IDC Security Roadshow Moscow 2014

12 марта 2014, «Холидей Инн Сокольники»

Информзащита

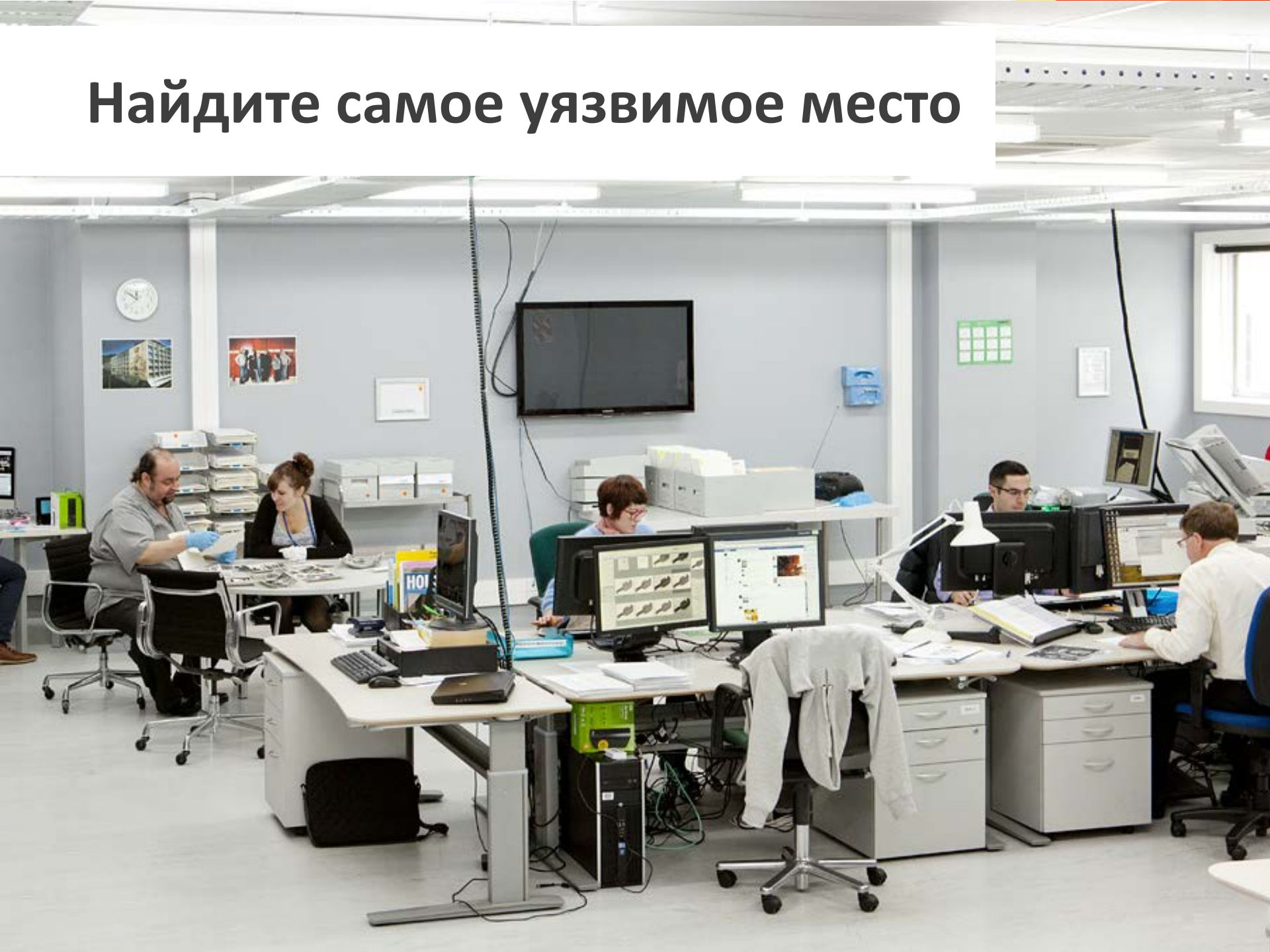
Системный интегратор

Социальная инженерия – козырь в руке злоумышленника

Алексей Бабенко

руководитель направления, PA&PCI QSA

Найдите самое уязвимое место



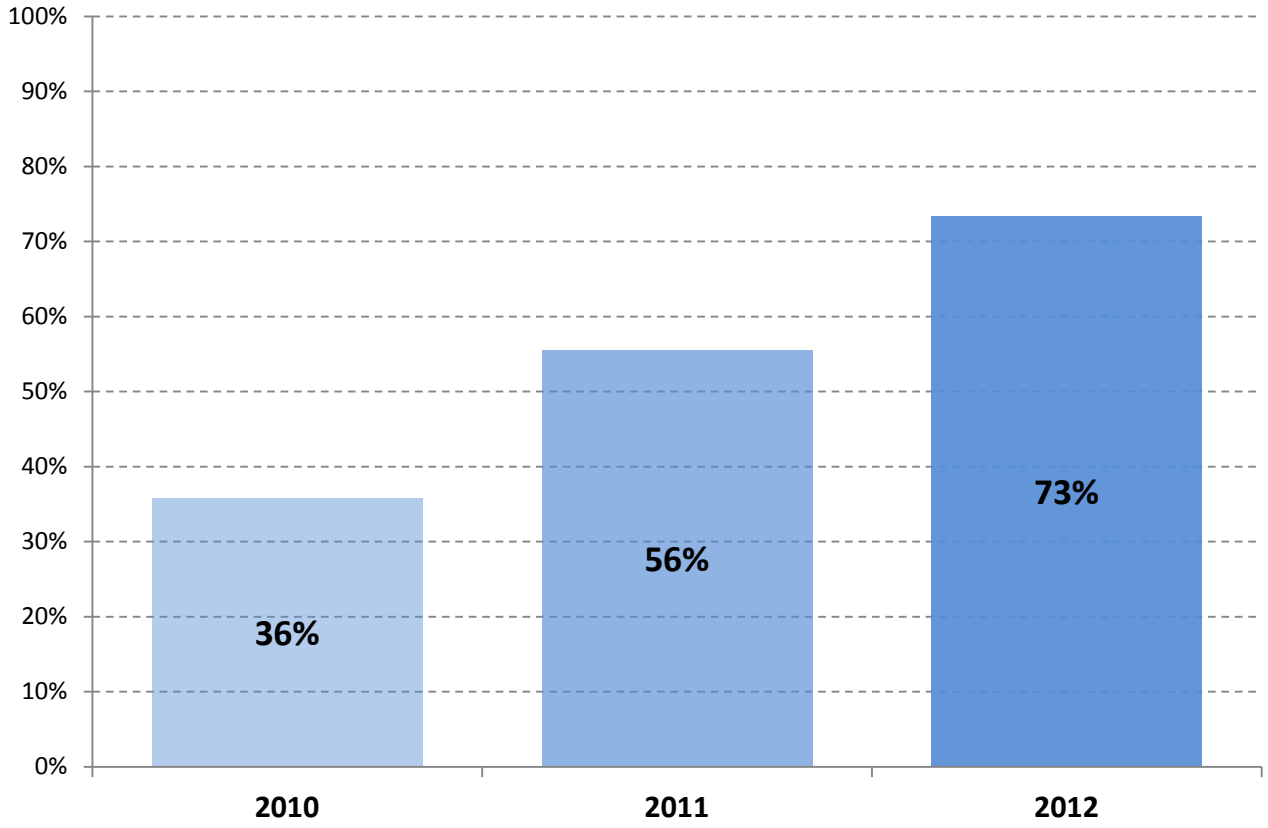
Социальная инженерия

- Слабое звено – человек
