“Стандарт PA-DSS: безопасность платежных приложений”

Семинар компании «Информзащита»

г. Москва, 25 марта 2010 г., Holiday Inn Suschevsky

Введение в проблематику PA-DSS

Гольдштейн Анна, PA QSA

Заместитель директора департамента аудита

Информзащита

Системный интегратор

PA-DSS: Причины появления

- Невозможность или сложность выполнения требований PCI DSS
  - Сохранение TRACK,CVC2/CVV2,PINBLOCK приложением
  - Невозможность удалить/вычистить TRACK,CVC2/CVV2 из архивов
  - Хранение номеров карт (PAN) в открытом виде
  - Отказ поддержки вендором приложения патчей на СУБД

“Серебряная пуля” PCI DSS

- Реализация переложена на разработчиков:
  - Все применимые к прикладному уровню требования PCI DSS
  - Возможность работы приложения в PCI DSS-compliant среде
  - Контроль уровня безопасности приложения
  - Решение проблемы совместимости с обновлениями безопасности платформ

PA-DSS: краткая информация

- Основная цель – поддержка реализации PCI DSS
- Является прямым наследником VISA PABP
- Дата рождения: апрель 2008
- Разработчик – PCI Security Standards Council (PCI SSC)
- Ориентирован на разработчиков платежных приложений
- Форма подтверждения соответствия – сертификация
- Сертификацию проводит компания, имеющий статус PA QSA

Что сертифицировать?

- Подлежит сертификации, если:
  - Обрабатывает номера карт (PAN) в рамках авторизации/расчетов
  - Разрабатываются на продажу, не являются разовой заказной разработкой
- Основные виды сертифицируемого ПО
  - ПО процессинга (front-office, back-office (расчеты), middleware/switching)
  - ПО для банкоматов
  - ПО для POS-терминалов
  - ПО для поддержки электронной коммерции
  - ПО мобильной коммерции
- Исключение: отдельно стоящие POS терминалы, если:
  - подключены напрямую к эквайеру
  - не хранят данных платежных карт
  - обновляются разработчиком ПО

Поддержка сертификации

- Сертифицируется конкретная версия приложения
- Срок действия сертификата – 3 года
- При обновлении приложения необходима досертификация
- Процедура зависит от характера вносимых изменений

- Затронуты вопросы безопасности или реализация платежного процесса ?
  - «НЕТ» - подтверждение от аудитора факта отсутствия влияния
  - «ДА» - проведение сертификационных проверок (их части)

Зачем сертифицировать?

- Внедрение PA-DSS реализуют МПС независимо друг от друга
- Требования по внедрению направлены на членов МПС
- Обязательные сроки перехода на PA-DSS сертифицированные приложения от Visa Inc.:
  - С 1 июля 2010г - Новые мерчанты обязаны соответствовать PCI DSS или использовать PA-DSS сертифицированное ПО
  - до 1 июля 2012 г - Эквайеры обязаны удостовериться, что все мерчанты и агенты используют PA-DSS сертифицированное ПО

Рынок сертифицированного ПО

- Более 150 вендоров имеют сертификат PA-DSS*
- Около 700 сертифицированных приложений
- 60% приложений – «POS-related»
- Основной поток сертификации начался в 2009г
- Сертифицированное ПО процессинга (из любимых в России): Base24, Way4, Tranzware
- Ежегодная плата PCI SSC за публикацию в списке сертифицированных $1 250

* - Информация по опубликованным данным PCI SSC (https://www.pcisecuritystandards.org/security_standards/vpa/)

Информзащита
Системный интегратор

Требования стандарта PA-DSS

ВСЕГО 14 ТРЕБОВАНИЙ И ПОЧТИ 120 ПРОЦЕДУР АУДИТА

Сертифицируемое приложение	Компания-разработчик
Исключение хранения критичных данных карт (TRACK,CVC2/CVV2,PINBLOCK) Безопасное хранение и передача номеров платежных карт Контроль доступа и протоколирование событий	Формализация процесса разработки с учетом вопросов ИБ практики безопасного программирования тестирование приложения анализ кода мониторинг уязвимостей платформ и тестирование совместимости с патчами
Возможность встраивания в PCI DSS Compliant инфраструктуру	Руководство по выполнению требований стандарта PCI DSS

Информзащита
Системный интегратор

PA-DSS vs PCI DSS

№	PA DSS	PCI DSS
1	Запрет хранения критичные данные после авторизации (TRACK,CAV2, CID, CVC2, CVV2 или PIN-блок)	3.2
2	Защита данных платежных карт при хранении (PAN)	3.1, 3.3, 3.4, 3.5, 3.6
3	Безопасные механизмы аутентификации	8.1,8.2, 8.4, 8.5.8–8.5.15
4	Протоколирование событий	10.1, 10.2, 10.3
5	Разработка защищенных платежных приложений	6.3, 6.4, 6.5, 2.2.2
6	Защита беспроводного обмена данными платежных карт	1.3.8, 2.1.1, 4.1.1
7	Тестирование приложения для устранения уязвимостей	6.2
8	Защита сети	1, 3, 4, 5, 6.6
9	Хранение данных платежных карт во внутренней сети	1.3, 1.3.4
10	Защита удаленного обновления приложения	1, 1.3.9, 12.3.9
11	Защита удаленного доступа к платежному приложению	8.3
12	Шифрование критичного трафика при передаче по открытым каналам	4.1, 4.2
13	Шифрование неконсольного административного доступа	2.3
14	Документация и обучение для клиентов/дилеров/интеграторов	Нет аналогов

“Стандарт PA-DSS: безопасность платежных приложений”

Семинар компании «Информзащита»
г. Москва, 25 марта 2010 г., Holiday Inn Suschevsky

ВОПРОСЫ ?

Гольдштейн Анна
Заместитель директора департамента аудита

- (495) 980 23 45
- goldanna@infosec.ru

Информзащита
Системный интегратор