Оценка защищенности сети и приложений в соответствии с PCI DSS

Тарас Иващенко
Специалист отдела общего аудита
Департамента Аудита,
Компания «Информзащита»
OSCP

PCI DSS – что это?

- Стандарт безопасности данных индустрии платежных карт (PCI DSS) разработан в целях повсеместного обеспечения и улучшения защиты данных платежных карт и принятия соответствующих мер по обеспечению безопасности данных
- 12 требований: от конфигурации МСЭ и политики безопасности до регламентирования физического доступа
- Требования распространяются на все компании, работающие с данными платёжных карт

Оценка защищенности сети

- Внешнее сканирование уязвимостей
- Внутреннее сканирование уязвимостей
- Комплексный тест на проникновение

Оценка защищенности приложений

- Анализ кода веб-приложений
- Тестирование общедоступных веб-приложений / WAF
- Анализ кода самостоятельно разработанного ПО

PCI DSS о сканированиях уязвимостей

«...11.2 Внутренние и внешние сканирования уязвимостей сети должны проводиться по крайней мере ежеквартально или после любого значительного изменения в инфраструктуре сети (например, при установке новых системных компонентов, изменениях в сетевой топологии, модификации правил межсетевого экранирования или обновлении версий продуктов)

Примечание. Ежеквартальное внешнее сканирование уязвимостей сети должно выполняться организацией, имеющей статус ASV (Approved Scanning Vendor), квалификация которой подтверждена Payment Card Industry Security Standarts Council (PCI SSC). Сканирования, проводимые после внесения изменений в сеть, могут выполняться внутренним персоналом компании...”

Кто и как может проводить сканирование уязвимостей?

- Перечень ASV - www.pcisecuritystandards.org
- Сканирование регламентируется документами PCI Security Standards Council (SSC):
  - PCI DSS Security Scanning Procedures
    - цель и границы сканирования
    - критерии оценки соответствия
  - PCI DSS Technical and Operational Requirements for Approved Scanning Vendors
    - общие требования к проведению сканирования
    - требования к отчетности и техническим решения для сканирования

Границы проведения внешнего сканирования

- Сканирование производится через Internet
- Сканированию подлежат все публичные IP адреса компании:
  - системы и сервисы, участвующие в обработке данных платежных карт
  - системы и сервисы, компрометация которых может повысить риск компрометации данных платежных карт (DNS, Email)
- Исключение: адекватная физическая или логическая сегментация сети

Распределение ответственности

ASV

- Сканирование уязвимости в соответствии с процедурой и без нанесения ущерба работе сети (- не нарушать работоспособность сервисов, не эксплуатировать уязвимости, не использовать перебор паролей, не перегружать каналы связи)
- Категорирование найденных уязвимостей и определение степени соответствия стандарту PCI
- Рекомендации по устранению найденных уязвимостей

