ідентифікується, авторизується, виявляється, документується і при цьому забезпечується необхідний або заданий рівень її захищеності.

Список літератури

1. *Хорошко В.А.* – Методы и средства защиты информации/ Хорошко В.А., Чекатов А.А. – К.: Изд. Юниор, 2003. -504с.

2. *Ленков С.В.* – Методы и средства защиты информации. В 2-х томах/ Ленков С.В., Перегудов Д.А., Хорошко В.А. – К.: Арий, 2008.

3. *Домарев В.В.* – Безопасность информационных технологий. Методология создания систем защиты/ Домарев В.В. – К.: ООО «ТИД» ДС», 2001. -688с.

4. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.

5. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

6. *Егоров Ф.И.* – Задачи защиты информации/ Егоров Ф.И., Тискина Е.О., Хорошко В.А.// Захист інформації, №1, 2009. –с.5-12.

7. *Невойт Я.В.* – Модель потенциально-опасной группы для предупреждения утечки информации/ Невойт Я.В., Мазуренко Л.Н, Хорошко В.А., Чередниченко В.С.// Системи обробки інформації, вип.7 (79), 2009. -с.82-86.

8. *Кобозева А.А.* – Анализ информационной безопасности/ Кобозева А.А., Хорошко В.А. – К.: Изд. ГУИКТ, 2009. -251с.

У роботі розроблені вимоги до систем захисту інформації, які розробляються для захисту об'єктів. Наведена сукупність вимог до систем захисту і запропонований порядок проведення робіт.
Ключові слова: система захисту інформації, несанкціонований доступ.

В работе разработаны требования к системам защиты информации, которые разрабатываются для защиты объектов. Приведена совокупность требований к системам защиты и предложен порядок проведения работ.

Ключевые слова: система защиты информации, несанкционированный доступ.

The requirements to information security systems for objects defence are developed in the article. A set of requirements to the systems of defence is resulted and the order of operations is offered.
Key words: information security, unauthorized access.

Надійшла 13.05.2010

УДК 004.4

к.т.н., доцент Козюра В.Д., (ГУИКТ)
Юрх Н.Г. (НА СБ Украины)

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, БАЗИРУЮЩАЯСЯ НА ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ

Для описания технологии защиты информации конкретной информационной системы строится Политика информационной безопасности (ПИБ), которая представляет собой набор законов, правил, практических рекомендаций и практического опыта, определяющих управленческие и проектные решения в области защиты информации. По сути – это совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. На основе ПИБ строится управление, защита и распределение критической информации в системе. Она должна охватывать все особенности процесса обработки информации, определяя поведение информационной системы в различных ситуациях.

Целью разработки ПИБ является определение правильного (с точки зрения организации) способа использования информационных ресурсов, а также разработка процедур, предотвращающих или реагирующих на нарушения режима безопасности.

При разработке и проведении в жизнь ПИБ руководствуются следующими принципами:

–невозможность обойти защитные средства;
–усиление защиты самого слабого звена;
–недопустимость перехода в открытое состояние;
–минимизация привилегий пользователей;
–разделение обязанностей;
–многоуровневая комплексная защита;
–разнообразие используемых защитных средств;
–простота и управляемость информационной системы;
–обеспечение всеобщей поддержки мер безопасности.

Для конкретной информационной системы политика безопасности должна быть индивидуальной. Она зависит от технологии обработки информации, используемых программных и технических средств, структуры организации и т.д.

Для построения ПИБ рассматриваются следующие направления защиты информационной системы:

–защита объектов информационной системы;
–защита процессов, процедур и программ обработки информации;
–защита каналов связи;
–подавление побочных электромагнитных излучений и наводок;
–управление системой защиты.

По каждому из указанных направлений ПИБ должна описывать следующие этапы создания средств защиты информации:

1. Определение информационных и технических ресурсов, подлежащих защите.
2. Выявление полного множества потенциально возможных угроз и каналов утечки информации.
3. Проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки.
4. Определение требований к системе защиты.
5. Осуществление выбора средств защиты информации и их характеристик.
6. Внедрение и организация использования выбранных мер, способов и средств защиты.
7. Осуществление контроля целостности и управление системой защиты.

С момента начала финансового кризиса наблюдается повышение спроса на технологии виртуализации. Если в сегментах других технологических решений неблагоприятная экономическая ситуация спровоцировала спад продаж, то спрос на решения, построенные на технологиях виртуализации, значительно вырос. Большинство организаций оценило преимущества виртуальных технологий, а также простоту перевода текущих инфраструктур в виртуальную среду.

