PCI DSS: Scope, банкоматы, управление соответствием мерчантов

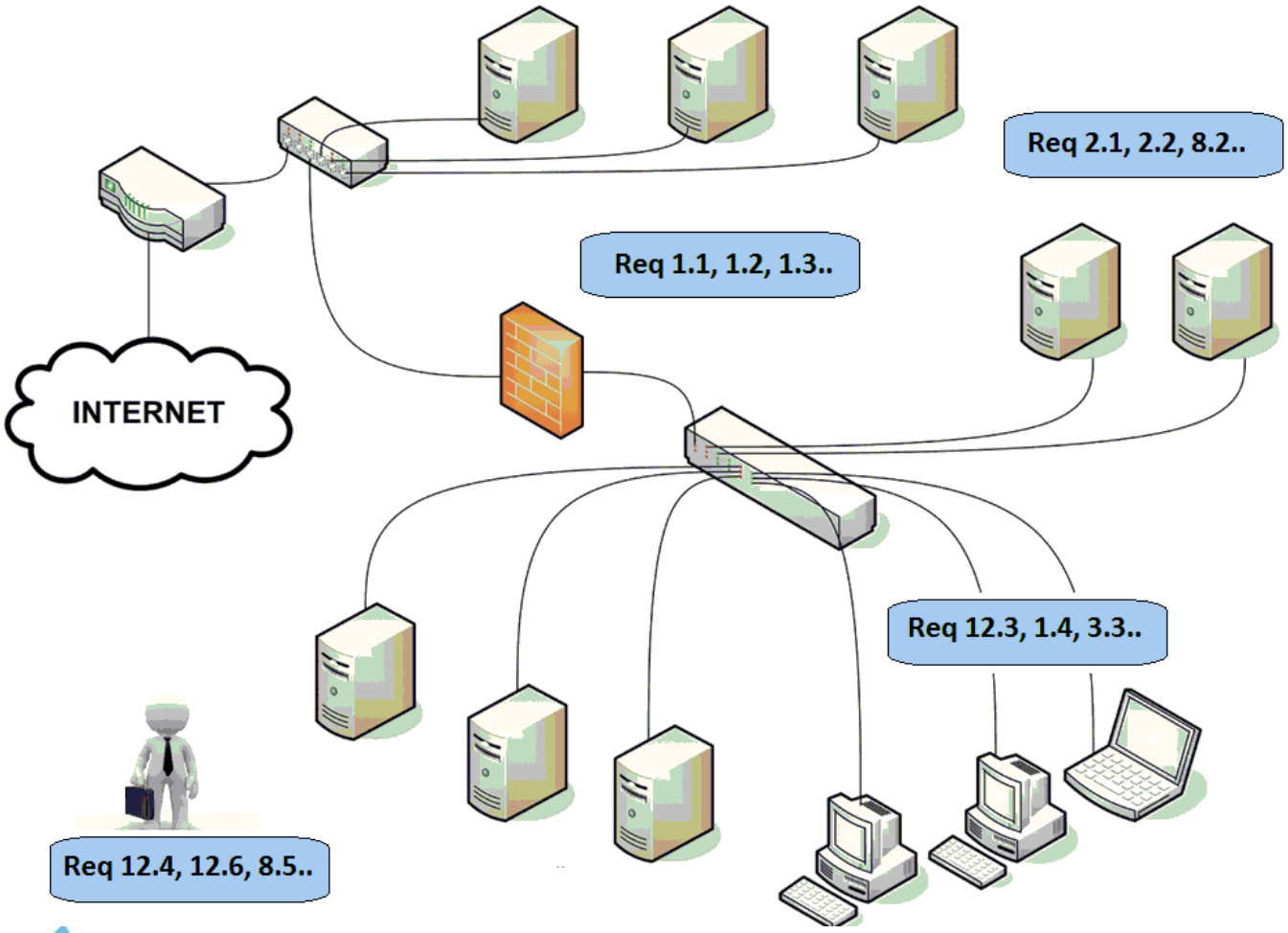
Алексей Бочкарев,
Департамент консалтинга и аудита
ЗАО НИП «Информзащита»

Определение области оценки

- Первый шаг в достижении соответствия
- Снижение рисков «потерять» часть системных компонентов
- Понятнее процесс выполнения требований

Информзащита
Системный интегратор

Знаем scope + знаем требования = эффективнее соответствуем стандарту



Информзащита
Системный интегратор

Ответственность QSA

- QSA на аудите: подтверждение корректности определения предоставленной области оценки
- QSA консультант:
  - ✓ Критерии отнесения систем к области оценки
  - ✓ Выявление и описание процессов обработки данных
  - ✓ Построение процесса документирования scope

Информзащита
Системный интегратор

Документирование

- Идентифицируем процессы обработки
- Идентифицируем задействованные ресурсы (информационные, персонал)
- Определяем формат документирования
  - схемы потоков, перечень системных компонентов
- Фиксируем на «бумаге»
- Любые изменения – контроль влияния и актуализация scope

