УДК 004.4

к.т.н., доц. Козюра В.Д., Юрх Н.Г. (ГУИКТ)

БЕЗОПАСНОСТЬ ВИРТУАЛЬНОЙ СРЕДЫ

Виртуализация принесла в мир настольных компьютеров и серверных систем множество новых и перспективных возможностей, которые были восприняты большинством пользователей. Технологии виртуализации представляют собой концепцию, существенно изменяющую подход к ИТ-инфраструктуре и позволяющую увеличить ее эффективность и гибкость за счет одновременного запуска нескольких виртуальных систем на одной физической системе. На данный момент виртуализация применяется на самых различных уровнях абстракции программных и аппаратных систем, начиная от виртуализации приложений и заканчивая виртуализацией систем хранения данных (СХД).

Принимая решение о виртуализации, необходимо учитывать некоторые особенности этой технологии. В частности, процесс виртуализации сопряжен с определенными проблемами безопасности. Прежде чем внедрять виртуализацию, требуется провести анализ основных уязвимых мест системы, на которой будет реализовываться виртуальная среда.

Компании, внедряющие технологии виртуализации серверов и настольных систем, столкнулись при этом с рядом проблем. В то время как технически в виртуализации нет ничего сложного, и в перспективе затраты на ее внедрение полностью окупают себя в течение небольшого времени (один-два года), есть некоторые моменты, которые являются спорными при решении вопроса: «внедрять виртуализацию или нет?». В частности к этим проблемам можно отнести:

- сложность оценки эффективности и возвращения инвестиций;
- надежность виртуальных систем;
- безопасность виртуальных систем.

Помимо этих моментов, существуют еще ряд причин, заставляющих многие компании и домашних пользователей с осторожностью использовать платформы виртуализации, такие как лицензионные ограничения, совместимость ПО и оборудования и прочие. На данный же момент, безопасность виртуальных машин является ключевой проблемой в их использовании и находится в центре внимания ИТ-сообщества

Внутренние и внешние угрозы в виртуальной инфраструктуре. Технологии виртуализации доказали свою эффективность на множестве примерах, но для того чтобы знать как следует защищать виртуальные системы необходимо рассмотреть все варианты угроз которые могут быть применимы к виртуальной среде.

Принимая решение о виртуализации, необходимо учитывать некоторые особенности этой технологии. В частности, процесс виртуализации сопряжен с определенными проблемами безопасности. Прежде чем решительно внедрять виртуализацию, требуется провести анализ основных уязвимых мест. Кроме того, необходимы практические решения, применимые почти к любым компаниям.

Простая переносимость виртуальных систем на другие физические платформы и популярность использования виртуальных машин по модели SaaS (Software as a Service) приводят к тому, что критически важные системы со всеми конфиденциальными данными могут быть украдены путем копирования виртуальной машины на обычную флэш-карту за несколько минут. Далее эта виртуальная машина может использоваться злоумышленником на любом компьютере.

Помимо этого, виртуальная машина может использоваться для незаконного распространения информации, упакованной в готовую к использованию «коробку». Достаточно лишь запустить виртуальную машину и получить доступ к нелегальной информации или сервису. Так например виртуальная машина VMware под названием Melinda Gates с нелегальным KMS (Key Management Server) для Windows Vista, позволяла

производить незаконную активацию некоторых изданий Vista. После этого компании Microsoft пришлось запретить виртуализацию изданий Vista Home и Home Premium по причине возможности нелегального распространения мультимедиа-контента в виртуальной машине.

Опасность бесконтрольного развертывания виртуальных систем заключается еще и в том, что нередки случаи нарушения лицензионного соглашения на операционные системы или программное обеспечение при создании их копий в виртуальных машинах, что может явиться источником проблем для организации.

Существует опасность полной или частичной потери информации в случае сбоя аппаратной части машины, или в случае заражения машины вирусами.

Ниже будут приведены примеры новых видов угроз, которые несут собой технологии виртуализации. Нужно учитывать, что в цепочке объектов, нуждающихся в защите, появляется также платформа виртуализации, необходимо убедиться в ее соответствии современным стандартам безопасности, а также своевременно устанавливать на нее все необходимые обновления. Вендоры платформ крайне заинтересованы в повышении уровня безопасности своих продуктов и их сертификации, например, платформа VMware ESX Server на данный момент сертифицирована по уровню безопасности CCL2 (Common Criteria Level 2) и ведется работа по сертификации виртуальной инфраструктуры VI3 на соответствие уровню CCL4, а продукты компании XenSource уже соответствуют уровню CCL5.

