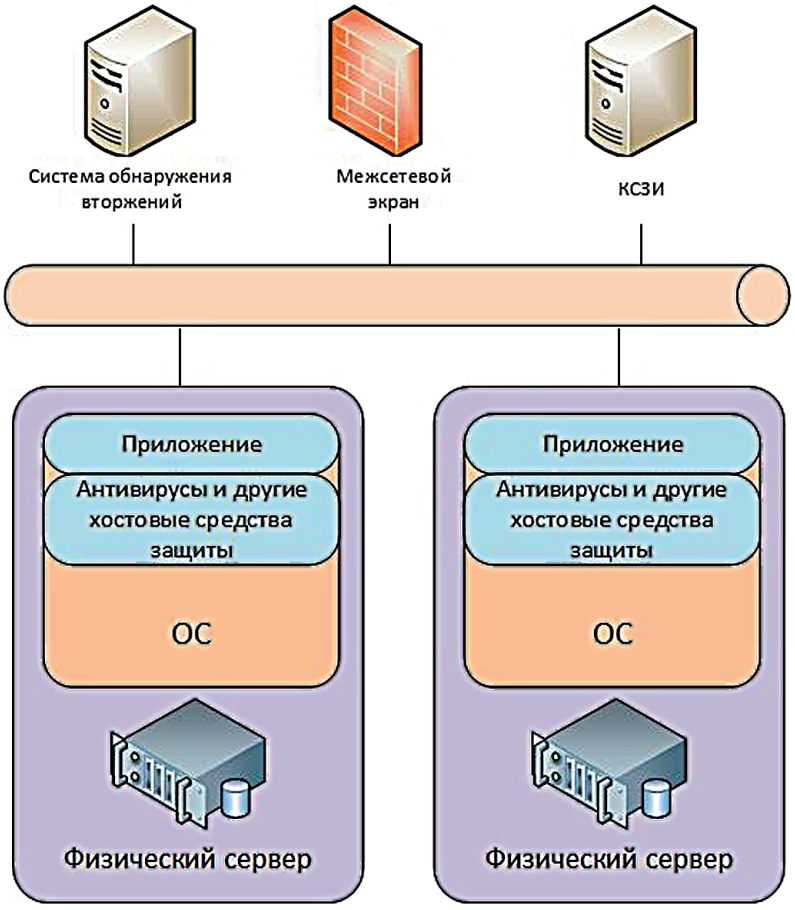

***Рис. 1**. Элементы физической вычислительной среды*

актуальных копиях продуктивных систем и др. [3].

Однако обеспечение безопасности виртуализации необходимо рассматривать как отдельное направление в рамках общей безопасности ИТ-инфрастуктуры, для которого неприменимы традиционные для физической среды средства и методы защиты [4-11].

В физической среде (рис. 1) нет ограничений на применение средств защиты на хосте: сетевой трафик может быть отфильтрован стандартным сетевым оборудованием, а злонамеренный код – обнаружен системами предотвращения вторжений и контентной фильтрации.

В виртуальной же среде (рис. 2) применение традиционных средств защиты информации иногда невозможно или нецелеобразно. Например, одновременная антивирусная проверка жестких дисков нескольких виртуальных машин создаст значительную нагрузку на оборудование. Сетевой трафик между виртуальными машинами не покидает физического сервера, и, следовательно, традиционные сетевые средства защиты информации его не видят. Кроме того, имеется дополнительный программный слой, который также необходимо защищать.

Проблемные вопросы безопасности виртуализации

Рассмотрим «узкие» места безопасности виртуализации: гипервизор, сервер управления, виртуальные машины, приложений и др.[2]

1. Гипервизор – это программа или аппаратная схема, обеспечивающая или позволяющая одновременное параллельное выполнение нескольких операционных систем на одном и том же хост-компьютере. Он обеспечивает изоляцию ОС друг от друга, защиту и безопасность, разделение ресурсов между различными запущенными ОС и управление ресурсами. В этом смысле гипервизор обозначает целый класс ПО, которое отвечает за процесс исполнения ВМ, и отделяет эту категорию продуктов от других компонентов системы виртуализационного ПО (в частности, от средств управления теми же гипервизорами и виртуальными средами)

Компрометация гипервизора может привести к компрометации всех его виртуальных машин. Автономный гипервизор (работающий непосредствен-

2 См. http://habrahabr.ru/company/securitycode/blog/200346/

но на оборудовании) наиболее распространенных платформ виртуализации представляет собой «урезанную» версию одной из ОС общего пользования (Windows, Linux, BSD и т.д.), и, несмотря на то что здесь отключен лишний функционал и разработчики обычно заявляют о повышенной безопасности данной версии, говорить о полном отсутствии в них невыявленных уязвимостей нельзя. Помимо кода самого гипервизора, на этом уровне может быть запущен и код сторонних разработчиков: дополнения, драйверы устройств и приложения.

