Лаборатория Касперского

Сценарий из области здравоохранения для Kaspersky interactive protection simulation

Контекст / описание проблемы:

У любого, даже самого креативного решения для ИТ-безопасности есть слабое место – его пользователи. Предприятия теряют огромные деньги из-за инцидентов, связанных с человеческим фактором, несмотря на то, что во многих организациях действуют программы повышения осведомленности в области информационной безопасности...

- Почему обучение кибербезопасности терпит неудачу?
- Что нужно изменить, чтобы создать действительно безопасную корпоративную кибер-среду?
- Как сочетать кибербезопасность с эффективностью бизнеса?

В «Лаборатории Касперского» мы считаем, что любая программа обеспечения безопасности должна не просто давать сотрудникам компании общие знания об информационной безопасности, но должна способствовать формированию кибербезопасного поведения сотрудников. Это достигается за счет набора обучающих продуктов, которые включают в себя геймификацию, обучение на практике, симулированные атаки, пути обучения и пр.

Задача:

Разработать и описать сценарий из области здравоохранения для Kaspersky interactive protection simulation. Создать Game board с физической структурой организации (больница / клиника / и др.) и ИТ-инфраструктурой.

Требования к решению:

1. Создать Gameboard с физической структурой организации (больница / клиника / etc) и ИТ-инфраструктурой.
2. Опишите «ценности», которые могут заинтересовать киберпреступников. Предположите, какая средняя сумма ущерба / убытка возможна для каждого типа «ценностей» и какова ожидаемая вероятность инцидента, направленного на этот тип «ценностей».
3. Основываясь на реальных случаях и их комбинациях, опишите 2-4 потенциальных вектора атак.

Технические требования к решению:

Разработать набор презентационных материалов:

• Game board с физической и ИТ-инфраструктурой (эскизы также приемлемы)

• Краткое описание атак, аналогичное приведенному в примере (материалы для проработки). Рекомендуются ссылки на реальные случавшиеся атаки.

Критерии оценки:

- Критерий: Реалистичность предложенной физической и ИТ структуры (насколько типичной является предложенная среда)
  Шкала оценки: максимальный балл - 5, минимальный балл - 1
- Критерий: Разнообразие угроз
  Шкала оценки: максимальный балл - 5, минимальный балл - 1
- Критерий: Опора на реальные кейсы
  Шкала оценки: максимальный балл - 5, минимальный балл - 1
- Критерий: Качество проработки (четкое понимания влияния каждой атаки на систему и возможных последствий для игрового сценария)
  Шкала оценки: максимальный балл - 5, минимальный балл - 1

Материалы для проработки:
https://box.kaspersky.com/f/17412466d064424facc4/