

Применение компенсационных мер при реализации требований стандарта PCI DSS

Максим Эмм

Директор департамента аудита
MBA, CISA, CISSP, PCI QSA



Информзащита
Системный интегратор

Информзащита и стандарты PCI

- Комплексные услуги по достижению PCI DSS и PA DSS compliance
- Более 150 успешных проектов по тематике PCI с 2006 года



**Дедлайн по достижению
соответствия PCI DSS
30 сентября 2010 г.**



**Дедлайн по использованию не
сертифицированных по PA DSS
приложений для новых решений
1 июля 2010 г.**

**Дедлайн по завершению перехода
на использование сертифицированных
по PA DSS приложений
1 июля 2012 г.**



Титаник – непотопляемое судно



Соответствие стандартам = Безопасность?

- Стандарт по безопасности судов был разработан в 1884 году
 - Для судов водоизмещением более 10000 тонн требовалось не менее 16 спасательных лодок
 - Модель угроз не предполагала столкновение с айсбергом
- Титаник затонул 14 апреля 1912 года
 - Водоизмещение было более 50000 тонн
 - На судне имелось 16 спасательных лодок, которые не могли вместить и 50% пассажиров и экипажа

Судно полностью соответствовало всем нормативным документам по безопасности!



PCI Compliance и безопасность

- Самые используемые пути проникновения
 - общеизвестные/разделяемые/украденные пароли
 - веб-уязвимости
 - некорректная конфигурация межсетевых экранов
 - среднее время доступности патча - 1 год
- Выявление инцидентов:
 - Внешние источники -70% случаев
 - Внутренние сотрудники и сбои в работе систем 25%
 - Мониторинг безопасности - 6%

81% не имели статуса PCI DSS Compliant
100% не выполняли требования PCI DSS



PCI Compliance в России

- 13 PCI DSS Compliant сервис-провайдеров в регионе CEMEA
 - UCS
 - ЗСПЦ
 - Cronopay
 - ~~Рукард~~
- Около 30 PA DSS Compliant вендоров (middleware). Из популярных в России
 - Way4
 - Base24
 - Compass+
- Средние результаты
 - 1-го аудита - 54%
 - 2-го аудита - 72%
- Самостоятельное исполнение годового плана нормативная база и «hardening security»



Структура стандарта PCI DSS



Требования PCI DSS

Построение и поддержание защищенной сети

- 1. Должны быть обеспечены разработка и управление конфигурацией межсетевых экранов в целях защиты данных платежных карт
- 2. Не должны использоваться параметры безопасности и системные пароли, установленные производителем по умолчанию

Защита данных платежных карт

- 3. Должна быть обеспечена защита данных платежных карт при хранении
- 4. Должно обеспечиваться шифрование данных платежных карт, передаваемых по сетям общего пользования

Реализация программы управления уязвимостями

- 5. Должно использоваться и регулярно обновляться антивирусное программное обеспечение
- 6. Должна обеспечиваться безопасность при разработке и поддержке систем и приложений



Требования PCI DSS (продолжение)

Реализация мер по строгому контролю доступа

- 7. Доступ к данным платежных карт должен быть ограничен в соответствии со служебной необходимостью
- 8. Каждому лицу, имеющему доступ к вычислительным ресурсам, должен быть назначен уникальный идентификатор
- 9. Физический доступ к данным платежных карт должен быть ограничен

Регулярный мониторинг и тестирование сетей

- 10. Должен отслеживаться и контролироваться любой доступ к сетевым ресурсам и данным платежных карт
- 11. Должно выполняться регулярное тестирование систем и процессов обеспечения безопасности

Поддержание политики информационной безопасности

- 12. Должна поддерживаться политика информационной безопасности, регламентирующая деятельность сотрудников и контрагентов



Риск-ориентированный подход и PCI DSS



PCI DSS - Компенсационные меры

Допускаются для большинства требований

- Должны соответствовать цели оригинального требования
- Должны превосходить оригинальное требование и обеспечивать не меньший уровень защиты

Должны быть обоснованы техническими или бизнес ограничениями

- Необходимо документировать в соответствии с шаблоном
- Должны проверяться аудитором QSA
- Необходимо поддерживать в течение срока действия



Описание компенсационных мер

Ограничения	<ul style="list-style-type: none">• Перечислить ограничения, препятствующие выполнению исходного требования
Цель	<ul style="list-style-type: none">• Определить цель исходных защитных мер и компенсационных мер
Риск	<ul style="list-style-type: none">• Описать дополнительные риски, возникающие вследствие невыполнения исходного требования
Компенсационные меры	<ul style="list-style-type: none">• Определить компенсационные меры
Оценка компенсационных мер	<ul style="list-style-type: none">• Описать как компенсационные меры будут оцениваться и проверяться
Поддержание компенсационных мер	<ul style="list-style-type: none">• Описать как компенсационные меры будут поддерживаться



Когда необходимы компенсационные меры

- Программное обеспечение не сертифицировано по PA DSS
- «Вырожденная» разработка ПО
- Нестандартный или малый масштаб бизнеса
- Более высокий уровень обеспечения ИБ в компании чем требует PCI DSS



Шаблон описания КОМПЕНСАЦИОННЫХ мер



Appendix C: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where compensating controls are used to meet a PCI DSS requirement. Note that compensating controls should also be documented in the Report on Compliance in the corresponding PCI DSS requirement section.

Note: Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.