Рассмотрим основные классы уязвимостей гипервизоров на примере VMware vSphere.

A. Переполнение буфера и вызов произвольного кода

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, с правами администратора или без них, или со стороны виртуальных машин. Во втором случае возможен выход за пределы виртуальной машины и выполнение любых команд на гипервизоре.

Примеры известных уязвимостей:

CVE-2012-1516…1517, CVE-2012-2448…2450 – VMX-процесс уязвим из-за ошибки в обработке команд, при эксплуатации уязвимости, возможно переполнение памяти и выполнение произвольного кода на хостовой операционной системе из гостевых операционных систем.

CVE-2013-3657 – Удаленный пользователь может отправить специально сформированный пакет и вызвать переполнение буфера с запуском произвольного кода или отказом в обслуживании.

CVE-2013-1405 – Удаленный пользователь может отправить специально сформированный пакет авторизации в vSphere Server 4.0-4.1, который вызовет переполнение буфера и запуск произвольного кода.

CVE-2012-2448 – Удаленный пользователь может отправить специально сформированный NFS-пакет в vSphere Server 4.0-4.1 и вызвать переполнение буфера с запуском произвольного кода или отказом в обслуживании.

B. Повышение прав пользователя внутри виртуальной машины

Целый класс уязвимостей гипервизора позволяет нарушить работу гостевой операционной системы виртуальной машины и повысить права пользователя в ней. В виртуальной среде такие атаки реализуются обычно через два основных направления – эксплуатация уязвимостей в VMware Tools (набор утилит и драйверов для гостевой операционной системы) или через прямой доступ к памяти виртуальной машины через гипервизор в обход механизмов доступа гостевой операционной системы.

Примеры известных уязвимостей:

CVE-2012-1666 – уязвимость VMware Tools позволяет повысить права доступа пользователю гостевой операционной системы внутри неё с помощью заражения вредоносным кодом файла tpfc.dll.

CVE-2012-1518 – уязвимость, позволяющая повысить права доступа пользователю гостевой операционной системы внутри неё с помощью переполнения буфера в VMware Tools, если права доступа для директории с VMware Tools настроены неправильно.

C. Отказ в обслуживании

Это наименее опасный в плане компрометации информации класс уязвимостей, однако, подобные уязвимости влияют на другой показатель – доступность. И их реализация негативно сказывается на качестве услуг облачного провайдера, репутацию сервиса и, в конечном итоге, на прибыли. Речь идет об ошибках гипервизора, используя которые злоумышленник может привести к отказу в обслуживании, не затрачивая при этом больших усилий. Отказ в обслуживании путем генерации большого объема мусорного трафика не рассматривается как специфичная для гипервизора угроза. Речь идет об уязвимостях, при которых один или несколько простых сетевых пакетов или команд приводят к остановке в работе гипервизора целиком или отдельных его служб. Как и в случае с переполнением памяти эти ошибки могут содержаться и во внешних интерфейсах, и во внутренних функциях виртуальных машин.

Примеры подобных уязвимостей:

CVE-2013-5970 – сервис hostd-vmdb может быть выведен из строя путем отправки специально подготовленного сетевого пакета.

CVE-2012-5703 – API для работы внешних служб (vSphere API) содержат ошибку, которая может вызвать падение и отказ в обслуживании службы, принимающей запросы API.

Для организации защиты на этом уровне требуется:

- разработать и формализовать процессы доступа к гипервизору и изменения конфигурации;
- максимально ограничить доступ к гипервизору по сети;
- использовать возможность запуска гипервизора с флэш-памяти или с неизменяемого раздела жесткого диска;

• следить за своевременной установкой всех обновлений. Однако у такой защиты есть два недостатка. Во-первых, существует большое множество уязвимостей, известных только узкому кругу злоумышленников, но пока неизвестных производителю и, соответственно, неучтённых им. Во-вторых, при использовании сертифицированного гипервизора его обновления запрещены, так как нарушают целостность бинарных файлов;

• регулярно проводить тесты сканерами уязвимостей;

• тщательно отслеживать перемещение образов жестких дисков, подключение внешних накопителей и передачу больших объемов данных;

• тщательно проверять сторонний код и особо контролировать физический доступ к оборудованию.

