Повышение осведомленности сотрудников Компании в вопросах ИБ

Директор департамента по информационной безопасности
ПАО «ВымпелКом»
Голубев А.В.

г. Магнитогорск, 13-17.02.2017 г.

Билайн

Проблематика

- **80 % инцидентов ИБ связанных с человеческим фактором**
- **Социальная инженерия – один из самых эффективных способов неправомерного доступа!**
- **Неумышленные действия сотрудников:**
  - невнимательность сотрудников к правилам и требованиям обеспечения ИБ или нежелание выполнять требования, принятые в компании;
  - незнание сотрудниками правил и требований обеспечения ИБ в компании;
- **Требования:**
  - СТО БР ИББС
  - PCI DSS
  - другие (ISO, NIST, FISMA, FFIEC, …)

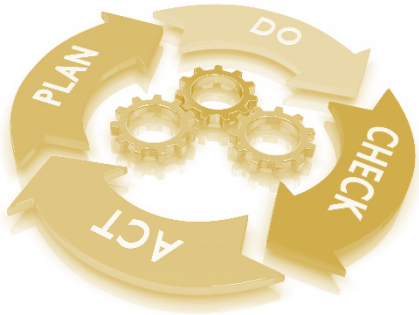
Программа повышения осведомленности в вопросах ИБ

- Под повышением осведомленности в вопросах ИБ обычно понимается обучение сотрудников компании вопросам обеспечения ИБ, повышение осведомленности об актуальных угрозах ИБ, мерах и способах реализации атак и средствах защиты, фокусировка внимания сотрудников на важности обеспечения ИБ и т.п.

Основные шаги при внедрении

- **Все просто:**

еще один процесс в вашей организации (plan-do- check-act)



Основные шаги при внедрении

- **Планирование**
  - Определите ответственных за создание и реализацию программы
  - Определите цели и задачи программы
  - Определите роли (категории вашей целевой аудитории). Разным ролям потребуется разное обучение в разном объеме, например, все сотрудники, ИТ-персонал, менеджмент, внешние исполнители и т.п.
  - Для каждой категории целевой аудитории определите актуальный набор мероприятий (курсы, тренинги, рассылки …)
  - Определите способы взаимодействия с аудиторией (семинары, тренинги, мультимедиа курсы, рассылки, бюллетени безопасности, постеры и т.п.)
  - Определите метрики для анализа эффективности программы
  - Разработайте план реализации программы и план мероприятий по проверке/тестированию знаний

Основные шаги при внедрении

- **Реализация**
  - Разработайте/приобретите материалы для реализации программы
  - Выберите необходимые инструменты для реализации
  - Проводите мероприятия в соответствии с программой
  - Проводите мероприятия по тестированию осведомленности

Основные шаги при внедрении

- **Оценка эффективности**
  - Анализируйте результаты и показатели эффективности
  - Доводите результаты и получайте обратную связь менеджмента компании
  - Получайте обратную связь от аудитории, вовлеченной в обучение (полезность, качество материалов, рекомендуемые изменения и т.п.)

Основные шаги при внедрении

- **Совершенствование**
  - Развивайте свою систему в соответствии с полученными показателями эффективности, результатами тестирования (проверки знаний) и по результатам обратной связи
  - Анализируйте ландшафт угроз и дополняйте свою программу обучения новыми материалами
  - Анализируйте новые требования и вносите изменения в программу обучения
  - Развивайте свою программу с учетом долгосрочных бизнес-целями компании
  - Переходите на проактивный подход в обучении.

Лучшие практики

- Сделайте обучение увлекательным и интересным: используйте геймификацию и интерактивные техники
- Стимулируйте и поощряйте достижение высоких результатов в программе, привлекайте самых успешных к обучению
- Обращайте внимание на применимость полученных навыков и знаний в личной жизни, дома
- Интегрируйтесь с системой корпоративного обучения

Ключевые факторы успеха

- Поддержка руководства компании и руководителей подразделений (HR, юристы, внутренний аудит и др.), а также их вовлечение в программу
- Роли для информирования по вопросам безопасности
- «Базовый» (или минимальный) уровень осведомленности по вопросам безопасности
- Способ доставки материалов и сами материалы должны соответствовать аудитории
- Своевременно обновляйте свою программу и материалы
- Измеряемые и понятные метрики эффективности программы

Как измерить эффективность?

- Измеряемые показатели эффективности (уровень проникновения программы; уровень проникновения для конкретных ролей; количество инцидентов ИБ, обнаруживаемых пользователями; результаты оценки знаний документов, процедур; осведомленность пользователей об угрозах; и т.п.)
- Обратная связь по итогам обучения (Анкетирование, Интервьюирование, фокус-группы).
- Регулярное тестирование осведомленности

Как реализовать?

- В поиске «вдохновения»:
  – СТО БР ИББС
  – PCI Security Standards Council.

  Information Supplement: Best Practices for Implementing a Security Awareness Program

  – COBIT 5

  Detailed Guidance: Services, Infrastructure and Applications Enabler, Security Awareness

  – NIST

  Building an Information Technology Security Awareness and Training Program

  – ENISA

  Raising awareness on information security across public and private organisations.

  The new user's guide: How to raise information security awareness.

Как реализовать?

- Где взять материалы:
  - Вендеры / Учебные центры
  - ENISA

    https://www.enisa.europa.eu/media/multimedia/material
  - CIS

    https://www.cisecurity.org/training/
  - Интеграторы

Как реализовать?

- Как организовать тестирование:
  - На базе корпоративных систем обучения и тестирования
  - На базе учебных центров
  - Специализированные решения (эмуляция атак, phishing’овых рассылок и др.)

Итоги

- Успешная реализация программы превратит «слабое звено» в надежный элемент защиты корпоративных интересов!

Спасибо за внимание