Виртуализация – это не только консолидация и уплотнение инфраструктуры. Это переход на другой уровень сервиса, гораздо более высокий уровень безопасности не только в области хранения данных, но и в области надежности инфраструктуры в целом. Если раньше для достижения аналогичного уровня надежности требовалось использовать дорогостоящие решения, то сейчас можно меньшими усилиями добиться требуемого результата. Повышение уровня безопасности работы с данными является основным стимулом, приводящим заказчиков либо к терминальным решениям, либо к виртуализации.

Например, средства серверной виртуализации позволяют более эффективно использовать имеющееся серверное оборудование вычислительных сетей. Происходит некое уплотнение инфраструктуры за счет более рационального использования серверных

мощностей. В последнее время на рынок стали выходить и другие средства виртуализации, например, виртуальные рабочие места.

Перспективной технологией является виртуализация приложений. У современного пользователя компьютерной техники есть потребность в запуске определенного программного приложения, но нет технической возможности или необходимости его устанавливать (допустим, оно конфликтует с другими приложениями). При виртуализации приложение упаковывается в своеобразный «контейнер» с собственной файловой структурой и реестром, а пользователю направляется ссылка, щелкнув по которой он может запустить приложение и работать таким же образом, как и в случае его локальной установки. Такой механизм обеспечивает как доступность приложения для пользователя, так и возможность контроля прав доступа со стороны администратора.

С появлением технологий виртуализации появилась насущная необходимость расширить перечень позиций, входящих в свод политики информационной безопасности.

Обеспечение информационной безопасности инфраструктуры информационных технологий предусматривает решение двух основных задач:

1. Обеспечение состояния конфиденциальности, целостности и доступности информации, наблюдаемости и управляемости информационных систем организационными и программно-техническими средствами.

2. Обеспечение соответствия требованиям законодательства и нормативным документам по технической защите информации в отношении защиты конфиденциальной информации и персональных данных.

Вместе с тем обработка информации в виртуальной среде имеет свои специфические особенности, отсутствующие в физической среде:

–информация обрабатывается, как правило, в гостевых машинах, которые находятся под полным контролем гипервизора, способного абсолютно незаметно для традиционных средств защиты информации перехватывать все данные, идущие через устройства;

–администратор виртуальной инфраструктуры, имеющий права доступа к гипервизору, становится важнейшим субъектом безопасности информационной системы – фактически он может получить доступ к информационным ресурсам в обход существующей политики информационной безопасности компании;

–средства управления виртуальной инфраструктурой представляют собой самостоятельный объект атаки, проникновение к ним дает возможность нарушителю получить доступ к гипервизорам серверов виртуализации, а затем к конфиденциальным данным, обрабатываемым на гостевых машинах;

–традиционные средства защиты информации, разработанные для защиты физической инфраструктуры, могут не учитывать существование гипервизора, являющегося фактически нарушителем, реализующим атаку «человек в середине», при взаимодействии гостевой машины со всеми устройствами;

–диски гостевых машин обычно размещаются в сетевых хранилищах, которые должны физически защищаться как самостоятельные устройства;

–традиционные межсетевые экраны не контролируют трафик внутри сервера виртуализации, где могут находиться десятки гостевых машин, взаимодействующих между собой по сети, однако этот сетевой трафик не покидает сервера виртуализации и не проходит через физические межсетевые экраны и другое физическое сетевое оборудование;

–каналы передачи служебных данных серверов виртуализации обычно не защищены, хотя по этим каналам среди прочих данных передаются фрагменты оперативной памяти гостевых машин, которые могут содержать конфиденциальные данные.

К особенностям виртуальных инфраструктур относится также простота создания и ввода в эксплуатацию гостевых машин, что приводит к эффекту разрастания парка

виртуальных машин, получившему название Virtual Sprawl. Слабоконтролируемый рост числа виртуальных машин приводит к проблемам безопасности, поскольку часть виртуальных машин не получает должного уровня администрирования, включая установку обновлений и настройку параметров безопасности.