В условиях большого количества серверов виртуализации, необходимы средства централизованного управления обновлениями для поддержания уровня безопасности во всей инфраструктуре организации. Поскольку несколько виртуальных серверов размещены на одном оборудовании, то нельзя, к примеру, разделить приватные и публичные данные между ними физически, в отличие от реальных компьютеров, между которыми можно, условно говоря, разорвать сетевой кабель. Кроме того, технологии виртуализации сами по себе являются средством для создания новых видов угроз, как, например, руткиты Blue Pill и SubVirt.

Blue Pill представляет собой средство получения контроля над компьютером (руткит), которое основывается на технологиях виртуализации и нацелено на операционную систему Windows Vista. На данный момент Blue Pill использует технологию виртуализации AMD-V (бывшая Pacifica), которая присутствует во всех последних процессорах компании AMD.

Механизм работы руткита выглядит следующим образом:

- вредоносный код проникает в целевую систему
- затем происходит незаметная виртуализация хостовой системы, которая превращается в гостевую на данном компьютере, а Blue Pill действует как гипервизор, при этом не требуется перезагрузка операционной системы
- все необходимые руткиту интерфейсы для взаимодействия с внешней средой «прячутся» за пределами этой системы, а ПО для обнаружения вторжений не может найти руткит, поскольку он расположен вне операционной системы

Способы защиты виртуальной инфраструктуры

При использовании парка виртуальных машин в пределах инфраструктуры организации необходима точно такая же их защита, как и физических серверов. Все традиционные меры и политики безопасности, применимые к ним, требуется использовать и в виртуальной инфраструктуре. Кроме того, поскольку сервер с платформой виртуализации является наилучшей точкой для получения доступа злоумышленников к целевым системам в виртуальных машинах, нужно уделить особенное внимание его защите и обновлениям.

К основным рекомендациям для поддержания виртуальной инфраструктуры в безопасном состоянии можно отнести следующие:

1. Контроль защиты данных не только внутри виртуальных машин, но и образов виртуальных систем.

2. Использование специализированных решений для защиты серверов виртуализации. К сожалению, на данный момент их не так много, но в ближайшем времени они, несомненно, появятся. В качестве примера можно привести проект sHype компании IBM.

3. Для критически важных машин в пределах серверов виртуализации использование системы обнаружения или предотвращения вторжений (Intrusion Detection/Prevention Systems, IDS/IPS). Работа этих систем зачастую завязана на физическое расположение компьютеров, что усложняет работу по защите виртуальной инфраструктуры ввиду легкой переносимости виртуальных машин на другое оборудование.

4. Для распространения конфиденциальной информации в виртуальных машинах использование специализированных защищенных платформ виртуализации. Они позволяют шифровать содержимое дисков виртуальных машин, защищая их паролем, и применять к ним различные политики безопасности.

5. Использование систем резервного копирования для восстановления данных.

6. Защита администратора и администраторских учетных записей на компьютере хоста. Исследования показали, что администраторская (корневая) учетная запись на машинах хоста значительно менее защищена по сравнению с учетными записями и паролями виртуальных машин или машин физической сети.

7. Обновление ОС и приложений на всех виртуальных машинах и на хосте. Приложения на хосте должны быть в минимально возможном количестве, устанавливать только то, что действительно необходимо.

8. Установление и обновление антивирусных программ на всех виртуальных машинах и на хосте, виртуальные машины могут быть заражены вирусами и червями так же, как и физические машины.

9. Не выходить в Интернет с компьютера хоста. Машины хоста управляют виртуальными машинами, и проблемы, возникающие на виртуальной машине хостов, могут привести к серьезному снижению производительности или вообще отказу служб.

10. Укреплять ОС хоста и отключать ненужные службы. Использование ОС по минимуму обеспечит минимальную потенциальную возможность для атак. Отключать неиспользуемые виртуальные машины.