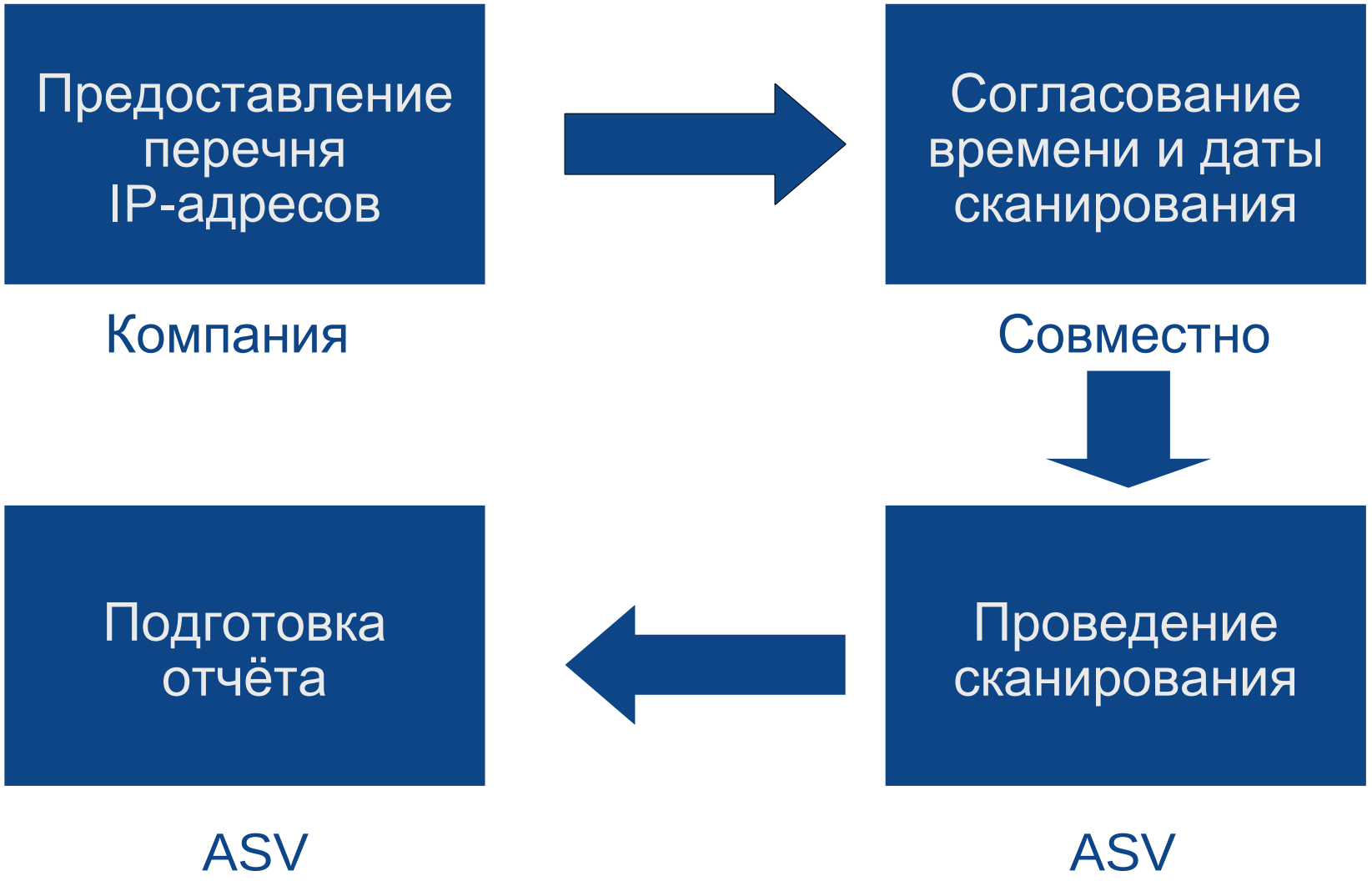
Сканируемая компания

- определение перечня IP адресов для сканирования
- проведение ежеквартального сканирования у компании со статусом ASV
- предоставление доказательства отсутствия уязвимости в случае ложных обнаружений
- исправление найденных уязвимостей и заказ дополнительных сканирований для подтверждения их устранения

Критерии соответствия PCI

- IP адрес соответствует требованиям PCI, если при его сканировании не обнаружено ни одной уязвимости с CVSS ≥ 4 или уровня High, Critical или Urgent
- Особые уязвимости
- Компания соответствует требованиям PCI, если все сканируемые IP адреса соответствуют требованиям PCI

Порядок проведения работ



PCI DSS о тестах на проникновение

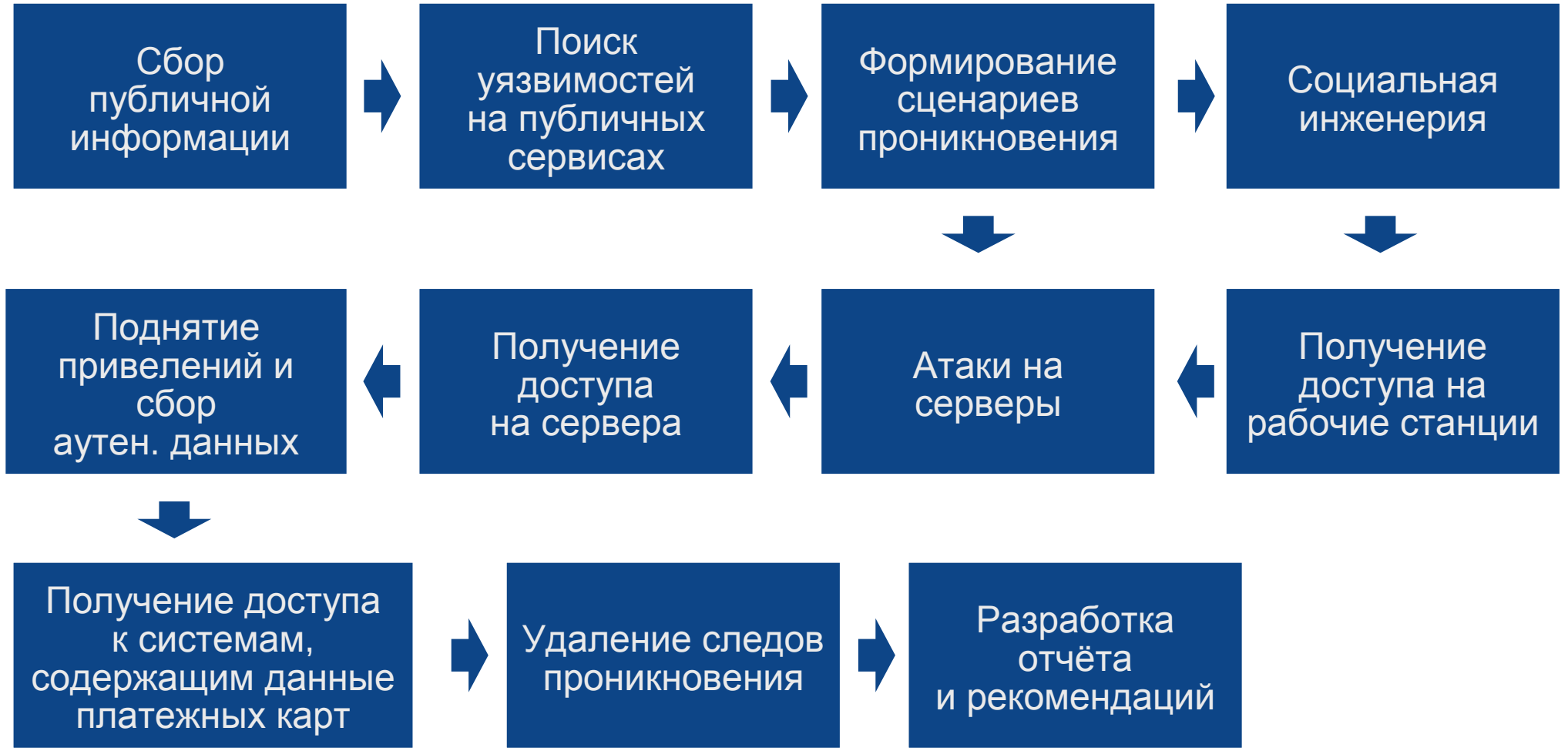
“...11.3 По крайней мере ежегодно, а также после любых значительных модернизаций или модификаций инфраструктуры или приложений (например, обновление версии ОС, добавление подсети или веб-сервера) должны проводиться внешние и внутренние тесты на проникновение...”

