PCI DSS: Scope, банкоматы, мерчанты

Алексей Бочкарев,
Департамент консалтинга и аудита
ЗАО НИП «Информзащита»

Область оценки

- 1.1.2 Схемы сети
- 1.1.3 Схемы потоков данных карт
- 2.4 Перечень системных компонентов, попадающих под требования стандарта
- 3.1 Перечень мест хранения данных карт
- 9.9 Перечень устройств захвата данных
- Регулярная актуализация области оценки

Информзащита
Системный интегратор

Зачем это нужно?

PCI DSS в текущем виде – перечень контролей

- Знаем что защищать (scope)
- Знаем как защищать (требования 1-12)

=>

- Выполняем требования
- Не забываем актуализировать знания о scope и требованиях (новые версии стандарта) – BAU подход – один из основных тезисов PCI DSS 3.0

Информзащита
Системный интегратор

Важность актуализации

- Бизнес постоянно развивается
- Новый процесс – новые границы scope
- Отсутствие процессов, направленных на описание области оценки – риски для последующих сертификаций
- Процессный подход позволяет нашим клиентам уже сейчас выполнять новые требования 1.1.3 и 2.4

Информзащита
Системный интегратор

Терминальные устройства

- Банкоматы,POS-терминалы, инфоматы – все привносят дополнительные риски, связанные с обработкой данных карт
- АТМ – такой же системный компонент, как сервер, рабочая станция, сетевое устройство
- Дополнительная мотивация - требования ЦБ – 382-П, 34-Т

Информзащита
Системный интегратор

ATM – системный компонент с точки зрения PCI DSS

```
C:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:990            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1039           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1433           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1503           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1720           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2492           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5022           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8083           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8093           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1074         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1180         127.0.0.1:1181         ESTABLISHED
  TCP    127.0.0.1:1181         127.0.0.1:1180         ESTABLISHED
  TCP    127.0.0.1:1198         127.0.0.1:1199         ESTABLISHED
  TCP    127.0.0.1:1199         127.0.0.1:1198         ESTABLISHED
  TCP    127.0.0.1:1434         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:3792         127.0.0.1:8093         TIME_WAIT
  TCP    127.0.0.1:3799         127.0.0.1:8093         ESTABLISHED
  TCP    127.0.0.1:5679         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:7438         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:8093         127.0.0.1:3799         ESTABLISHED
  TCP    127.0.0.1:9080         0.0.0.0:0              LISTENING
```

Информзащита
Системный интегратор

VISA BULLETIN

31 March 2011

Issuers' Payment Card Industry Data Security Standard Frequently Asked Questions

6. Are an issuing bank's ATMs within the scope of the PCI DSS?

Yes. The PCI SSC states that the PCI DSS applies to any entity that stores, processes or transmits cardholder data. The ATM's network and the physical environment in which it resides must also comply with the PCI DSS.

9. For Visa PCI DSS compliance validation requirements, are issuing banks that acquire ATM transactions (i.e., cash disbursements only) considered to be merchants*?

In accordance with Visa-defined merchant PCI DSS compliance validation levels, a bank that acquires ATM transactions (i.e., cash disbursements only) **is not** considered to be a merchant. However, a bank offering product sales (e.g., postage stamps) via an ATM **is** considered to be a merchant, and all such transactions acquired by all participating ATMs must be aggregated to determine the merchant level and any validation requirements.

Banks identified as a Level 4 merchant based on the aggregate total of annual product sales transactions may decide at their own discretion to validate PCI DSS compliance.

* A "merchant" is any business entity that accepts Visa payment cards as a form of payment for goods or services rendered.

Риски

- Использование устаревших ОС
  - Windows XP
  - до сих пор встречаются АТМ с OS/2
- Передача функций по управлению сторонним организациям
  - поставщики услуг должны выполнять применимые требования PCI DSS
- Сетевое оборудование для подключения АТМ
- Вопросы по обеспечению физической безопасности

Информзащита
Системный интегратор

Решения

- Осознанное включение сети АТМ в область оценки
- Работа с вендорами и поставщиками услуг
  - переход на актуальные версии ОС, ПО
  - требования по безопасности в договорах
  - стандарты конфигурирования
  - стандартные схемы подключения к ПЦ
  - управление изменениями
  - использование специализированных СЗИ

Информзащита
Системный интегратор

POS-терминалы

- Эксплуатируются мерчантами
- Как и ATM, зачастую отдаются на откуп поставщикам услуг
- Отсутствие контроля за сетью POS’ов – все это может привести к неконтролируемому хранению данных карт и рискам их компрометации

Соответствие мерчанта требованиям PCI DSS – головная боль эквайера

Информзащита
Системный интегратор

Ответственность эквайера

- Программы безопасности AIS, SDP говорят:
  - эквайер несет ответственность за компрометации карт, произошедшие по вине своих мерчантов
  - должен регулярно отчитываться перед МПС о статусе соответствия своих мерчантов
  - должен контролировать соответствие сервис-провайдеров, которых используют мерчанты

Информзащита
Системный интегратор

Управление соответствием

- Эквайер определяет требования по подтверждению соответствия
- Эквайер влияет на способ приема карт к оплате – использование «правильных» способов значительно снижает риски
- Работа с поставщиками услуг – оценка рисков, договорные обязательства
- Обучение сотрудников ТСП

Информзащита
Системный интегратор

Соответствие – это процесс

- PCI DSS – это базовые правила, позволяющие повсеместно повысить защищенность процессов обработки карт
- Использование BAU подхода позволяет выполнять правила своевременно
- Защита терминальных сетей – несправедливо «забытый» аспект соответствия
- Организация взаимодействия всех вовлеченных в процесс обработки сторон - важный шаг в определении зон ответственности и снижении рисков компрометации

Информзащита
Системный интегратор

Спасибо за внимание!

Ваши вопросы?

Алексей Бочкарев, CISA, PCI QSA
a.bochkarev@infosec.ru
http://infosec.ru

Информзащита
Системный интегратор