Виртуальная инфраструктура повышает степень внедрения вычислительных средств, уменьшая количество физического оборудования при таком же количестве сетевых приложений, сервисов, рабочих мест и т.п., что означает усложнение структуры взаимодействия субъектов. Поэтому повышать защищенность виртуальной инфраструктуры нужно комплексно, комбинируя сетевые и локальные средства защиты. Необходимо использовать широкий спектр набора защитных механизмов:

–средства сетевой аутентификации и авторизации пользователей;

–межсетевое экранирования как внутри сервера виртуализации между гостевыми машинами, так и по периметру виртуальной инфраструктуры;

–системы регистрации, сбора и корреляционного анализа событий безопасности;

–средства разграничения доступа (и делегирования полномочий) к виртуальным машинам и к самому серверу виртуализации (его гипервизору);

–системы контроля целостности конфигураций, распределенных компонентов виртуальной инфраструктуры;

–средства антивирусной защиты и управления доступом к элементам виртуальной инфраструктуры.

Администратору виртуальной инфраструктуры предоставляется доступ к серверу виртуализации, что фактически означает предоставление доступа к десяткам виртуальных машин, поэтому здесь нужна политика управления доступом и организация ролевой модели управления, построенной на базе делегирования административных функций от главного администратора к подчиненным. Организациям, модель нарушителя которых включает администраторов серверов, следует так предоставлять полномочия, чтобы исключить возможность «самосанкционирования». Модель такого предоставления полномочий может реализовываться через:

–систему заявок на предоставление доступа, проходящих процедуру согласования у владельцев соответствующих информационных ресурсов;

–специальный механизм управления правами в системе разграничения доступа администратором безопасности, не имеющим прав на систему виртуализации, а администратор системы виртуализации, в свою очередь, не имеет полномочий на назначение прав в системе разграничения доступа.

Разумно также использовать комбинацию этих двух подходов.

Необходимо обеспечить безопасность информации в сетевых хранилищах данных. Для этого надо преобразовать сеть таким образом, чтобы файлы-изображения виртуальных машин размещались в изолированном сетевом хранилище, доступ к которому контролируется межсетевым экраном. Кроме того, если стоит задача обеспечить изоляцию данных в сетевом хранилище от администратора сервера виртуализации, то необходимо убедиться, что эта задача решается выбранными техническими средствами. Для получения доступа к данным виртуальных машин администратор может воспользоваться как штатными возможностями среды управления виртуализацией, так и своими административными полномочиями на самом сервере виртуализации, благодаря которым он может иметь прямой доступ к дискам виртуальных машин. Важно обеспечить такую модель безопасности, чтобы администратор мог в полном объеме выполнять свои функции по администрированию виртуальной инфраструктуры, но при этом не имел доступа к данным, обрабатываемым внутри виртуальных машин, которые создаются их пользователями.

Если отсутствует возможность выделить средство хранения данных для серверов

виртуализации (а к этому хранилищу обращаются также приложения и сервисы с самих гостевых виртуальных машин и пользователи физических рабочих мест), то задача обеспечения безопасности усложняется. В этом случае необходимо обеспечить фильтрацию трафика по протоколам, которые поддерживаются сетевыми хранилищами данных, запретить создание несанкционированных устройств сетевого хранения данных на физических рабочих местах и внутри гостевых виртуальных машин.

Следует подчеркнуть необходимость контроля целостности конфигураций виртуальных машин с целью предотвращения добавления неразрешенных устройств (в основном накопителей различных типов) в гостевой виртуальной машине, на которые нарушитель может выполнить копирование конфиденциальной информации.

Нужно отметить, что при защите персональных данных, обрабатываемых на серверах виртуализации, требуется использование межсетевого экранирования высокого класса защищенности. В частности, необходимо проводить аутентификацию входящих и исходящих соединений, определять начало и окончание сеансов связи. Эти действия должны выполняться и в отношении соединений со стороны администратора виртуальной инфраструктуры.

Одним из решений для обеспечения эффективного управления и обеспечения безопасности в виртуальной инфраструктуре предприятия является Reflex Virtualization Management Center (VMC), который предоставляет возможность центрам обработки данных нового поколения, использующим технологии виртуализации, обеспечивать выполнение комплексных политик информационной безопасности, управлять и обеспечивать защиту виртуальных серверов, рабочих станций и сетей в сложной гетерогенной среде.

Reflex VMC предоставляет единую среду управления для сложных виртуальных сред, построенных на решениях различных производителей. Единая база данных событий, механизмы анализа в сочетании с удобным пользовательским интерфейсом делают Reflex VMC удобным инструментом администратора для мониторинга, контроля и управления динамической виртуальной инфраструктурой. Следствием этого является эффективное управление инфраструктурой виртуализации и высокий уровень обеспечения информационной безопасности.

