RISSPA
be professional

Сообщество профессионалов в области информационной безопасности

Проблема выбора средств защиты информации для виртуализированных инфраструктур

Рабочая группа:
Мария Сидорова
Евгений Родыгин

Рецензенты:
Евгений Климов
Денис Безкоровайный
Максим Федотенко
Андрей Прозоров
Константин Феоктистов
Александр Кузьмин
Михаил Михеев

Санкт-Петербург
2013 год

Введение

Сегодня для большинства компаний, которые применяют технологии виртуализации, особую сложность представляет выбор средств защиты информации для виртуализированных инфраструктур. Несмотря на то, что рынок уже предлагает и средства защиты, адаптированные для работы в виртуальной среде, и специализированные инструменты, многим экспертам пока сложно разобраться, чем они отличаются друг от друга, и какими принципами следует руководствоваться при их выборе. С появлением в 2013 году приказов ФСТЭК России № 17 и № 21 вопросы защиты информации в виртуализированных инфраструктурах приобрели еще большую значимость. Большое количество вопросов, поступающих экспертам ассоциации RISSPA, подтолкнуло ассоциацию к подготовке этой брошюры. Эксперты RISSPA постарались подробно описать проблематику вопроса и подготовили информативные таблицы, которые могут помочь в выборе средств защиты и построении оптимальной системы защиты для виртуализированной инфраструктуры.

Коротко о выгодах виртуализации

Сегодня технологии виртуализации популярны как никогда. При таких очевидных преимуществах, как совокупное сокращение затрат на информационные технологии, простота развертывания новых серверов и рабочих станций, удобство резервного копирования и восстановления данных, виртуализация предоставляет и новые возможности в обеспечении защиты информации и всей корпоративной инфраструктуры компании. Что это за возможности, и в чем их специфика? Во-первых, некоторые виды атак, которые можно осуществить в физической среде, невозможно реализовать в условиях виртуализированной инфраструктуры. Так, известно, что виртуальные коммутаторы нечувствительны к некоторым атакам, присущим физическим коммутаторам, к примеру – атакам подмены адресов. Во-вторых, за счет особенностей архитектуры виртуализированной инфраструктуры проводить, к примеру, антивирусную проверку виртуальных машин можно даже тогда, когда они находятся в выключенном состоянии. В условиях традиционной инфраструктуры это невыполнимо. Эти и другие возможности расширяют защитные функции виртуализированной инфраструктуры, однако чтобы обеспечить безопасность информации и корпоративной инфраструктуры недостаточно просто разместить ресурсы компании в виртуальной среде.

Специфические угрозы и уязвимости среды виртуализации

Среда виртуализации – это особый программно-аппаратный слой в инфраструктуре компании, который отличается от традиционной физической архитектуры наличием абсолютно новых компонентов: гипервизора, средств управления и обслуживания виртуализированной инфраструктуры. Ключевым элементом архитектуры среды виртуализации является гипервизор. Он обеспечивает выполнение нескольких операционных систем, их изоляцию друг от друга и разделение ресурсов между ними. Получив контроль над гипервизором, злоумышленник приобретает практически неограниченные возможности: он незаметно для средств защиты, установленных в виртуальных машинах, может перехватывать данные. Фактически именно эти компоненты становятся основными объектами атак виртуализированной инфраструктуры, так как компрометация гипервизора может привести к компрометации всех виртуализированных серверов и рабочих станций, а захват средств управления виртуализированной инфраструктуры поставит под угрозу всю инфраструктуру компании. Следовательно, вместе с плотностью размещения виртуальных машин растут и риски. В связи с этим защита компонентов виртуализации является ключевой задачей в общей стратегии защиты информации в виртуализированной инфраструктуре. Помимо традиционного мониторинга и аудита компонентов виртуализации, необходимо применять методы и правила выявления инцидентов, специфичных для виртуализированной инфраструктуры.