- Information Supplement: Requirement 11.3 Penetration Testing
- Данные тесты на проникновение должны включать тесты на проникновение на сетевом уровне, так и на уровне приложений

Ключевые особенности

- Цель – получение данных платежных карт и/или управления системами, где обрабатываются, передаются или хранятся данные
- Атаки проводятся из сети Internet и изнутри локальной сети
- Эксплуатируются как технические уязвимости так и методы социальной инженерии
- Не производятся атаки типа «отказ в обслуживании»
- Используются только публичные уязвимости
- Тестирование методом “белого ящика” (от англ. “white-box”)

Внешний тест на проникновение



Внутренний тест на проникновение

Содержание отчёта

- Описание методики проведения работ
- Перечень выявленных уязвимостей и рисков
- Рекомендации по снижению рисков
- Описание хода работ
- Перечень всей полученной в ходе теста информации

PCI DSS об анализе кода веб-приложений

"...6.5 Все веб-приложения (внутренние и внешние, включая доступ к приложению с правом администратора) должны разрабатываться с учётом рекомендаций по защищённому программированию веб-приложений, например, рекомендаций Open Web Application Security Project Guide (OWASP). С целью идентификации уязвимостей, связанных с ошибками программирования, должен выполняться анализ кода разработанных приложений, позволяющий предотвратить следующие распространенные уязвимости:

Примечание. Уязвимости, перечисленные в пунктах с 6.5.1 по 6.5.10, уже были описаны в руководстве OWASP, когда была опубликована версия стандарта PCI DSS 1.2. Однако при обновлении руководства сообщества OWASP необходимо обеспечить соответствие с требованиями текущей версии стандарта PCI DSS..."

Уязвимости веб-приложений

- 6.5.1 Межсайтовое выполнение сценариев (XSS)
- 6.5.2 Инъекции, в частности SQL-инъекции. Также следует принять во внимание LDAP- и Xpath-инъекции, как и другие угрозы внедрения кода
- 6.5.3 Выполнение вредоносного кода
- 6.5.4 Небезопасные прямые ссылки на объекты
- 6.5.5 Подделка межсайтового запроса
- 6.5.6 Утечка информации и неправильная обработка ошибок
- 6.5.7 Уязвимости подсистемы аутентификации и управления сеансами
- 6.5.8 Уязвимости, связанные с хранением криптографических материалов
- 6.5.9 Небезопасные коммуникации
- 6.5.10 Невозможность ограничения доступа пользователей к URL-адресам

PCI DSS о сканировании веб-приложений

“...6.6 Необходимо постоянно работать над нейтрализацией новых угроз и устранением новых уязвимостей в общедоступных веб-приложениях, которые также должны защищаться от известных атак с помощью одного из приведенных ниже методов:

Анализ веб-приложений с помощью ручных или автоматизированных средств или методов оценки защиты приложений от уязвимостей не реже чем 1 раз в год или после внесения в них любых изменений

Установка межсетевого экрана для защиты общедоступных веб-приложений ...”

PCI DSS об анализе кода самостоятельно разработанного ПО

“...6.3.7 Для идентификации потенциальных уязвимостей в разработанном программном обеспечении должен выполняться анализ кода перед запуском этого ПО в эксплуатацию или его передачей заказчику

Примечание. Требование анализа кода должно применяться ко всем типам кодов (как к внутренним, так и к общедоступным) на всех стадиях процесса разработки системы в соответствии с требованием 6.3. Анализ кода может выполняться как квалифицированными сотрудниками компании, так и третьими сторонами. Если веб-приложения являются общедоступными, то к ним также должны применяться дополнительные меры защиты для устранения угроз безопасности и уязвимостей после их реализации в соответствии с требованием 6.6....”

Вопросы?