Решения Microsoft и 5nine для выполнения требований PCI DSS в среде виртуализации Hyper-V

ОБЗОР

Быстрый рост числа кибератак и нарушений конфиденциальности персональных данных делает критически важной защиту финансовых операций.

Ведущие мировые операторы платежных систем: Visa, MasterCard, American Express, JCB и Discover – совместно установили стандарт «Стандарт безопасности данных индустрии платежных карт (PCI DSS). Требования и процедуры аудита безопасности», чтобы повысить надежность финансовых транзакций.

Все организации, которые хранят, обрабатывают и передают данные держателей платежных карт вышеупомянутых платежных систем, обязаны выполнять требования PCI DSS.

Хотя, требования стандарта PCI DSS не являются законом, его соблюдение значительно повышает защищенность финансовых операций и данных клиентов:

- Финансовые учреждения повышают доверие владельцев платежных карт, обеспечивая безопасность среды оплаты при обмене конфиденциальными данными;
- Выполнение требований стандарта улучшает репутацию банков-эквайеров и эмитентов карт;
- Использование предлагаемых PCI DSS технологий помогает предотвратить утечку персональных данных и мошенничество со средствами банков и клиентов.

Кроме того, банки конкурируют в борьбе за клиентов и сталкиваются с противоречием: нужно повышать защищенность платежей и при этом уменьшать стоимость услуг.

Использование виртуализации при создании банковских информационных систем помогает разрешить это противоречие.

Но применение этой технологии, помимо экономии средств, гибкости и масштабируемости несет в себе новые угрозы, неизвестные при построении ИС на базе аппаратных решений: динамическое изменение ресурсов и конфигураций виртуальной среды, необходимость изоляции виртуальных машин и сетей, атаки на уровне гипервизора и виртуальных сетей и многое другое. Обеспечить выполнение этих противоречивых требований можно только при помощи современных средств защиты информации, интегрированных в операционную систему на уровне гипервизора. Это единственный путь закрыть уязвимости виртуальной среды без понижения ее производительности и управляемости.

Такой подход позволит снизить стоимость средств защиты и ускорить отдачу вложений в виртуализацию, что в нынешнее время является ключевым фактором внедрения современных информационных технологий, в т.ч. в сфере ИБ финансовых институтов.

5nine Cloud Security является решением, которое может помочь финансовым учреждениям выполнить большинство требований PCI DSS. Его централизованное управление упрощает администрирование безопасности и обеспечивает возможности аудита на соответствие требованиям PCI DSS и законов РФ, таких как *Федеральный закон N°152-ФЗ «О персональных данных», Приказов ФСТЭК N°17, 21* и других.

5nine Cloud Security представляет собой комплексное решение по обеспечению безопасности виртуальной среды, разработанное специально для защиты Microsoft Hyper-V с помощью запатентованных технологий, устраняя необходимость в закупке дополнительного дорогостоящего и ресурсоемкого оборудования и ПО.

Решение от 5nine Software включает в себя все три необходимых уровня защиты ИС: многопользовательский межсетевой экран, безагентный антивирус Лаборатории Касперского и Систему обнаружения вторжений для защиты от атак на уровне приложений.

В самом стандарте, приведены 12 требований и описаны соответствующие процедуры проведения оценки соответствия. Давайте посмотрим, как эти требования выполняются при помощи средств **Windows Server 2012 R2** и **5nine Cloud Security** в среде Hyper-V:

ЦЕЛИ КОНТРОЛЯ	ТРЕБОВАНИЯ PCI DSS	РЕАЛИЗАЦИЯ ПРИ ПОМОЩИ 5NINE CLOUD SECURITY
ПОСТРОЕНИЕ И СОПРОВОЖДЕНИЕ ЗАЩИЩЁННОЙ СЕТИ	Установка и обеспечение функционирования межсетевых экранов для защиты данных держателей карт	5nine Cloud Security обеспечивает защиту при помощи многопользовательского межсетевого экрана, который встроен в виртуальный коммутатор Hyper-V и позволяет контролировать любой тип трафика (внутренний, внешний, частные виртуальные сети), изолировать как отдельные ВМ, так и их группы. Возможна настройка расписания применения правил межсетевого экрана.
	Неиспользование выставленных по умолчанию производителями системных паролей и других параметров безопасности	5nine Cloud Security поддерживает Active Directory Windows Server (AD) для управления доступом пользователей и паролями в многопользовательской среде. При этом не используются пароли по умолчанию, чтобы уменьшить возможность ошибки администраторов.
ЗАЩИТА ДАННЫХ ДЕРЖАТЕЛЕЙ КАРТ	Обеспечение защиты данных держателей карт в ходе их хранения.	Это требование относится к ограничению физического доступа и не относятся к защите среды виртуализации.
	Обеспечение шифрования данных держателей карт при их передаче через общедоступные сети	5nine Cloud Security не имеет функции криптографии, однако он поддерживает передачу шифрованного трафика по виртуальной сети, защищая его, как любой другой вид трафика.

