POSITIVE TECHNOLOGIES

POSITIVE TECHNOLOGIES

Практические аспекты оценки защищенности государственных информационных систем

Дмитрий Кузнецов

Заместитель технического директора

Positive Technologies

ТБ Форум 2014

Эволюция нормативных требований

— Приказ ФСТЭК №58 (2010 г.)

5. Анализ защищенности проводится для распределенных информационных систем и информационных систем, подключенных к сетям международного информационного обмена, путем использования в составе информационной системы программных или программно-аппаратных средств (систем) анализа защищенности.

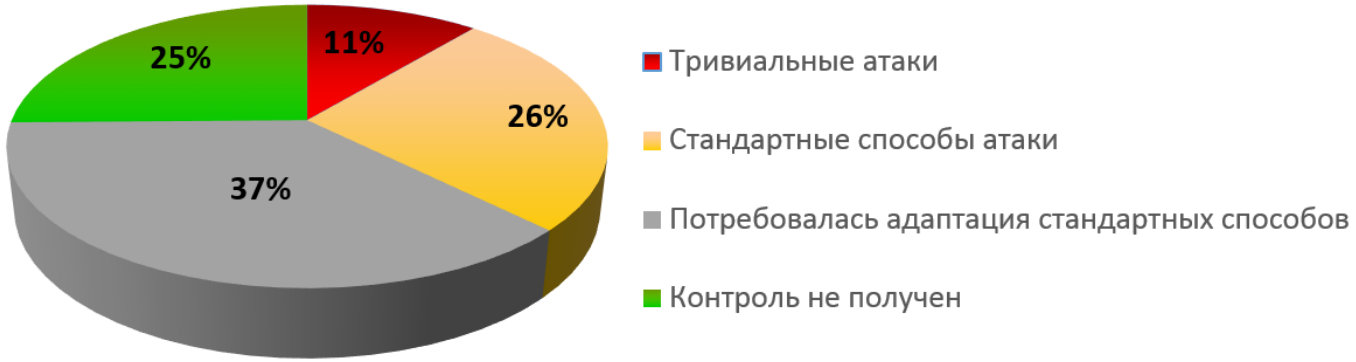
— Приказ ФСТЭК №17 (2013 г.)

АН3.1	Выявление, анализ уязвимостей		+	+	+
АН3.2	Контроль установки обновлений	+	+	+	+
АН3.3	Контроль работоспособности, параметров настройки и правильности функционирования		+	+	+
АН3.4	Контроль состава ТС, ПО и СЗИ		+	+	+
АН3.5	Контроль паролей, учетных записей, разграничения доступа		+	+	+

“Умножающий знание умножает скорбь”

— 75% тестов на проникновение заканчиваются получением полного контроля над ИС

— И это несложно



Методическая база оценки защищенности

— Проекты государственных стандартов
  - ГОСТ Р «Уязвимости ИС. Классификация уязвимостей информационных систем»
  - ГОСТ Р «Уязвимости ИС. Правила описания уязвимостей»
  - ГОСТ Р «Уязвимости ИС. Содержание и порядок выполнения работ по выявлению и оценке уязвимостей»

— Проекты отраслевых стандартов
  - Рекомендации по стандартизации Банка России «Требования к обеспечению информационной безопасности на стадиях жизненного цикла банковских приложений»

(Само)оценка защищенности на практике

— Выявление и устранение известных уязвимостей
— Выявление ошибок конфигурации
— Выявление недостатков архитектуры
— Контроль исходного и объектного кода
— Тестирование на проникновение
— *Реагирование на сообщения хакеров*

Выявление известных уязвимостей

— Выявляются уязвимости ПО

— Унифицированные базы уязвимостей

- Источники наполнения: независимые исследователи, разработчики ПО, антивирусные лаборатории

— Автоматизированная оценка

- Около десятка сканеров, в том числе сертифицированные
- Альтернативы
  - Установка последних версий ПО и обновлений безопасности
  - Отслеживание публикаций CERT и специализированных порталов (Securitylab.Ru, Securityfocus.com и т.п.)

Выявление ошибок конфигурации

— Выявляются особенности настройки СЗИ, при которых не в полном объеме выполняются их функции

— В идеале оценка заключается в сравнении фактических значений параметров конфигурации с рабочей документацией

  - Альтернатива – руководства по безопасной настройке

— Автоматизированная и экспертная оценка

Выявление недостатков архитектуры

— **Примеры:**
  - **АРМ администраторов и пользователей в одном VLAN**
  - **Отсутствие CAPTCHA в форме ввода имени и пароля пользователя**
  - **Передача идентификатора сессии в URL HTTP**
— **Экспертная оценка**
  - **Анализ документации**
  - **Проблема квалификации эксперта**

Контроль исходного и объектного кода

— Комплекс мер
  - Контроль отсутствия НДВ в исходных текстах
  - Восстановление исходного кода по объектному, деобфускация, обход защиты от отладки и эмуляции
  - Поиск характерных ошибок в объектном коде

— Экспертная оценка
  - Эффективность варьируется в зависимости от языков программирования
  - Основной метод анализа мобильных приложений
  - Проблема квалификации эксперта

Тестирование на проникновение

— Поиск и практическая демонстрация уязвимостей
  - Поиск уязвимостей, к которым известны эксплойты
  - Поиск «вслепую» типовых ошибок архитектуры ИС и настройки ее компонентов
  - Анализ реакции пользователей на социальную инженерию
  - Анализ реагирования на факт атаки
— Экспертная оценка
  - Частично формализуемая оценка
  - Проблема квалификации эксперта
  - Потенциальная опасность выполняемых проверок

Резюме

— Ожидаемый результат оценки не уязвимости, а подтвержденное устранение ранее найденных уязвимостей

— Наиболее часто используемые виды оценки автоматизируемы

- Поиск известных уязвимостей и ошибок конфигурации может производиться самостоятельно
- Прочие виды оценки проводятся однократно при приемке системы после разработки или модернизации

Спасибо за внимание

Дмитрий Кузнецов

Зам. технического директора

DKuznetsov@ptsecurity.ru

POSITIVE TECHNOLOGIES