Digital Compliance

Соответствие PCI DSS как побочный эффект

Павел Федоров, CISA, QSA, PA-QSA
Управляющий партнер

PCI DSS: эффективность

- Согласно последнему отчёту Verizon, за десять лет их работы ни одна компания, в которой произошёл инцидент, не соответствовала требованиям стандарта в полной мере на момент инцидента.

- Значит ли это, что соответствие требованиям стандарта — панацея?

Актуальные подходы к соответствию PCI DSS:

- Система живёт своей жизнью, документация — своей, а к аудиту их подгоняют под требования стандарта.
- Система и документация синхронизированы, требования PCI DSS выполняются, потому что этого требуют сотрудники ИБ и руководство.

Правило: PCI DSS — это стандарт, которому нужно соответствовать.

- Руководство боится санкций со стороны платёжных систем больше, чем реального инцидента.
- Существует трактовка результата оценки соответствия как «соответствует/не соответствует».
- У сотрудников, занимающихся вопросами ИБ, недостаточно ресурсов для качественного выполнения своих обязанностей.

Кстати, это значит, что требование 12.5 выполняется не в полной мере.

К чему это приводит?

- Бумажная безопасность вместо реальной.
- Выполнение контролей ради PCI DSS без оглядки на смысл.
- Построение контролей и процедур на основании «прочтения» стандарта, а не фактических задач.

Можно ли этого избежать?

Давайте представим себе, что у нас нет стандарта PCI DSS.

Нам просто нужно защитить карточные данные.

Как и любые другие данные, нужные для бизнеса.

Анализ рисков

- Определить активы: карточные данные;
- Определить угрозы — в первую очередь, компрометацию;
- Провести оценку рисков.

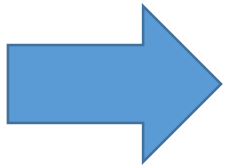
Оценка рисков — промежуточные этапы

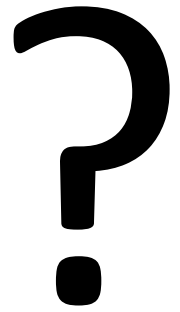
- Нарисовать схему инфраструктуры, отметить, на каких компонентах присутствуют карточные данные и где передаются и описать эти процессы.
- Определить оборудование и ПО, которые нужны для их обработки/передачи/хранения или влияет на эти процессы.
- …

Оценка рисков — результаты

- Необходимо ограничивать доступ к данным;
- При хранении и передаче данные нужно шифровать;
- Для разработки ПО нужно использовать SDLC;
- Для контроля изменений нужно использовать механизмы контроля целостности;
- Для проверки эффективности защитных мер нужно проводить тест на проникновение;
- Для разделения ответственности с другими организациями нужно прописывать эту ответственность в договоре;
- …

А как же сотрудники?





Вовлечение пользователей в процессы ИБ

- Объясняйте, *почему*, а не только *как*.
- Требования, причины которых понятны или хотя бы близки, исполнять проще, чем взятые из непонятного стандарта.
- Понимание задач ИБ хотя бы частью рядовых сотрудников позволяет улучшить их исполняемость.

Изменения в инфраструктуре: как быть с ними?

Инфраструктура живая и всё время меняется. Часто изменения происходят быстрее, чем их можно документировать. Важно помнить:

- Обеспечение мер безопасности на период изменения необходимо продумывать заранее, и они не должны быть менее серьёзными, чем в обычное время.

- Необходимо заранее регламентировать, как соотносятся между собой инфраструктура и регламентирующие документы.

Всё готово? PCI DSS как чеклист

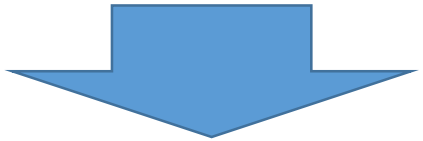
PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
12.1	Is a security policy established, published, maintained, and disseminated to all relevant personnel?	• Review the information security policy	☐	☐	☐	☐	☐
12.1.1	Is the security policy reviewed at least annually and updated when the environment changes?	• Review the information security policy • Interview responsible personnel	☐	☐	☐	☐	☐
12.2	(a) Is an annual risk assessment process implemented that: • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk? *Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.*	• Review annual risk assessment process • Interview personnel	☐	☐	☐	☐	☐
	(b) Is the risk assessment process performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.)?	• Review risk assessment documentation • Interview responsible personnel	☐	☐	☐	☐	☐

Новые версии стандарта

- Анализ рисков нужно проводить регулярно.
- К моменту выхода новой версии можно сверить предлагаемые изменения по результатам анализа рисков с новыми требованиями стандарта .

Итог:

- Анализ рисков как основа для использования любых защитных мер.
- Понимание задач бизнеса и ИБ, а не необходимость соблюдать набор требований.
- Использование PCI DSS как метрики правильности направления работы.



Соответствие требованиям PCI DSS как побочный эффект

Digital Compliance

Вопросы?

115054, Россия,
Москва,
ул. Ленинская Слобода, д.26

197046, Россия,
Санкт-Петербург,
Петроградская наб., 16 А

+7 (812) 703-15-47
+7 (495) 223-07-86
info@digitalcompliance.ru