- Социальная инженерия – метод несанкционированного доступа к информации/ системам хранения информации основанный на использовании слабостей человеческого фактора
- Социальная инженерия = обман

Информзащита
Системный интегратор

Статистика Информзащиты

Успешность проведение атак методом социальной инженерии



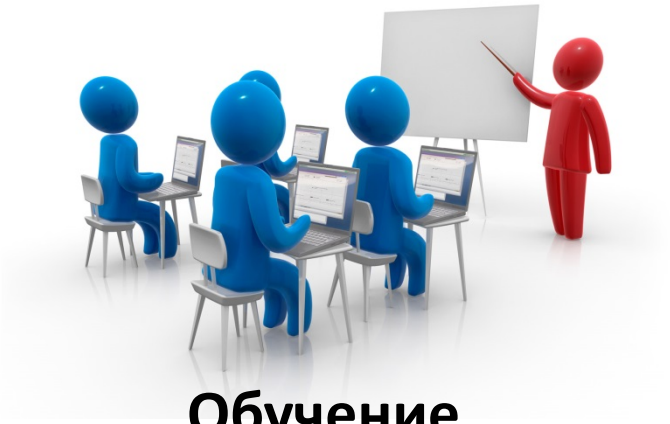
Информзащита
Системный интегратор

Как это происходит?

