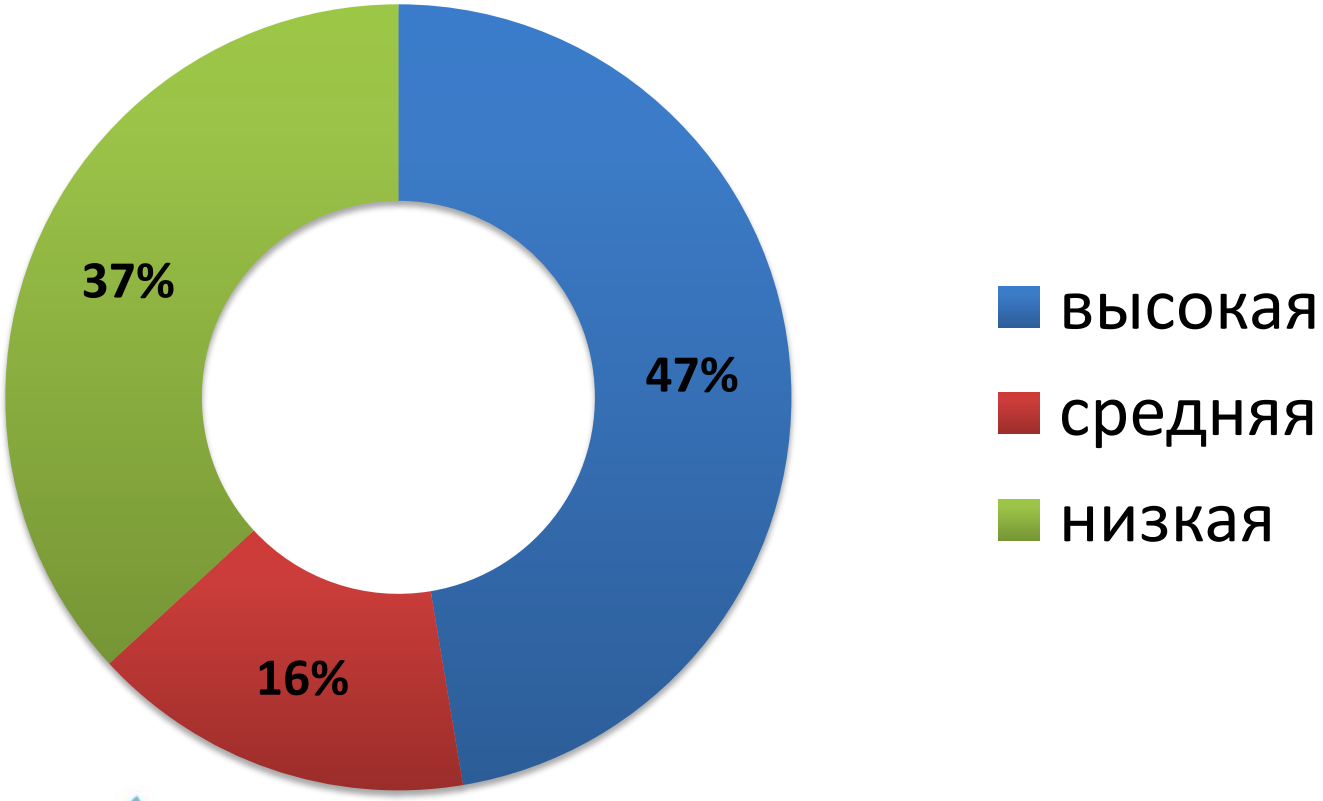
Контроль за разработкой ПО со стороны ИБ

Леонид Плетнев
PCI QSA, CISM, CISA

Статистика проектов ИНФОРМЗАЩИТЫ по анализу кода за 2013-2014 годы

Выявленные уязвимости



Информзащита
Системный интегратор

Три причины разработки уязвимого ПО

1. В организации **не могут** ПРАВИЛЬНО разрабатывать безопасное ПО

2. В организации **не хотят** ПРАВИЛЬНО разрабатывать безопасное ПО

- Пример из практики:

пароль XOR фрагмент текста ->

пароля в открытом виде нет, но вычислить его можно

Информзащита
Системный интегратор

Три причины разработки уязвимого ПО

3. В организации **не знают** как ПРАВИЛЬНО разрабатывать безопасное ПО

- Пример из практики:

Неверный режим шифрования 3DES привел к тому, что сообщения с одинаковыми 16 байтами в конце подписывались одинаково.