Актуальными специфическими угрозами для компонентов виртуализации являются:

- Несанкционированный доступ к данным виртуальных машин путем использования уязвимостей гипервизора.
- Несанкционированный доступ к данным виртуальных машин с использованием средств управления виртуализированной инфраструктурой:
    - прямой доступ к файлам и данным виртуальных машин;

    - изменение конфигурации виртуальных машин;
    - модификация команд управления.
- Заражение и модификация гипервизора вредоносным программным обеспечением.
- Потеря производительности и отказ в обслуживании гипервизора за счет некорректного использования ресурсов.

Выбор средств защиты информации

На сегодняшний день реализовать защиту от специфических угроз для компонентов виртуализации только традиционными средствами защиты не представляется возможным. Надежную систему защиты виртуализированной инфраструктуры необходимо строить сразу в нескольких направлениях: одновременно применять защитные механизмы, встроенные в платформу виртуализации, специализированные средства защиты, а также те средства защиты, которые уже используются в инфраструктуре компании.

С чего начать и какими принципами руководствоваться при выборе специализированных средств защиты? Существует несколько основных правил:

- Во-первых, перед тем как приступить к выбору, необходимо определить цели и задачи защиты информации и виртуализированной инфраструктуры.
- Во-вторых, все средства защиты можно разделить на отдельные категории: средства защиты от несанкционированного доступа, антивирусные средства и средства защиты от вредоносных программ, межсетевые экраны и так далее. Поэтому сравнение функционала и выбор решения необходимо осуществлять в рамках одной категории, но отличной от устоявшейся на сегодняшний день группы «средства для защиты виртуализированной инфраструктуры».
- В-третьих, необходимо помнить, что большая часть из этих средств защиты не является специализированными средствами для виртуализированной инфраструктуры, а представляет собой лишь адаптированные средства защиты для работы в виртуальной среде. Такие решения работают внутри виртуальной машины, так же как и на физическом сервере, не зная о своем виртуальном окружении и не позволяя бороться со специфическими угрозами и уязвимостями виртуальной среды. Сложность возникает в том, чтобы отличить одно решение от другого.
- В-четвертых, необходимо рассматривать функционал продукта и проверять, как он реализуется на практике. Рекомендуется посетить специализированные интернет-ресурсы, где специалисты обмениваются опытом и обсуждают сильные и слабые стороны конкретного продукта.
- В-пятых, необходимо учитывать, для каких конкретно платформ виртуализации (и их версий) предназначено средство защиты. Например, продукты, предназначенные для защиты виртуализированных инфраструктур, построенных на платформах компании VMware, могут поддерживать как полный перечень всех выпускаемых компанией VMware платформ виртуализации, так и ограничиваться поддержкой только флагманской платформы VMware vSphere. При этом системы защиты для инфраструктур, построенных на разных платформах даже одного производителя, могут иметь существенные различия.
- В-шестых, при выборе сертифицированных продуктов необходимо обращать внимание на технические условия, по которым этот продукт прошел сертификацию. В них должны быть прописаны: среда тестирования, ограничения по эксплуатации и функционал, на который выдан сертификат.

Использование традиционных средств защиты информации

Можно ли обойтись без применения специализированных решений? В некоторых случаях можно использовать и традиционные средства защиты или компенсировать отсутствие специализированных решений дополнительными техническими и организационными мерами, которые могут повлечь за собой дополнительные риски, связанные с человеческим фактором, необходимостью увеличения количества требуемых ресурсов и проблемами совместимости.

Например, для защиты виртуальных машин могут применяться антивирусные средства, которые уже используются в компании. В этом случае необходимо более тщательно подойти к составлению расписания, по которому будут проверяться виртуальные машины. Таким образом можно избежать критической загрузки виртуальных серверов.

Еще один момент, на который стоит обратить внимание, – применение средств контроля несанкционированного доступа. Практически все проблемы в этой области возникают из-за невыполнения рекомендаций производителей платформ виртуализации. Документы, в которых четко описаны действия администратора по безопасности, имеются для множества платформ виртуализации. Часть из них выпущена самими производителями, часть – экспертными сообществами. Например, подобные руководства предостерегают от использования встроенных «по умолчанию» в платформу ролей. Перед началом работы необходимо составить матрицу доступа и уже по ней сформировать требуемые для работы с виртуализированной инфраструктурой роли.