- **Социальные сети** – копирование друга
- **Почтовая рассылка** – реиндексация зарплат, web-интерфейс портала, настойчивая просьба
- **Физические носители** – потерянная флешка, посылка начальнику
- **Телефонная сеть** – техническая поддержка, забытый пароль, ограбленный клиент

Информзащита
Системный интегратор

Методы противодействия



Обучение

Отладка процессов

Тестирование

Разбор полетов

Информзащита
Системный интегратор

Повышение осведомлённости

- **Знать** > **уметь** > **выполнять**
- Разные формы обучения:
  - Ознакомление с документацией
  - Рассылки по e-mail
  - Плакаты/ заставки
  - Внутренние семинары
  - Внешнее обучение
- Контроль знаний
- Направленное обучение

Информзащита
Системный интегратор

Повышение осведомлённости

- Говорить на одном языке:
  - НСД с АРМ к КТ запрещено
  - Вычисление закрытого ключа RSA эквивалентно нахождению нетривиального квадратного корня из 1

Информзащита
Системный интегратор

Отладка процессов

- Лишние и нелогичные действия
- Создание процедур в отрыве от исполнителей

Информзащита
Системный интегратор

Встроенное качество

«Покончите с зависимостью от массового контроля: Уничтожайте потребность в массовых проверках и инспекции как способе достижения качества, прежде всего путем «встраивания» качества в продукцию»

(14 ключевых принципов Деминга)

- Встроенное качество – решения, которые делают невозможным (крайне сложными) некорректные действия сотрудников.
- Примеры:

Информзащита
Системный интегратор

Разделение обязанностей

- Снижает риск «человеческого фактора»
- Для намеренного выполнения неправомерного действия требуется сговор
- Деление ответственности (не всегда в пользу)
- Двойной контроль ≠ двойная работа

Информзащита
Системный интегратор

Тестирование и разбор полетов

- «Учебные тревоги»
- Тестирование на проникновение
- Плановое vs внезапное vs непрерывное
- Недостатки это хорошо (когда их нашли раньше злоумышленников)
- Тестирование в стол = крик в вакуум
- По результатам тестирования:
  - Доведение результатов до руководства с вариантами коррекции
  - Разбор полетов с сотрудниками
  - Коррекция внутренних контролей, процессов, программы обучения

Информзащита
Системный интегратор

Сухой остаток

- Любая система может быть взломана
- Системы защиты с каждым годом все совершеннее, сотрудники – неизменны.
- Самое слабое звено – человек, но можно максимально сократить риски:
  - Объяснив сотрудникам, что их могут обмануть и как
  - Внеся корректировки в существующие процессы
  - Проводя периодические тестирования и делая выводы из результатов
  - Лучшая проверка – независимая, максимально приближенная к реальности

Информзащита
Системный интегратор

ВОПРОСЫ?

Алексей Бабенко
руководитель направления, PA&PCI QSA

a.babenko@infosec.ru
+ 7 (495) 980-23-45 #458
+ 7 905 991-99-19

skype: arekusux
arekusux.blogspot.com

www.infosec.ru

Информзащита
Системный интегратор

Полезные ссылки

Социальная инженерия:

- http://www.social-engineer.org

Обучение:

- http://itsecurity.ru

Тестирование на проникновение:

- http://www.isecom.org/research/osstmm.html
- http://www.infosec.ru/katalog/bezopasnost-it-infrastrukturyi/obespechenie-bezopasnosti-setevoy-infrastrukturyi

Встроенное качество:

- http://ru.wikibooks.org/wiki/ТРИЗ
- http://ru.wikipedia.org/wiki/Кайдзен

Информзащита
Системный интегратор