Стандарт PA-DSS: безопасность платежных приложений

Москва, 25.03.2010

PA-DSS: Практика. Типовые задачи и способы их решения.

Владимир Кузнецов

Старший аудитор

Информзащита

Системный интегратор

Процесс сертификации

- Проверка процесса разработки и внесения изменений
- Лабораторные испытания
- Проверка исходного кода

Как долго процесс сертификации идет?

Недолго, так как разработчики оказались в высокой степени готовности благодаря достаточно зрелому процессу разработки и внесения изменений в ПО

Анализ исходного кода

Разработчик обоснованно не желает передавать исходный код на сторону для анализа

Решение

- Организация безопасного удаленного просмотра кода
- Локальная проверка кода разработчиком (заранее оговоренными специализированными инструментами) и отправка логов аудитору

Хранение номеров платежных карт

Номера платежных карт хранятся в журнале транзакций в незашифрованном виде (требование 2.3)

Решение

Так как в данном конкретном случае:

- журнал транзакций находится в файловой системе ОС Hypercom (Nucleos OS);
- для каждого приложения, устанавливаемого на POS-терминал через Application Manager, создается каталог с правами доступа только этому приложению;
- интерфейса командной строки в Application Manager нет. Доступ к каталогу ПО и следовательно к журналу транзакций получить не возможно,

то требование к журналу транзакций признано не применимым

Нестандартная схема идентификации

Приложение не поддерживает подход авторизации пользователей по идентификаторам/паролям (требование 3.1)

Решение

Так как возможности пользователей и администратора ограничены лишь операциями, не дающими доступ к данным платежных карт (не представляющими риск безопасности), то требование было признано не применимым в данном конкретном случае

Отсутствие требуемого функционала

- Пароли хранятся в открытом виде
- Двухфакторная аутентификация при удаленном доступе не реализована

Решение

- Доработка кода

Стандарт PA-DSS: безопасность платежных приложений

www.pcisecurity.ru

Кузнецов Владимир
Старший аудитор

- (495) 980-2345 доб. 248
- v.kuznetsov@infosec.ru