Информзащита
Системный интегратор

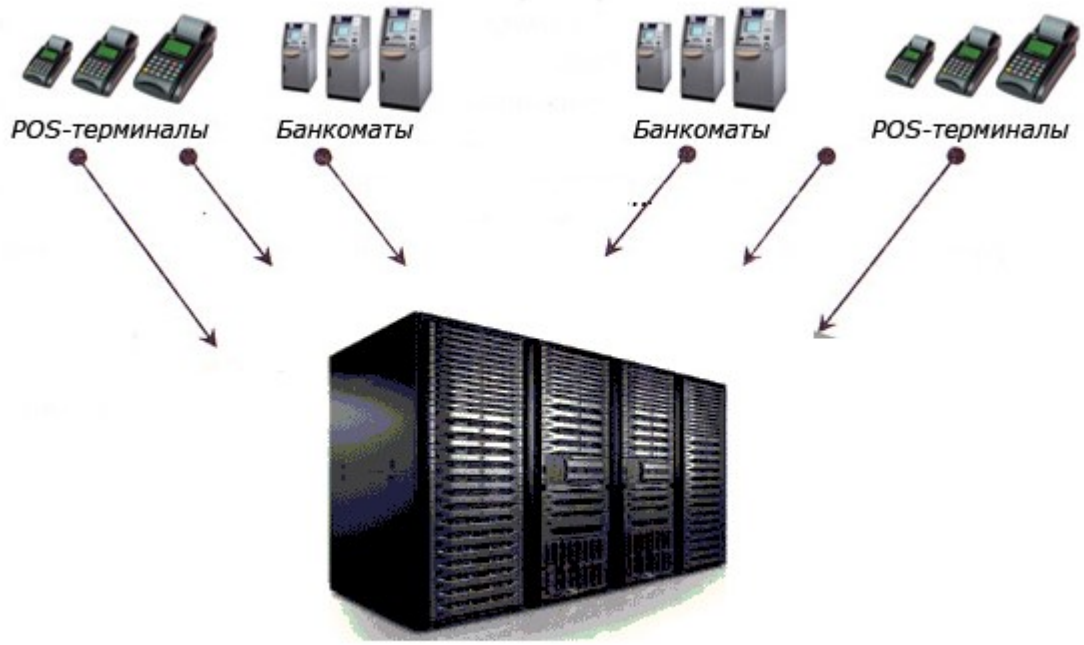
Важность актуализации

- Бизнес постоянно развивается
- Новый процесс – новые границы scope
- Отсутствие процессов, направленных на актуализацию 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

- **Являются системными компонентами , как и сервер, рабочая станция, сетевое оборудование, со своими специфичными угрозами**



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.

Угрозы

- Использование устаревших ОС
  - Windows XP
  - до сих пор встречаются ATM с OS/2
- Передача функций по управлению сторонним организациям
  - выполняют ли поставщики услуг применимые требования PCI DSS?
- Сетевое оборудование для подключения ATM
- Угрозы физического характера – кража, скимминг..

Информзащита
Системный интегратор

Решения

- Осознанное включение сети АТМ в область оценки
- Переход на актуальные версии ОС, ПО
- Стандарты конфигурирования
- Использование специализированных СЗИ
- Стандартные схемы подключения к ПЦ
- Требования по безопасности в договорах
- Управление изменениями

Информзащита
Системный интегратор

POS-терминалы

- Эксплуатируются торгово-сервисными предприятиями
- Как и АТМ, зачастую обслуживаются поставщиками услуг
- Отсутствие контроля за сетью POS-терминалов 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, используемых мерчантами

Информзащита
Системный интегратор

Управление соответствием

- Эквайер определяет требования по безопасности для магазинов
  - ✓ оценка рисков при подключении новых магазинов
  - ✓ приоритетный подход для ТСП
  - ✓ прогноз роста и своевременные требования по изменению способов подтверждения соответствия

Информзащита
Системный интегратор

Управление соответствием

- Эквайер влияет на процесс приема карт к оплате – использование «правильных» способов значительно снижает риски
  - ✓ Внедрение SDLC при разработке своего ПО
  - ✓ Использование PA-DSS, P2PE сертифицированного покупного ПО
  - ✓ Использование PTS сертифицированных терминалов
  - ✓ Использование p2p шифрования

Информзащита
Системный интегратор

Управление соответствием

- Работа с поставщиками услуг
  - ✓ оценка рисков при подключении
  - ✓ выявлений требований PCI в зоне ответственности поставщиков, включение требований в договорные обязательства, контроль выполнения
- Обучение сотрудников ТСП

Информзащита
Системный интегратор

Спасибо за внимание!

Ваши вопросы?

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

Информзащита
Системный интегратор