2. Консоль/сервер управления. Большое количество виртуальных машин, используемых в облаках требует наличие систем управления, способных надежно контролировать создание, перенос и утилизацию виртуальных машин. Вмешательство в систему управления может привести к появлению виртуальных машин — невидимок, способных блокировать одни виртуальные машины и подставлять другие. Консоль или сервер управления (в зависимости от платформы виртуализации) – такой же программный код с доступом к его функциям по сети, следовательно, он может содержать уязвимости, которые способны привести к компрометации всех виртуальных машин. Для организации защиты на этом уровне требуется:

• управлять изменениями конфигурации (существующие средства защиты платформ виртуализации позволяют отслеживать изменения настроек и проводить их проверку на соответствие различным стандартам и/или принятым в компании политикам безопасности);

• ограничить доступ по сети (доступ только из определенных сегментов сети или размещение сервера управления в отдельном сегменте);

• обеспечить регулярное обновление;

• сканировать уязвимости;

• организовать журналирование и мониторинг.

3. Виртуальная машина и приложения. Стандартные средства защиты не всегда применимы для виртуальных серверов, однако развитие платформ виртуализации показывает, что этот недостаток становится еще одним преимуществом. Например, платформа VMware имеет набор интерфейсов VMsafe для взаимодействия со средствами защиты сторонних разработчиков. Для организации защиты на этом уровне требуется следующее:

• антивирусная защита. Для антивирусов, агенты которых устанавливаются на виртуальные серверы, необходимо предусмотреть расписание запуска полной проверки, чтобы избежать повышенной нагрузки на оборудование. Если платформа виртуализации предоставляет такую возможность, то наиболее эффективным средством является безагентный антивирус, который интегрируется с гипервизором и через API осуществляет проверку процессов в памяти виртуальной машины и ее дисков даже в том случае, если машина выключена. Кроме того, он позволяет избежать конкуренции за ресурсы оборудования;

• разделение виртуальных машин по зонам доверия. Возможна и допустима ситуация, когда на одном физическом сервере находятся, например, внешний сервер и компоненты ПО, реализующие функциональные задачи должностных лиц ОВУ, но при этом необходимо соблюдение как минимум тех же принципов, что и при разворачивании физических серверов. Комплексные средства защиты платформ виртуализации таких производителей, как Trend Micro, Reflex Systems, позволяют изолировать машины из разных зон доверия, а также создать профили и политики безопасности, автоматизирующие применение таких настроек. Более того, при перемещении машины на другой сервер такой профиль может предотвратить ошибочное подключение внутренней системы к внешней сети;

• своевременное выполнение обновлений ПО, периодические сканирования уязвимостей и мониторинг событий информационной безопасности;

• обновление средств защиты. Благодаря простоте включения, выключения и клонирования виртуальных серверов появление в сети машины с устаревшими антивирусными базами и обновлениями происходит гораздо чаще, чем для физических серверов. При использовании средств защиты, которые интегрируются с гипервизором, вероятность компрометации виртуальной машины минимальна.

4. Сетевое взаимодействие. Очень часто не учитывают тот факт, что сетевой трафик между виртуальными машинами, находящимися на одном сервере, не покидает этого сервера, и предполагают, что систем фильтрации и предотвращения вторжений до платформы виртуализации достаточно, чтобы защитить все виртуальные серверы. Предположим, что диверсионная группа получила доступ к одному из виртуальных серверов и это осталось незамеченным средствами защиты, стоящими на периметре платформы виртуализации, например они использовал одну из техноло-

гий туннелирования или раздобыли легитимный доступ к одному из серверов. Результатом могут стать атаки на соседние виртуальные серверы, и такие атаки могут быть не обнаружены. Организация защиты на этом уровне складывается из нескольких составляющих.