Особую роль при построении системы обеспечения безопасности виртуализированных и гибридных инфраструктур (имеющих в своем составе как виртуализированные, так и физические сегменты инфраструктуры) играют сетевые средства защиты. Одним из объектов воздействия на виртуализированную инфраструктуру могут служить сетевые каналы взаимодействия виртуальных машин и внешние сетевые каналы управления виртуализированной инфраструктуры. При этом важно понимать, что такие средства защиты широко представлены на рынке, но мы рассматриваем только те средства защиты сети, которые специально предназначены для виртуализированных инфраструктур и заявлены самим разработчиком.

Требования регуляторов к средствам защиты информации

Структурировать средства защиты можно по самым разным критериям. Рассмотрим представленные на рынке средства защиты для виртуализированных инфраструктур в контексте новых законодательных требований ФСТЭК России. 18 февраля 2013 года ФСТЭК России выпустила приказ № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», в котором указаны меры по защите персональных данных в среде виртуализации. В перечне приведено 10 технических мер:

1. Идентификация и аутентификация субъектов доступа и объектов доступа в виртуализированной инфраструктуре, в том числе администраторов управления средствами виртуализации.
2. Управление доступом субъектов доступа к объектам доступа в виртуализированной инфраструктуре, в том числе внутри виртуальных машин.
3. Регистрация событий безопасности в виртуализированной инфраструктуре.
4. Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуализированной инфраструктуры, а также по периметру виртуализированной инфраструктуры.
5. Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией.
6. Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных.
7. Контроль целостности виртуализированной инфраструктуры и ее конфигураций.
8. Резервное копирование данных, резервирование технических средств, программного обеспечения виртуализированной инфраструктуры, а также каналов связи внутри виртуализированной инфраструктуры.
9. Реализация и управление антивирусной защитой в виртуализированной инфраструктуре.
10. Разбиение виртуализированной инфраструктуры на сегменты (сегментирование виртуализированной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей.

Аналогичные требования (различаются в части их реализации) присутствуют и в перечне Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденном приказом ФСТЭК России от 11 февраля 2013г. № 17.

Приведем функциональные возможности некоторых существующих на рынке средств защиты в контексте требований раздела «Защита среды виртуализации (ЗСВ)» приказа ФСТЭК России от 18 февраля 2013 г. № 21.

Таблица 1. Технические меры по обеспечению безопасности в соответствии с приказом ФСТЭК России от 18 февраля 2013 г. № 21 и продукты, помогающие их выполнить*

Наименование продукта	Технические меры по обеспечению безопасности в соответствии с приказом ФСТЭК России от 18.02.2013 № 21
Аккорд-В	1, 2, 3, 5, 6, 7, 10
vGate R2	1, 2, 3, 4, 5, 6, 7, 10
vGate-S R2	1, 2, 3, 4, 5, 6, 7, 10
ПАК «Соболь»	5
HyTrust Appliance	1, 2, 3, 4, 5, 6, 7, 10
Trend Micro Deep Security	3, 4, 7, 9, 10
Kaspersky Security for Virtualization	9
McAfee MOVE AntiVirus	9
Symantec Endpoint Protection	9
HP TippingPoint SVF	1, 2, 3, 4, 6, 7, 10
Check Point Security Gateway VE	3, 4, 9, 10
IBM Security Virtual Server Protection for VMware	2, 4, 10
Cisco Virtual Security Gateway	1, 2, 3, 4, 6, 7, 8, 10
Cisco ASA 1000V	1, 2, 3, 4, 6, 7, 8, 10
Cisco ASA 5585-X	1, 2, 3, 4, 6, 7, 8, 10
StoneGate Firewall	1, 2, 3, 4, 7, 8, 10
StoneGate Firewall/VPN	1, 2, 3, 4, 7, 8, 10
StoneGate IPS	1, 2, 3, 4, 7, 8, 10
StoneGate SSL	1, 2, 3, 4, 7, 8, 9, 10
StoneGate SSL VPN	1, 2, 3, 4, 7, 8, 9, 10
StoneGate Authentication server	1, 2, 3
Veeam Backup & Replication	8
Symantec Backup Exec	8
Symantec NetBackup	8
EMC Avamar	8
Acronis Backup & Recovery Virtual Edition	8
Acronis vmProtect	8