Контроль соответствия – это одна из важных функций Reflex VMC, которая позволяет определять политики безопасности, контролировать их выполнение, и, в случае обнаружения нарушений, предпринимать корректирующие действия. Политики могут быть определены для отдельных виртуальных машин, групп машин, зон доверия и т.п. Каждая политика может включать в себя широкий набор критериев, основанных на конфигурации виртуальных машин и инфраструктуры, поведении машин, анализе сетевого трафика.

Немаловажную роль играет возможность эффективно управлять сетевой безопасностью виртуальной инфраструктуры, предоставляя функциональность межсетевых экранов и систем предотвращения вторжений для контроля трафика между виртуальными машинами. Отличительной особенностью Reflex VMC является формирование динамических «зон доверия», для которых определяются детальные политики безопасности. Включение виртуальных машин в определенную зону доверия может осуществляться как вручную администратором системы, так и автоматически на основе различного рода критериев, как например, наличие на машине конкретного программного обеспечения, или используемой операционной системы, или просто названия машины.

Список литературы

1. *Петренко С.А., Курбатов В.А.* Политики информационной безопасности. — М.: Компания АйТи, 2006. — 400 с.

2. *Бармен Скотт.* Разработка правил информационной безопасности. М.: Вильямс, 2002. — 208 с.

У статті розглянуто питання побудови політики безпеки для технологій, які використовують віртуалізацію, приведені принципи, які використовуються для побудови політики безпеки, а також наводяться приклади напрямів захисту інформації, які слід враховувати при побудові політики безпеки.
Ключові слова: політика безпеки, інформаційна безпека, віртуальне середовище.

В статье рассматривается вопрос построения политики безопасности для технологий, которые используют виртуализацию. Определены принципы, которые используются для построения политики безопасности, а также приводятся примеры направлений защиты информации, учитываемые при построении политики безопасности.
Ключевые слова: политика безопасности, информационная безопасность, виртуальная среда.

In this article the question of construction of policy of safety is considered for technologies which use a virtualization, principles which are used for the construction of policy of safety are resulted, and also examples of directions of defence information are made, which are necessary to take into account at the construction of policy of safety.
Keywords: security policy, information security, virtual environment.

Поступила 27.04.2010

УДК 681.3.96

к.т.н. Волощенко А.С.
військова частина Е-6133

КОНЦЕПТУАЛЬНІ ПІДХОДИ ВПРОВАДЖЕННЯ НОВІТНІХ ТЕХНОЛОГІЙ ДО ПОБУДОВИ КОМПЛЕКСІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Проблема забезпечення ефективного технічного захисту інформації набуває все більшої актуальності, що обумовлено багатьма причинами, пов'язаними як із загальним технічним прогресом у всьому світі, так і з внутрішніми політичними, економічними та соціальними факторами. Присутня на теперішній час підвищена вразливість інформації, що обробляється, передається та зберігається із застосуванням засобів обчислювальної техніки, зв'язку, запису, розмножувальної техніки та інших технічних засобів і систем, якими в теперішній час широко устатковуються будь-які державні та комерційні структури, є наслідком стрімкого розвитку як самих перелічених технічних засобів та систем, так і методів та засобів перехоплення інформації.

Розвиток ринкових відносин в нашій державі загострив проблему безпеки інформації, при цьому стрімкого розвитку набули два процеси:

- перший, з добутку інформації або завдання їй деструктивної шкоди;
- другий, із захисту інформаційних ресурсів.

За умов політики відкритості та свободи преси, особливо важливим стає забезпечення ефективного захисту інформації. Ця проблема однаково актуальна для інформаційних систем, систем зв'язку та управління, що належать підприємствам різної форми власності, взагалі там, де циркулюють великі об'єми інформації різного рівня конфіденційності.

Для запобігання витоку інформації технічними каналами є необхідними спеціальні заходи, методи та засоби захисту.

Слід відмітити, що активний метод захисту (зашумлення) розвивався інтенсивніше та швидше впроваджувався, оскільки не потребував серйозних фінансових витрат при виробництві. Така ситуація зберігалася до початку 90-х років минулого століття. Процес, так званої, перехідної економіки згенерував створення структур недержавної власності, що займаються проблемами безпеки інформації, до яких увійшли досвідчені фахівці з державних підприємств та організацій. Доступнішими стали новітні технології і публікації з питань інформаційної безпеки. Зазначені фактори стимулювали прискорення розвитку низки методів, способів та засобів захисту інформації.