Формирование корпоративной культуры кибербезопасности как способ контроля киберрисков, связанных с персоналом

Игорь Долотин
id@ubs.ru

В чём проблема?

Предпосылки

1. Рост роли ИТ в бизнесе даёт не только новые бизнес-возможности, но и обуславливает рост киберрисков, в т.ч. критичных для бизнеса. → Рост «ассортимента» и вероятности реализации киберрисков.

2. Темп роста вложений в ИБ не покрывает весь ландшафт киберугроз и, кроме того, отстает от темпов роста киберрисков – ИБ-шники всегда в роли догоняющих. → Деньги тратятся на софт и железо, а персонал лишён внимания - не обучается и не развивается.

↓

Очень вероятное следствие

Миллионы потрачены на внедрение программно-технических средств защиты, но банальное открытие недумающим сотрудником фишингового письма с вирусом-шифровальщиком «ставит на колени» и госорганы, и компании.

↓

Утечка конфиденциальной информации, блокирование операционной деятельности, репутационный ущерб. Затраты на устранение последствий могут кратно превосходить стоимость всех внедрённых программно-технических средств защиты.

Что делать?

1. **Ничего**

   • «10 лет работали, всё было нормально – и ещё 10 так же проработаем, зачем сейчас на это деньги тратить?»
   • «Риски преувеличены - сейчас не то время, чтобы тратить деньги ещё и на эти вещи сомнительной эффективности»

Очень вероятное следствие

Миллионы потрачены на внедрение программно-технических средств защиты, но банальное открытие недумающим сотрудником фишингового письма с вирусом-шифровальщиком «ставит на колени» и госорганы, и компании.

2. **Начать работать с персоналом (повышение осведомлённости персонала или security awareness)**

   • «Но ведь работать с людьми - это же такая головная боль!»
   • «Разве эти олдскульные курсы и тесты могут кого-нибудь чему-нибудь научить?»
   • «И кто это будет делать? У нас 2,5 ИБ-шника и все по уши в текучке!»
   • «А это можно сделать самим или обязательно надо консультантов звать?»
   • «Это же, наверно, дорого!?»

Зачем?

Повышение безопасности бизнеса за счёт снижения рисков совершения преднамеренных и/или непреднамеренных действий персоналом, а также бездействия персонала при возникновении предпосылок для инцидентов информационной безопасности.

1. Научить сотрудников «работать в сознании», поднять общий «уровень тревожности» рядового сотрудника.
2. Привить базовые навыки реагирования на ИБ-инциденты на почти рефлекторном уровне – всего 4-5 базовых правил ИБ, «закрывающих» 95% ИБ-инцидентов в организации.

Что?

Решение сложной на практике задачи:

ПРОЧИТАТЬ ⇒ **ПОНЯТЬ** ⇒ **ВЫПОЛНЯТЬ**

Поэтому необходима системная методологически верная и организационно подкрепленная работа с персоналом, направленная на формирование навыков распознавания и правильного своевременного реагирования на ИБ-инциденты.

Как?

1. Кратко, креативно, с выгодой для сотрудника

Отвлечение от созидательного труда должно быть не только полезным, но и развлекать с учётом профессиональной специфики.
А понимание личной выгоды обычно повышает мотивацию работника.

2. «Обложить» со всех сторон

Необходимо использовать все каналы доставки контента: интерактивные тренинги и игры, памятки на столах, ролики и плакаты в местах общего пользования, email-рассылки, дни кибербезопасности.

3. Поголовно

«Танцуют» все: секретари, инженерно-технические работники, менеджеры, высшее руководство.
И особенно высшее руководство!

4. Непрерывно

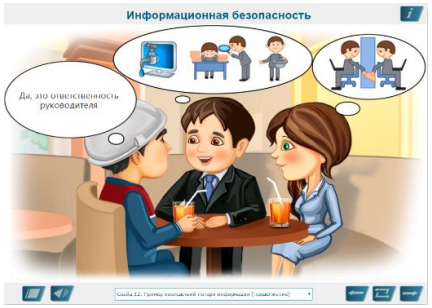
Периодические мероприятия, своевременная актуализация материалов, учёт обратной связи.

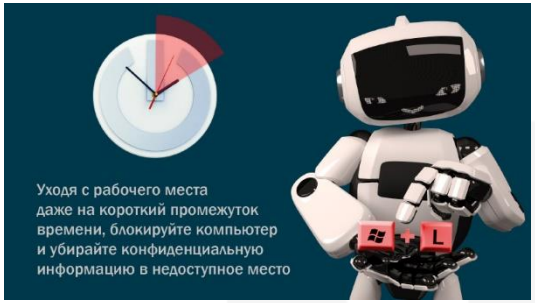
5. При поддержке высшего руководства

Адмінресурс необходим для успеха.

Чем?

1. Интерактивные мультимедийные курсы с тестами, квизами и викторинами
2. Вводные и плановые инструктажи
3. Информационно-обучающие скринсейверы (анимационные и слайдовые)
4. Агитационные плакаты, памятки и прочая печатная продукция
5. Информационно-обучающие видеоролики
6. Компьютерные (в т.ч. браузерные) игры
7. Изображения для сувенирной и канцелярской продукции
8. Рассылки-дайджесты для персонала – одна страничка: новости из мира ИБ, весёлая, но поучительная картинка, статья о правилах ИБ, написанная доступным языком
9. Учебные фишинговые атаки и другие тесты на проникновение методами социнженерии (прозвон с компрометацией, флешки с вредоносным содержимым и др.)
10. Тимбилдинг – корпоративный день кибербезопасности





Все изображения взяты не из открытых источников
(а сделаны в UBS)

С чего начать или примерный план действий

1. Осознать необходимость
2. Определить целевые метрики (что хотим в итоге? как меряем?), кого и как обучаем (делаем сами/не сами? какие методы и средства используем?)
3. Заручиться поддержкой руководства (административная, ресурсная)
4. Разработать процесс повышения осведомлённости: роли, зоны ответственности, ресурсы, целевые показатели и т.д. Замерить начальный уровень осведомлённости персонала
5. Разработать организационно-распорядительной документации и материалов для повышения осведомлённости
6. Реализовать мероприятий по повышению осведомлённости (тренинги, учебные атаки и т.д.)
7. Проводить периодический мониторинг (замер) результатов + оценка эффективности + корректирующие меры

Что в итоге даёт создание корпоративной культуры кибербезопасности (если делать правильно)

1. Значительно снижает вероятность реализации киберрисков, связанных с персоналом
2. Помогает поднять общий средний уровень ЕИ (естественного интеллекта) в работе персонала (а это, в свою очередь, имеет прямое положительное влияние на всю работу организации, и не (с)только в области ИТ/ИБ)