**Харківський національний економічний університет**

**імені Семена Кузнеця**

**ЗВІТ**

**З ВИКОНАННЯ ЛАБОРАТОРНОЇ РОБОТИ № 1**

**за дисципліною: *“*** **Корпоративні мережі та системи доступу**”

**на тему: “Розробка політики безпеки корпоративної інформаційної мережі”**

**Виконав: студент факультету Інформаційних технологій**

**3 курсу, спец. Кібербезпека,**

**групи 6.04.125.010.21.2**

**Бойко Вадим Віталійович**

**Перевірив:**

**Чугай Андрій Михайлович**

**ХНЕУ ім. С. Кузнеця**

**2023**

**Мета:** Навчитись розробляти імовірні загрози та приймати заходи для забезпечення безпеки корпоративної інформаційної мережі шляхом створення політики безпеки.

**Завдання:**

1. Аналіз системи інформаційної безпеки:
   1. Провести аналіз поточного стану інформаційної безпеки в обраній корпоративній інформаційній системі.
   2. Визначити можливі загрози та вразливості системи.
2. Визначення активів:
   1. Визначити всі активи, що потребують захисту в системі (дані, обладнання, програмне забезпечення тощо).
3. Оцінка загроз і ризиків:
   1. Створити список імовірних загроз для корпоративної інформаційної системи.
   2. Оцінити ризики, пов'язані з цими загрозами (використовуючи матрицю ризиків або інші методи).
4. Розробка політики безпеки:
   1. Визначити стратегію і принципи безпеки для корпоративної інформаційної системи.
   2. Сформулювати правила та процедури безпеки для співробітників і адміністраторів системи.
   3. Визначити механізми виявлення та відповіді на інциденти безпеки.
5. План впровадження:
   1. Розробити план впровадження політики безпеки в корпоративну інформаційну систему.
   2. Визначити кроки, які потрібно вжити для забезпечення безпеки.
6. Документація:
   1. Підготувати документ з політикою безпеки корпоративної інформаційної системи, включаючи всі вищенаведені елементи.
7. Презентація:
   1. Провести презентацію результатів лабораторної роботи, де ви поясните вибрані стратегії та політику безпеки.

**Хід роботи:**

1. Буде розроблена політика безпеки для організації з продажу товарів, дана організація має інтернет магазин, адміністративну панель та CRM систему
   1. Поточний стан організації такий, що все зберігається в одній базі даних та до будь яку систему можна відкрити просто написавши правильний URL у адресній стрічці браузера
   2. Можливі загрози:
      1. Взлам адмін панелі та CRM Системи
      2. Отримання даних для автентифікації про користувачів
2. Визначення активів
   1. Наступні активи потребують захисту
      1. Адмін панель та CRM система
      2. Дані для автентифікації користувачів
3. Оцінка загроз і ризиків
   1. Ймовірні загрози
      1. Sub-net enumeration
      2. SQL injection
   2. Оцінка ризиків

|  |  |  |  |
| --- | --- | --- | --- |
| Тип загрози | Загроза | Рівень небезпеки | Дії |
| Фізична | Вкрали сервер | Варіативний | Перемістити всі сервери до хмарових обчислень та робити резервне копіювання кожного дня |
| Фізична | Пожежа в кімнаті з серверами | Варіативний | Перемістити всі сервери до хмарових обчислень та робити резервне копіювання кожного дня |
| Фізична | Надзвичайна ситуація у будівлі (загроза для персоналу) | Варіативний | Має бути план евакуації для персоналу |
| Інформація | Пограбування | Екстремальний | Встановлення файерволу, логування, аудити, шифрування даних, DMZ зона для роботою з даними |
| Система | Внутрішня | Висока | Створення прав доступу, логування, аудити, шифрування, навчання співробітників |

1. Розробка політики безпеки
   1. Визначу стратегію і принципи безпеки для корпоративної системи
      1. Адмін панель та CRM система мають бути доступні лише через VPN
      2. Сервери мають бути перенесені до хмарних обчислень
      3. Паролі мають зберігатись окремо від основної інформації про користувача (за це має відповідати окремий сервіс)
      4. Встановити та налаштувати файервол
   2. Сформую правила та процедури безпеки для співробітників і адміністраторів
      1. Створити ролі та відповідно до ролей надавати доступ до якихось частин у системі
      2. Розробити план дій під час надзвичайних ситуацій
   3. Визначу механізми виявлення та відповіді на інциденти безпеки
      1. Для виявлення інцидентів буде впроваджено різні сервіси для моніторингу
      2. Для відповідей на інциденти також буде використовуватись сторонній сервіс
2. План впровадження
   1. Розроблю план впровадження політики безпеки в корпоративну інформаційну систему
      1. Перемістити всі сервери до хмарових обчислень та робити резервне копіювання кожного дня
      2. Створити плани евакуації для співробітників
      3. Проводити навчання співробітників
   2. Визначити кроки, які потрібно вжити для забезпечення безпеки.
      1. Фізична
         1. Перемістити всі сервери до хмарових обчислень та робити резервне копіювання кожного дня
         2. Створити плани евакуації для співробітників
      2. Інформація
         1. Встановлення файерволу
         2. Створити логування
         3. Проводити аудити
         4. Створити шифрування даних, щоб у разі пограбування даних, вони були зашифровані
         5. Створити DMZ зону для роботою з даними