- Защита сетевой среды платформы виртуализации не слабее, чем устанавливается для физической среды. Наиболее эффективным средством являются виртуальные модули (Virtual Appliance) систем предотвращения вторжений и межсетевого экранирования. Такие модули могут быть частью комплексного средства обеспечения безопасности платформы виртуализации или поставляться отдельно производителями сетевых средств защиты (Juniper, Check Point и др.).
- Изоляция виртуальных машин, относящихся к разным зонам доверия.
- Сетевая защита периметра платформы виртуализации. Эта мера, хотя и является недостаточной для обеспечения безопасности, но остается необходимой. Нужно учитывать объемы трафика на этом участке сети – выбранное средство защиты должно обеспечивать соответствующую пропускную способность.

5. Административные привилегии. Достаточно часто внедрение платформы виртуализации на стадиях планирования и разработки архитектуры начинаются без привлечения специалистов по информационной безопасности. В результате нередко встречаются ситуации, когда подразделения службы защиты государственной тайны не могут обеспечить защиту развернутых систем. Еще один риск – нарушение принципа разделения полномочий; например, клонирование, копирование и другие манипуляции с виртуальными машинами, содержащими продуктивные данные, проводящиеся без согласований и даже уведомления данных служб. Значит, велика вероятность утечки информации, содержащей сведения, составляющие государственную тайну. Для организации защиты на этом уровне требуется к проектам по внедрению системы виртуализации привлекать специалистов по информационной безопасности, а требования по защите виртуальной инфраструктуры обязательно включать в техническое задание на разрабатываемые образцы.

Также необходимо реализовать разделение полномочий при доступе к административным функциям. Здесь первоочередная задача – понимание и формализация того, кто и за управление какими рисками несет ответственность; например, управление сетевой инфраструктурой платформы виртуализации должно осуществляться подразделением, отвечающим за физические сети. Это справедливо и применительно к средствам защиты, установки обновлений, проведению аудита настроек на соответствие стандартам и политикам безопасности и т. д. Комплексные средства защиты виртуальных сред позволяют реализовать ролевое управление административными функциями и тем самым минимизировать вероятность предоставления избыточных привилегий.

6. Аудит и отчетность.

В общем случае аудит настроек и анализ логфайлов платформы виртуализации становятся еще одной задачей администраторов платформы виртуализации, и здесь главная рекомендация – соблюдать те же принципы разделения полномочий, что и для физической среды. Диверсант с административным доступом к серверу управления при недостаточном контроле настроек и журнальных файлов практически не ограничен в действиях. Для организации защиты на этом уровне требуется осуществлять анализ настроек платформы виртуализации на соответствие принятым политикам безопасности. Кроме того, необходимо проводить мониторинг событий информационной безопасности и корреляцию событий для выявления потенциально опасных действий и, безусловно, учитывать, что проблемы с производительностью платформы виртуализации затронут все работающие на ней системы, поэтому анализ загруженности виртуальных машин и всей платформы в целом необходим для обеспечения ее непрерывной работы – это позволит своевременно обнаружить и устранить «узкие» места оборудования и ПО, создающее чрезмерную нагрузку [12].

Заключение

Таким образом, исходя из количества приложений и компонентов, которые должны быть защищены, к управлению защитой платформы виртуализации нужно подходить комплексно – неполная защита на одном из уровней может сделать бессмысленным использование всех остальных средств. Платформы виртуализации очень уязвимы с точки зрения безопасности и, помимо стандартных потенциально опасных мест, имеют и свои. «Точечное внедрение» средств защиты не принесет положительных результатов – количество компонентов, защиту которых нужно обеспечить, слишком велико, а риски при компрометации всей платформы слишком значительны.