Requirement Number and Definition:

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	<input type="text"/>
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	<input type="text"/>
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	<input type="text"/>
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	<input type="text"/>
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	<input type="text"/>
6. Maintenance	Define process and controls in place to maintain compensating controls.	<input type="text"/>



Пример компенсационных мер 1

Требование	<ul style="list-style-type: none">• 8.1 Каждому пользователю должен быть присвоен уникальный идентификатор до предоставления доступа к системным компонентам или данным платежных карт
Ограничения	<ul style="list-style-type: none">• Используются сервер Unix с локальной аутентификацией, для администрирования которых должна использоваться учетная запись root различными сотрудниками
Цель	<ul style="list-style-type: none">• Обеспечить отслеживание действий каждого сотрудника в системе• Предоставить каждому сотруднику минимально достаточные права
Риск	<ul style="list-style-type: none">• В случае злоумышленных действий администратора ОС/СУБД или злоумышленника, завладевшего паролем администратора (кража злоумышленником части или целой БД), высок риск компрометации данных платежных карт клиентов
Компенсационные меры	<ul style="list-style-type: none">• Запрещается удаленный вход в систему для учетной записи root• Все администраторы должны аутентифицироваться под своими персональными учетными записями и использовать команду SU для выполнения задач по администрированию



Пример компенсационных мер 2

Требование	<ul style="list-style-type: none">• 3.4 Номера PAN должны быть приведены к нечитаемому виду вне зависимости от места хранения (включая данные на портативных носителях, резервных копиях, в журналах)
Ограничения	<ul style="list-style-type: none">• Временно используется ПО, не поддерживающее базы данных с реализованным шифрованием, что не позволяет привести PAN к нечитаемому виду
Цель	<ul style="list-style-type: none">• Минимизация риска несанкционированного копирования большого количества незашифрованных данных PAN путем внедрения дополнительных защитных мер по управлению и контролю доступа к этим данным
Риск	<ul style="list-style-type: none">• В случае злоумышленных действий администратора ОС/СУБД или злоумышленника, завладевшего паролем администратора, высок риск компрометации данных платежных карт клиентов
Компенсационные меры	<ul style="list-style-type: none">• Дополнительно ограничить доступ к БД Oracle и ОС серверов<ul style="list-style-type: none">• Выделение серверов с БД в отдельный сетевой сегмент и настройки ACL• Установка терминального сервера для доступа администраторов с протоколированием всех действий и двухфакторной аутентификацией



Примеры компенсационных мер 3

Требование	<ul style="list-style-type: none">• 8.5.15 При отсутствии активности во время пользовательского сеанса более чем 15 минут должен выполняться повторный запрос пароля пользователя для разблокировки терминала
Ограничения	<ul style="list-style-type: none">• В связи с производственной необходимостью для службы технической поддержки на серверах приложений не может быть установлен разрыв сессии при отсутствии активности пользователя меньше чем 3 часа
Цель	<ul style="list-style-type: none">• Минимизация риска несанкционированного доступа к серверам приложений через активные сессии
Риск	<ul style="list-style-type: none">• При отсутствии разрыва сессии на операционной системе сервера приложений повышается риск получения несанкционированного доступа к серверам приложений во время отсутствия сотрудника на рабочем месте или перехвата активной сессии
Компенсационные меры	<ul style="list-style-type: none">• Доступ к приложениям реализован через терминальный сервер Citrix в выделенном сетевом сегменте, где находятся сервера приложений и настроены ACL так что доступ в обход Citrix невозможен• Установить блокировку неактивных сессий на уровне Citrix – 15 минут для исключения риска использования консоли сотрудника во время его отсутствия• Включить шифрование доступа к Citrix для исключения перехвата сессий



Пример компенсационных мер 4

Требование	<ul style="list-style-type: none">• 3.5.2 Должно выполняться безопасное хранение криптографических ключей
Ограничения	<ul style="list-style-type: none">• Используемое ПО для резервного копирования не позволяет хранить ключи шифрования резервных копий баз данных в зашифрованном виде и хранит их в открытом виде в файле на диске
Цель	<ul style="list-style-type: none">• Минимизация риска несанкционированного доступа к ключу шифрования
Риск	<ul style="list-style-type: none">• Администратор ОС сервера резервного копирования обладает возможностью скопировать ключ шифрования, сделать копию зашифрованной резервной копии и расшифровать ее, получив несанкционированный доступ к данным платежных карт
Компенсационные меры	<ul style="list-style-type: none">• Настроить права доступа к файлу ключей таким образом, чтобы кроме приложения резервного копирования никто не имел доступа к файлу включая администраторов ОС• Настроить аудит ОС на доступ к файлу с ключом, на изменение прав доступа к файлу с ключом• Расследовать все попытки доступа или изменения прав доступа к файлу ключа шифрования за исключением доступа приложения



К чему нельзя применять компенсационные меры

- Хранение критичных данных авторизации
- Наличие политики безопасности
- Распределение ответственности за обеспечение безопасности
- Межсетевое экранирование
- Шифрование данных платежных карт при передаче через Internet



Безопасность критичных данных

	Элемент Данных	Хранение Разрешено	Требуется защита	PCI DSS 3.4
Данные платежных карт (Cardholder data)	Номер карты (PAN)	Да	Да	Да
	Имя держателя карты (Cardholder Name)*	Да	Да	Нет
	Сервисный код (Service Code)*	Да	Да	Нет
	Дата истечения срока действия (Expiration Date)*	Да	Да	Нет
Критичные данные авторизации (sensitive authentication data)	Полное содержание магнитной полосы (Full Magnetic Stripe)	Нет	n/a	n/a
	CVC2/CVV2/CID	Нет	n/a	n/a
	PIN / PIN Block	Нет	n/a	n/a

