УДК 004.056.53

Проблемы реализации разграничения доступа к функциям управления виртуальных сред

Д. В. Угаров, Д. А. Постоев
Закрытое акционерное общество "ОКБ САПР", Москва, Россия

Рассмотрены проблемы, возникающие при реализации разграничения доступа к функциям управления виртуальных сред. Предложены требования к наложенному средству защиты информации, позволяющему избежать ограничений существующих решений.

Ключевые слова: виртуальная инфраструктура, виртуальная машина, разграничение доступа, сегментация виртуальных инфраструктур.

Реализация разграничения доступа к объектам инфраструктуры является неотъемлемой частью процесса построения защищенной информационной системы. Однако несмотря на то, что для этого уже разработано множество моделей безопасности, не зависящих от конкретной информационной системы, большинство реализаций на практике имеют изъяны.

Не обошла эта проблема и виртуальные инфраструктуры, где сталкиваются со следующим фактом. *Администратор виртуальной инфраструктуры (АВИ) имеет максимальный уровень доступа ко всем объектам (в числе которых могут находиться ВМ, обрабатывающие информацию, различную как по уровню секретности, так и по категориям доступа) и функциям управления информационной системы.*

Проблемы, возникающие при проектировании системы

1. Для виртуальных сред не предусмотрено разделения ролей АВИ, т. е. того, кто управляет объектами информационной системы, и администратора безопасности информации (АБИ), того, кто назначает права пользователям системы, в том числе и АВИ. Таким образом, возникает ситуация сосредоточения максимальных привилегий в рамках одной роли (пользователя), т. е. проблема "суперпользователя".

Угаров Дмитрий Владимирович, руководитель группы разработки СЗИ для систем виртуализации.
E-mail: dugarov@okbsapr.ru
Постоев Дмитрий Александрович, программист группы разработки СЗИ для систем виртуализации.
E-mail: postoev@okbsapr.ru

Статья поступила в редакцию 26 июня 2016 г.

Для большинства систем такое положение неприемлемо, АБИ должен иметь возможность ограничивать действия АВИ: запрещать критичные для безопасности действия и разрешать некоторые действия только по согласованию, например к удалению виртуальной машины (нарушение целостности и доступности) или экспорту ее на диск (нарушение конфиденциальности).

2. Система может содержать различную информацию (категорируемую иерархически, т. е. разного уровня секретности, или неиерархически, т. е. разного вида). Может возникнуть ситуация, при которой она будет "перемешана", например случайное или умышленное переключение секретной ВМ в подсеть к несекретным или миграция ВМ разработчика на хранилище бухгалтерии.

К сожалению, данная проблема не может быть решена средствами самой виртуальной инфраструктуры, так как существующие продукты не предполагают мандатного механизма разграничения доступа, а сетевого сегментирования (с помощью VLAN или средствами межсетевых экранов) недостаточно в случае, если необходимо обеспечить не только изоляцию сети, но и изоляцию среды обработки информации и средств ее хранения [1—3]. По этой причине архитектор сталкивается с проблемой сегментирования, т. е. разбиения системы на сегменты и обеспечения их изоляции.

Решение рассмотренных задач

Устранять проблему "суперпользователя" приходится организационными мерами, например заменять учетную запись АВИ на аналогичную с урезанными правами, а учетные данные "суперпользователя" запечатывать в конверте до возникновения нештатных ситуаций. Однако это не решает проблемы полностью, а только переносит ее на иной уровень. Более того, в больших инфраструктурах это и вовсе может быть неприменимо

из-за необходимости частого доступа к вырезанным у АВИ функциям и их постоянного согласования с АБИ.

В свою очередь, на решение проблемы сегментирования претендуют следующие способы:

1. Полное физическое разделение, когда под каждый сегмент (в нашем случае это ВМ бухгалтерии и разработчика, а также ВМ с секретными и несекретными данными) выделяют отдельные сервера, не имеющие связи между собой (чтобы АВИ при желании не мог выполнить неправильное действие).

Минус такого подхода заключается в значительно возрастающих расходах на оборудование. Помимо этого, разделение приведет к снижению эффективности использования физических ресурсов (инфраструктура более разрознена), что скажется на эффективности балансировки нагрузки и отказоустойчивости.

2. Для каждого сегмента создать отдельную учетную запись АВИ.

Недостаток такого способа заключается в значительном увеличении количества учетных записей (например, вместо 1 учетной записи АВИ в нашем случае получаем 4) и усложнении работы с системой (в частности, отслеживании состояния всей системы).

Выводы

Все рассмотренные решения приводят либо к дополнительным значительным затратам, ведущим к снижению эффективности использования средств виртуализации, либо к введению дополнительных организационных мер, усложняющих работу АВИ. По этой причине логичным шагом является перенимание опыта из смежных областей и создание наложенного средства защиты для ухода от описанных проблем.

При этом данное средство защиты должно реализовывать [4, 5]:

- разграничение доступа к функциям управления виртуальной инфраструктурой, критичным с точки зрения безопасности;
- возможность создания нескольких ролей (пользователей), между которыми будут разделены полномочия по управлению виртуальной инфраструктурой, а также осуществления контроля назначения прав доступа с помощью отдельной учетной записи АБИ, которая имеет права только на чтение в рамках виртуальной системы;
- мандатную политику безопасности и изоляцию доступа к разным сегментам информационной системы на основе иерархических и неиерархических меток.

Разработчикам СЗИ, в свою очередь, стоит обратить внимание на данную сферу, так как несмотря на популярность систем виртуализации, решения для большинства сред до сих пор отсутствуют.

Литература

1. Методический документ ФСТЭК России от 11.02.2014 "Меры защиты информации в государственных информационных системах".
2. Приказ № 17 ФСТЭК России от 11.02.2013 "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".
3. Приказ № 21 ФСТЭК России от 18.02.2013 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".
4. *Постоев Д. А.* Управление доступом в виртуальных системах на основе контроля информационных потоков // Безопасность информационных технологий. — М., 2014. № 4. С. 86—91.
5. *Постоев Д. А.* Особенности применения средств защиты информации в виртуальных системах // Вопросы защиты информации. 2014. Вып. 4 (107). С. 22—23.

Problems in the implementation of access control system in virtual environments

D. V. Ugarov, D. A. Postoev
Closed Joint Stock Company "OKB SAPR", Moscow, Russia

The article provides an overview of the problems in the implementation of access control system in virtual environments. Authors propose set of requirements for security solution, which avoids the limitations of existing approach.

Keywords: virtual infrastructure, virtual machine, access control, segmentation virtual infrastructures.

Bibliography — 5 references. *Received June 26, 2016*