Литература

1. Зубарев И.В., Жидков И.В., Кадушкин И.В. Кибербезопасность автоматизированных систем управления военного назначения // Вопросы кибербезопасности. 2013. № 1(1). С.10-16.
2. Матвеев В.А., Цирлов В.Л. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации в 2014 г. // Вопросы кибербезопасности. 2013. № 1(1). С.61-64.
3. Krutz R.L., Vines R.D. Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Wiley, 2010. 384 p.
4. Беккер М.Я., Гатчин Ю.А., Кармановский Н.С., Терентьев А.О., Федоров Д.Ю. Информационная безопасность при облачных вычислениях: проблемы и перспективы // Научно-технический вестник информационных технологий, механики и оптики. 2011. № 1 (71). С. 97-102.
5. Богданов В.В., Новоселова Ю.С. Актуальность обеспечения информационной безопасности в системах облачных вычислений, анализ источников угроз // Доклады Томского государственного университета систем управления и радиоэлектроники. 2012. № 1-2. С. 78-82.
6. Гюнтер Е.С., Нарутта Н.Н., Шахов В.Г. «Облачные» вычисления и проблемы их безопасности // Омский научный вестник. 2013. № 2-120. С. 278-282.
7. Демурчев Н.Г., Ищенко С.О. Проблемы обеспечения информационной безопасности при переходе на облачные вычисления // Информационное противодействие угрозам терроризма. 2009. № 13. С. 147-151.
8. Иванов А.П., Андреев В.М., Тикин М.С. Информационная безопасность облачных вычислений // Информация и безопасность. 2012. Т. 15. № 3. С. 435-436.
9. Каретников А.В., Зегжда Д.П. Безопасность облачных вычислений. проблемы и перспективы // Проблемы информационной безопасности. Компьютерные системы. 2011. № 4. С. 7-15.
10. Марков А.С., Цирлов В.Л. Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. 2014. № 1(2). С. 28-35.
11. Сергеев Ю.К. Анализ угроз безопасности виртуальных информационных систем // Вестник Российского государственного гуманитарного университета. 2011. № 13. С. 160-170.
12. Уязвимости гипервизора – угроза виртуальной инфраструктуре и облаку. Блок «Код Безопасности». URL: http://habrahabr.ru/company/securitycode/blog/200346/ (Дата обращения: 9.05.2014).

References

1. Zubarev I.V., Zhidkov I.V., Kadushkin I.V. Kiberbezopasnost avtomatizirovannykh sistem upravleniya voyennogo naznacheniya, Voprosy kiberbezopasnosti, 2013, No 1(1), pp.10-16.
2. Matveyev V.A., Tsirlov V.L. Sostoyaniye i perspektivy razvitiya industrii informatsionnoy bezopasnosti Rossiyskoy Federatsii v 2014 g, Voprosy kiberbezopasnosti, 2013, No 1(1), pp.61-64.
3. Krutz R.L., Vines R.D. Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Wiley, 2010, 384 p.
4. Bekker M.Ya., Gatchin Yu.A., Karmanovskiy N.S., Terentyev A.O., Fedorov D.Yu. Informatsionnaya bezopasnost pri oblachnykh vychisleniyakh: problemy i perspektivy, Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki, 2011, No 1 (71), pp. 97-102.
5. Bogdanov V.V., Novoselova Yu.S. Aktualnost obespecheniya informatsionnoy bezopasnosti v sistemakh oblachnykh vychisleniy, analiz istochnikov ugroz, Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki, 2012, No 1-2, pp. 78-82.
6. Gyunter Ye.S., Narutta N.N., Shakhov V.G. «Oblachnyye» vychisleniya i problemy ikh bezopasnosti, Omskiy nauchnyy vestnik, 2013, No 2-120, pp. 278-282.
7. Demurchev N.G., Ishchenko S.O. Problemy obespecheniya informatsionnoy bezopasnosti pri perekhode na oblachnyye vychisleniya, Informatsionnoye protivodeystviye ugrozam terrorizma, 2009, No 13, pp. 147-151.
8. Ivanov A.P., Andreyev V.M., Tikin M.S. Informatsionnaya bezopasnost oblachnykh vychisleniy, Informatsiya i bezopasnost, 2012, Vol. 15, No 3, pp. 435-436.
9. Karetnikov A.V., Zegzhda D.P. Bezopasnost oblachnykh vychisleniy. problemy i perspektivy, Problemy informatsionnoy bezopasnosti. Kompyuternyye sistemy, 2011, No 4, pp. 7-15.
10. Markov A.S., Tsirlov V.L. Rukovodyashchiye ukazaniya po kiberbezopasnosti v kontekste ISO 27032, Voprosy kiberbezopasnosti, 2014, No 1(2), pp. 28-35.
11. Sergeyev Yu.K. Analiz ugroz bezopasnosti virtualnykh informatsionnykh sistem, Vestnik Rossiyskogo gosudarstvennogo gumanitarnogo universiteta, 2011, No 13, pp. 160-170.
12. Uyazvimosti gipervizora – ugroza virtualnoy infrastrukture i oblaku. Blok «Kod Bezopasnosti». URL: http://habrahabr.ru/company/securitycode/blog/200346/