11. Отключать технологию портов физических устройств на каждой виртуальной машине, если эта технология не используется; такие технологии, как USB, должны быть отключены на всех виртуальных машинах, если среда виртуальных машин не использует данную технологию.

12. Постоянно просматривать журналы регистрации событий и журналы безопасности на машинах хостов и виртуальных машинах. Мониторинг часто игнорируется в виртуальных средах, причина этого, вероятно, связана с мониторингом на основе хоста, который предлагает ПО виртуализации. Эти журналы должны храниться в вашем хранилище логов для более надежной защиты и в целях их просмотра в будущем.

Выводы

1. В последнее время безопасность является одним из ключевых факторов при принятии решения об использовании технологий виртуализации. В условиях необходимости защиты конфиденциальной информации виртуальные машины требуют повышенного внимания, хотя они и, напротив, могут использоваться для обеспечения безопасности (например, для изоляции критически важных систем друг от друга). Вредоносное ПО, использующее виртуализацию, может в ближайшем будущем являться угрозой не только для организаций, но и для конечных пользователей. Поэтому при использовании виртуализации необходимо грамотно спланировать стратегию защиты виртуальной инфраструктуры.

2. Простая развертываемость виртуальных систем требует постоянного контроля, поскольку «забытые» и не обновляемые системы могут являться точкой проникновения злоумышленников во внутреннюю сеть компании. К тому же, нельзя забывать об инсайдерских угрозах - необходимо правильно разграничивать права доступа персонала к информационным ресурсам, содержащих виртуальные системы. В больших масштабах нужно использовать специализированное ПО для контроля за ИТ-инфраструктурой и средства обнаружения вторжений.

3. Большое количество уязвимостей, найденных за последнее время в платформах виртуализации, говорит о том, что внимание хакеров к виртуальным системам в дальнейшем будет только расти. Поэтому, безусловно, необходимо тщательно следить за обновлениями платформ, точно так же, как и за обновлениями операционных систем.

Список литературы

1. *Гультяев А. К.* Виртуальные машины: несколько компьютеров в одном. — Питер, 2006.
2. *Стивен Браун.* Виртуальные частные сети.: Пер. с англ. - М.: Изд.дом «Лори», 2001.
3. *Крис Касперски.* Техника сетевых атак. Приемы противодействия.: Пер. с англ. - Том I. – Р. Изд.дом «СОЛОН», 2001.

У даній статті розглянуто питання забезпечення безпеки віртуального середовища, зроблено аналіз можливих загроз і запропоновано ряд рекомендацій для підтримки віртуальної інфраструктури в безпечному стані.

Ключові слова: віртуальне середовище, загрози, безпека.

В данной статье рассмотрен вопрос обеспечения безопасности виртуальной среды, сделан анализ возможных угроз и предложен ряд рекомендаций для поддержания виртуальной инфраструктуры в безопасном состоянии.

Ключевые слова: виртуальная среда, угрозы, безопасность.

In given article is considered the question of the virtual environment safety, is made the analysis of possible threats and is offered a number of recommendations for maintenance of a virtual infrastructure in a safe condition.

Key words: virtual environment, threats, safety.

Поступила 17.11.2009

УДК 004.621.391

к.т.н. Павлов І.М. (НТУУ «КПІ»)

ФОРМАЛЬНИЙ ОПИС ВПЛИВУ НЕБЕЗПЕЧНИХ ЗАГРОЗ НА СИСТЕМУ ЗАХИСТУ ІНФОРМАЦІЇ

Забезпечення захисту інформації на практиці проводиться в умовах випадкового або системного впливу будь-яких різних факторів (загроз), які, в цілому, систематизовані в стандартах. Причому стандарти, які прийняті в державі, та стандарти, якими керуються в світі – відрізняються як самим підходом до оцінки загроз так і системністю методології оцінки ефективності систем захисту інформації.

В статті [1] були розглянуті питання неформального підходу до методиці оцінки ефективності ескізного проектування комплексних систем захисту інформації. Були виділені в окремий етап та розглянуті основні підходи до аналізу як самої комп'ютерной системи, так і інформації, яка циркулює в цей системі, а також проаналізовані загрози по цілям застосування і визначені етапи подальшої оцінки ефективності комплексних систем захисту інформації під час ескізного проектування.