

Достижение соответствия PCI — best practice

Сергей Шустиков,
руководитель направления менеджмента ИБ, Digital Security,
PCI QSA

Определение приоритетов

1. Соответствие PCI — индикатор, а не самоцель
2. Погоня за соответствием отдаляет соответствие

Вывод:

Главная цель — обеспечение безопасности данных

Определение области применимости PCI DSS

1. Системы, обрабатывающие карточные данные
2. Связанные системы = не отделенные межсетевым экраном

Вывод:

Сегментация минимизирует область применимости и экономит ресурсы

Провели аудит — что дальше?

1. «Приоритетный подход» от PCI SSC
2. Никому не нужны «потемкинские деревни»

Вывод:

**Рекомендуется планирование поэтапного
достижения соответствия**

Приоритетный подход — этап 1

Удаление критичных аутентификационных данных и ограничение хранения данных о держателях карт

Отсутствие в информационной инфраструктуре критичных аутентификационных данных и других данных о держателях карт значительно снижает негативные последствия её компрометации

Приоритетный подход — этап 2

Защита периметра, внутренних и беспроводных сетей

Целью мероприятий этого этапа является защита наиболее уязвимых мест информационной инфраструктуры – активного сетевого оборудования и беспроводных точек доступа

Приоритетный подход — этап 3

Обеспечение безопасности платежных приложений

Уязвимости прикладного уровня предоставляют возможности для легкой компрометации данных о держателях карт

Приоритетный подход — этап 4

Управление и контроль доступа к системам

Необходимо отслуживать, кто, когда и как получает доступ к среде данных о держателях карт

Приоритетный подход — этап 5

Защита хранимых данных о держателях карт

Если с точки зрения бизнеса необходимо хранение данных о держателях карт, то следует внедрить механизмы защиты хранимых данных

Приоритетный подход — этап 6

Устранить оставшиеся несоответствия и убедиться в выполнении всех требований

Следует выполнить все оставшиеся требования стандарта и завершить разработку сопутствующих политик и процедур, необходимых для защиты данных о держателях карт

Организация работ

1. Достижение PCI — достаточно масштабный проект
2. Схема: «Заказчик» — «Консультант» — «Интегратор»

Вывод:

Необходима координация широкого круга сотрудников

Менеджмент ИБ

1. Документированный процесс — понятный процесс
2. Нормативная база должна быть простой

Вывод:

Формализация процесса избавит от бюрократии

ASV & Pentest

1. ASV — это сканирование, тест на проникновение — ручная работа
2. Цель теста на проникновение — привилегии в системе

Вывод:

**ASV и Pentest — механизмы мониторинга,
а не зачет и экзамен**

Соответствие достигнуто! Что дальше?

1. Поддержка соответствия — QSA окажет сопровождение
2. Нормативная база эффективна только в актуальном состоянии

Вывод:

Безопасность — непрерывный процесс

Вопросы?

PCI DSS.RU

by Digital Security

Сообщество, открытое для всех