* Таблица составлена на основе информации, предоставленной разработчиками средств защиты, без учета уровней защищенности персональных данных, предусмотренных приказом ФСТЭК России от 18.02.2013 № 21.

Необходимость использования сертифицированных средств защиты информации по-прежнему остается одним из самых спорных вопросов.

В разделе 11 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 12 февраля 2013 г № 17, указано: «Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации».

Приведем информацию о сертифицированных продуктах.

Таблица 2. Наличие сертификатов соответствия на продукты*

Производитель	Наименование продукта	Сертификат соответствия (система, номер)	Соответствие требованиям	Срок действия сертификата
ОКБ САПР	Аккорд-В	ФСТЭК России № 2598	СВТ-5, НДВ-4	До 20.03.2015
Код Безопасности	vGate R2	ФСТЭК России № 2308	СВТ-5, НДВ-4	До 28.03.2014
	vGate-S R2	ФСТЭК России № 2383	ТУ, НДВ-2	До 12.07.2014
	ПАК «Соболь»	ФСТЭК России № 1967	ТУ, НДВ-2	До 07.12.2015
Trend Micro	Trend Micro Deep Security	ФСТЭК России № 2861	СОВ (ИТ.СОВ.У4.ПЗ) по 4-му классу, САВЗ (ИТ.САВЗ.Б4.ПЗ) по 4-му классу, МЭ-4, НДВ-4**	До 03.04.2016
Лаборатория Касперского	Kaspersky Security for Virtualization	ФСТЭК России № 2818	НДВ-2	До 04.02.2016
Check Point	Check Point Security Gateway VE	ФСТЭК России № 2811	ТУ, МЭ-3	До 15.01.2016
Symantec	Symantec Backup Exec	ФСТЭК России № 2798	ТУ, НДВ-4	До 04.06.2016
	Symantec NetBackup	ФСТЭК России № 2872	ТУ, НДВ-4	До 30.04.2016
	Symantec Endpoint Protection	ФСТЭК России № 2586	ТУ, НДВ-4	До 13.03.2015
Cisco	Cisco ASA 5585-X	***	***	***
Stonesoft	StoneGate Firewall	ФСТЭК России № 2157	ТУ, МЭ-2, НДВ-4	До 16.08.2013
	StoneGate IPS	ФСТЭК России № 2163	ТУ, МЭ-3, НДВ-4	До 31.08.2013
	StoneGate SSL	ФСТЭК России № 2284	ТУ, МЭ-3, НДВ-4	До 25.02.2014
	StoneGate SSL VPN	ФСБ № СФ/124-1803	СКЗИ КС1/КС2	До 27.03.2015

* Таблица составлена на основе информации, предоставленной разработчиками средств защиты.
** Приказом ФСТЭК России от 06 декабря 2011 г № 638 «Об утверждении Требований к системам обнаружения вторжений» (СОВ, справедливо и для средств антивирусной защиты (САВЗ)) введены дополнительные требования доверия к безопасности и классам СОВ, сопоставлены как оценочные уровни доверия (ОУД), так и уровни контроля недекларированных возможностей (НДВ). Указанный Профиль защиты содержит компоненты, конкретизированные для обеспечения преемственности требованиям по контролю отсутствия НДВ, изложенных в руководящем документе ФСТЭК (Гостехкомиссии) России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации: Классификация по уровню контроля отсутствия недекларированных возможностей», для 4-го уровня контроля.