Информзащита
Системный интегратор

ПРАВИЛЬНО значит по правилам

- Принципы SDLC давно всем известны
- Отличия в SDLC-походах не значительны

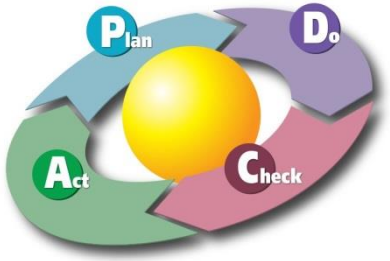
PCI DSS Development Lifecycle	Cisco Secure Development Lifecycle	Microsoft Security Development Lifecycle
Обучение	Secure Design	Training
Выявление уязвимостей	3rd Party Security	Implementation (частично)
Проектирование	Product Security Requirements	Requirements
Оценка рисков	Secure Design	Design
Создание	Secure Coding	Implementation
Анализ кода	Secure Analysis	Implementation
Тестирование безопасности	Vulnerability Testing	Verification, Release
Выпуск	-	Release
Поддержка	-	Response

Информзащита
Системный интегратор

Чтобы правила работали нужен ПРОЦЕСС

- Найти уязвимость, баг в ПО – частный случай

- Главные задачи для ИБ – **внедрение и контроль процессного подхода** разработки ПО



Информзащита
Системный интегратор

Нормативные акты

- PCI DSS,
- СТОБР-2014,
- НПС,
- Рекомендации ЦБ РФ Обеспечение ИБ на стадиях жизненного цикла АБС

Информзащита
Системный интегратор

Самые распространенные ошибки

- Добавили требование в договор и провели тестирование, как правило только функциональное
- Отсутствие разделения контрольной среды и среды разработки
- Сложные -> плохо работающие контроли

Информзащита
Системный интегратор

Принципы эффективного контроля

- Контроль не дороже возможного ущерба
- Действительно необходимо
- Мотивация
- Простота
- Несколько уровней

Информзащита
Системный интегратор

Рекомендации Компании ИНФОРМЗАЩИТА

1

- Подготовка договора и ТЗ с участием ИБ, только согласования мало
- Избегать общих фраз, требования по ИБ должны быть конкретными, по возможности, параметризованными
- Привлекать внутреннюю и внешнюю экспертизу при подготовке ТЗ

Информзащита
Системный интегратор

Рекомендации Компании ИНФОРМЗАЩИТА

2

- Внедрение SDLC
  - обучение,
  - учет требований ИБ,
  - анализ кода,
  - тестирование безопасности и т.п.
- Интеграция SDLC с другими процессами:
  - Управление изменениями;
  - Сбор и анализ событий;
  - Внутренние контроли и т.п.

Информзащита
Системный интегратор

Рекомендации Компании ИНФОРМЗАЩИТА

3

- В рамках SDLC служба ИБ должна получать реальные свидетельства выполнения процесса разработки ПО
- Актов тестирования с общими словами недостаточно

Информзащита
Системный интегратор

Рекомендации Компании ИНФОРМЗАЩИТА

4

- Тестирование на отсутствие негативного влияния изменения силами ИБ / СВК
- Независимый анализ небольших фрагментов кода
- Автоматизированный анализ – только инструмент
- Привлечение внешней экспертизы
- В случае выявления багов, анализ эффективности процесса безопасной разработки ПО

Информзащита
Системный интегратор

ПРОЦЕСС безопасной разработки ПО

Информзащита
Системный интегратор

ВОПРОСЫ?

Леонид Плетнев
PCI QSA, CISM, CISA

l.pletnev@infosec.ru
+ 7 (495) 980-23-45 #855
+ 7 926 411-41-00

www.infosec.ru

Информзащита
Системный интегратор

Об экспертизе Компании ИНФОРМЗАЩИТА

- Разработка Моделей угроз и Моделей нарушителя для приложений;
- Анализ кода;
- Анализ безопасности конфигураций приложений;
- Ручной и автоматизированный поиск уязвимостей;
- Тесты на проникновение для приложений;
- Консалтинг по построению контрольной среды.

Информзащита
Системный интегратор

Полезные ссылки

- Безопасное программирование
  - http://cwe.mitre.org
  - http://owasp.org
- Общие базы данных уязвимостей
  - http://www.securityfocus.com
  - http://nvd.nist.gov
  - http://secunia.com
- Информация по внешнему обучению
  - http://itsecurity.ru/catalog/kp75
  - http://www.sans.org/security-training.php
  - https://www.owasp.org/index.php/Category:OWASP_AppSec_Conference
  - http://www.giac.org/certification/gssp-java
- Материалы для организации внутреннего обучения:
  - https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project
  - https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
  - http://www.sans.org/top25-software-errors
  - http://projects.webappsec.org/w/page/13246978/Threat-Classification
  - http://www.cert.org/secure-coding
  - http://cwe.mitre.org/data/graphs/699.html
- Материалы с сайта консула:
  - https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_eCommerce_Guidelines.pdf
  - https://www.pcisecuritystandards.org/documents/information_supplement_6.6.pdf
  - https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Developers_v1.pdf