ЦЕЛИ КОНТРОЛЯ	ТРЕБОВАНИЯ PCI DSS	РЕАЛИЗАЦИЯ ПРИ ПОМОЩИ 5NINE CLOUD SECURITY
ПОДДЕРЖКА ПРОГРАММЫ УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ	Использование и регулярное обновление антивирусного программного обеспечения	5nine Cloud Security является единственным безагентным антивирусным решением для Hyper-V, созданным для увеличения производительности виртуальной платформы. Продукт обеспечивает защиту ВМ и сетей от вирусов без установки агента в ВМ в базовом сценарии, обеспечивая скорость сканирования до 70 раз быстрее стандартных антивирусов, устанавливаемых в ВМ. Безагентный антивирус не может быть отключен или удален пользователем. Предлагаются на выбор антивирусные ядра от Лаборатории Касперского, Bitdefender или ThreatTrack, которые дают максимальное покрытие уязвимостей. Сигнатуры могут обновляться как с ресурсов производителя, так и с локального прокси сервера для увеличения защищенности в соответствии с рекомендациями PCI DSS на ежедневном базисе.
	Разработка и поддержка безопасных систем и приложений	5nine Cloud Security дает возможность изолировать среду разработки/тестирования и производственного функционирования за счет использования групп безопасности. Продукт позволяет реализовать административный доступ к приложениям через консоль управления. Существует логирование операций с возможностью просмотра базы данных событий администратором безопасности для отслеживания угроз и попыток неавторизованного доступа к управлению системами защиты. В составе продукта есть Система обнаружения вторжений (IDS) на уровне приложений, которая отслеживает весь трафик внутри виртуального коммутатора Hyper-V, используя технологию Snort для проверки аномалий пакетов, которыюе могут быть потенциальными атаками.
РЕАЛИЗАЦИЯ МЕР ПО СТРОГОМУ КОНТРОЛЮ ДОСТУПА	Ограничение доступа к данным держателей карт в соответствии со служебной необходимостью	5nine Cloud Security поддерживает Active Directory Windows Server (AD) для управления доступом пользователей и паролями в многопользовательской среде.
	Присвоение уникального идентификатора каждому лицу, имеющему доступ к информационной инфраструктуре	5nine Cloud Security поддерживает Active Directory Windows Server (AD) для управления доступом пользователей и паролями в многопользовательской среде. Каждому пользователю в AD присваивается уникальный идентификатор доступа.
	Ограничение физического доступа к данным держателей карт	Это требование относится к ограничению физического доступа и не относятся к защите среды виртуализации
РЕГУЛЯРНЫЙ МОНИТОРИНГ И ТЕСТИРОВАНИЕ СЕТИ	Контроль и отслеживание всех сеансов доступа к сетевым ресурсам и данным держателей карт	Реализуется при помощи стандартных средств контроля доступа Windows Server и системы логирования событий безопасности 5nine Cloud Security.
	Регулярное тестирование систем и процессов обеспечения безопасности	5nine Cloud Security постоянно регистрирует и контролирует статистические данные о сетевом трафике, пакетах и их размерах. Затем, используя эвристический подход, он создает базовую модель вашего нормального рабочего трафика в течение дня. После этого он постоянно следит за средой, и, если изменения значений превышают установленные пороги чувствительности, немедленно оповещают вас о возможной атаке или злонамеренном сканировании сети.
ПОДДЕРЖКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	Разработка, поддержка и исполнение политики информационной безопасности	Это требование относится к администрированию процессов объекта защиты.

Подводя итог, 6 требований PCI DSS из 12 относятся к безопасности виртуальной среды и могут быть выполнены внедрением **5nine Cloud Security**. 4 решаются стандартными средствами **Microsoft Windows Server 2012 R2**, а остальные требования могут быть удовлетворены с помощью физических ограничений и корпоративных политик.

5nine Cloud Security в среде Windows Server поможет финансовым организациям технологично и экономно выполнить большинство требований PCI DSS, чтобы повысить безопасность финансовых операций и предоставить конкурентоспособные услуги клиентам.

Вы заинтересованы в получении дополнительной информации о соответствии PCI DSS? Оставьте свои комментарии или вопросы, и мы будем рады ответить на них!

Посетите www.5nine.ru или напишите на info@5nine.ru для получения дополнительной информации о решениях 5nine Software для PCI DSS.

Microsoft Partner
Gold Datacenter