Загрози .

1. Втручання в базу даних.

2. Компроментація пристроїв та облікових записів користувачів зі своєми девайсами.

3. Надмірний доступ до систем у користувачів.

4. Безпека IoT.

5. Втрата контролю над автентифікацією та авторизацією співробітників.

6. Доступ стороніх осіб до процесів бізнесу, в тому числі і споживачів.

Ризики.

1. Втрата особових даних споживачів та співробітників. Втрата фінансових та критичних даних.

Найвищий пріорітет.

1. Зараження системи та втрата даних та контролю через девайси співробітників.

Найвищий пріорітет.

1. Компроментація зсередини системи.

Середній приорітет.

1. Заволодіння контролем IoT.

Середній пріорітет.

1. Доступ злочинної особи або групи до системи.

Високий пріорітет.

1. Прослуховування та втрата інформації.

Заходи безпеки.

1. Встановлення додаткового брандмауера та максимальне обмеження доступу до серверів. Обовязкове шифрування при обміні даними. Резервне копіювання даних в зашифрованому вигляді.

2. Моніторинг та керування захистом девайсів співробітників. Встановлення ліцензійного антивірусу. Впровадження мультифакторної аутентифікації. Використання надійних паролів. Проведення постійних трененгів співробітників з кібербезпеки.

3. Впровадження централізованої системи контролю доступу (AD). Розбиття членів команди на підгрупи, які будуть мати мінімально необхідний доступ до ресурсів для виконання якісної роботи. Впровадження моделі нульової довіри та підвищення уваги на автентифікацію та авторизацію співробітників.

4. Шифрування даних та відокремлення IoT від підключення до робочих мереж. Створення окремого доступу до інтеренету та моніторинг активності.

5. Впровадження моделі нульової довіри та підвищення уваги на автентифікацію та авторизацію співробітників. Впровадження мультифакторної автентифікації , застосування надійних паролів. Централізоване керування доступом співробітників.

6. Сегментація мережі по відділам і рівню доступу. Створення окремої точки доступу для споживачів, можливе логічним шляхом. Застосування VPN зєднання між відділами та співробітниками у віддаленому зєднанні з мережею. Впровадження IDPS для контолю за трафіком та використання ШІ для виявлення аномальних явищ у мережі. Запровадження системи ID карток співробітників до доступу до робочого місця з занесенням у журнал даних користувача ID карти та час входу та виходу, використовуючи надійне шифрування зєднання датчиків зчитування.

Захист від фішингу.

Обовязкове пояснення фішингу співробітникам та наголошення на тому, що це найпоширеніший спосіб компроментації систем. Навчання користуванню поштовими клієнтами для фільтрації небезпечної пошти. Пояснення як виглядають піроблені листи та як їх розпізнати.