*** В связи с особенностями системы сертификации ФСТЭК России продукт имеет следующие сертификаты соответствия: № 2608, РД МЭ 4-го класса, до 26.03.2015; № 2694, РД МЭ 4-го класса, до 22.08.2015; № 2703, РД МЭ 4-го класса, до 06.09.2015; № 2724, РД МЭ 3-го класса, до 28.09.2015; № 2743, РД МЭ 4-го класса, до 07.11.2015; № 2745, РД МЭ 3-го класса, до 09.11.2015; № 2816, РД МЭ 4-го класса, до 16.01.2016; № 2842, РД МЭ 4-го класса, до 12.03.2016; № 2844, РД МЭ 4-го класса, до 15.03.2016.

Послесловие авторов

Виртуализация продолжает оставаться одной из самых перспективных технологий ИТ-рынка. Включение мер по защите сред виртуализации в новые приказы ФСТЭК России – это движение в правильном направлении. Однако, к сожалению, требования не так однозначны. Поэтому можно предположить, что приказ вызовет большое количество вопросов об интерпретации приведенных там терминов и понятий.

Популярность технологий виртуализации закономерно приводит к тому, что производители средств защиты информации стремятся максимально адаптировать свои продукты для работы в виртуальной среде. Необходимо или нет применять специализированные инструменты защиты – это вопрос, который на сегодняшний день актуален практически для всех российских экспертов. В большинстве специализированных решений для защиты информации в виртуализированной инфраструктуре уже предусмотрена тесная интеграция с платформой виртуализации, и следует ожидать, что поставщики платформ виртуализации будут расширять возможности их взаимодействия со средствами защиты или сами встанут на путь их разработки.

Сидорова М.Е.

Разработчики средств защиты при предоставлении информации ставили отметку о реализации технической меры, если продукт:

- Полностью или частично выполняет техническую меру для того или иного из уровней защищенности.
- Участвует или, в некоторых случаях, может участвовать в выполнении технической меры.
- В некоторых случаях, прямо или косвенно, может поддерживать выполнение технической меры. Например, обеспечивает выполнение требований только в части собственных средств и/или отдельных объектов или может использоваться только в гибридных инфраструктурах или с соблюдением особых условий.

Вопрос сертификации средств защиты информации продолжает оставаться «серой зоной». При проектировании и построении системы защиты информации архитектору системы необходимо изучить конкретные условия и ограничения по эксплуатации сертифицированной продукции, указанные в официальной документации на продукцию (а не в маркетинговых проспектах), и учитывать не только функциональные возможности продукции, но и требования действующих на момент принятия решения нормативных документов.

При использовании в информационных системах сертифицированных по требованиям безопасности информации средств защиты информации виртуализированной инфраструктуры необходимо руководствоваться положениями раздела 12 приказа ФСТЭК России от 18 февраля 2013 г. № 21 и приказом ФСТЭК России от 11 февраля 2013 г. № 17. При этом нужно отметить, что часть требований ФСТЭК России плохо адаптируется к специализированным средствам защиты виртуализированной инфраструктуры, за исключением требований к уровню контроля отсутствия недекларированных возможностей. В связи с этим часть средств защиты продолжает проходить сертификацию на соответствие требованиям технических условий.

Родыгин Е.В.

Дополнительная информация

Ассоциация профессионалов в области информационной безопасности RISSPA (Russian Information Systems Security Professional Association) создана в июне 2006 года под эгидой консорциума (ISC)2 и имеет официальный статус ALIG (Affiliated Local Interest Group).

Основные цели RISSPA: формирование сообщества профессионалов в области информационной безопасности, обмен опытом, повышение уровня знаний специалистов отрасли, продвижение идей информационной безопасности.

На базе RISSPA создано Cloud Security Alliance Russian Chapter - официально аккредитованное представительство Cloud Security Alliance в России (международная некоммерческая организация, лидер в области разработки стандартов, рекомендаций и инициатив, направленных на повышение безопасности и защищенности использования облачных вычислений).

RISSPA регулярно организует семинары и вебинары по актуальным темам в области информационной безопасности. Ассоциация некоммерческая, членство и участие в семинарах бесплатно.