Приорітети: 1 - найвищий, 3 - найнижчий

Цифрові активи: клієнтська база (1), кадрова база (3), журнал замовлень(1), податкова звітність(2), база доходів та витрат(3), офіційні накладні(1)

1. Ризик: Втрата конфіденційності клієнтської бази.

Оцінка ризику: Високий

Наслідки: Репутаційні втрати

Заходи попередження: Використання сильного шифрування для збереження та передачі даних клієнтів, моніторинг доступу до бази та обмеження прав доступу.

2. Ризик: Компрометація кадрової бази.

Оцінка ризику: Високий

Наслідки: Можливіть конкуретів переманити цінного співробітника.

Заходи попередження: Введення механізмів аутентифікації та авторизації для керування доступом до даних персоналу.

3. Ризик: Незаконний доступ до журналу замовлень.

Оцінка ризику: Високий

Наслідки: Фінансові + репутаційні втрати

Заходи попередження: Моніторинг активності користувачів, впровадження системи виявлення вторгнень та логування подій.

4. Ризик: Незаконний доступ до податкової звітності.

Оцінка ризику: Високий

Наслідки: Порушення законодавства щодо оподаткування доходів

Заходи попередження: Захист податкової інформації за допомогою сильного шифрування та обмеженням доступу лише для уповноважених співробітників.

5. Ризик: Втрата бази доходів та витрат.

Оцінка ризику: Низький

Наслідки: Ускладнення аналізу динаміки розвитку бізнесу

Заходи попередження: Регулярне резервне копіювання даних та забезпечення доступу лише обраному персоналу.

6. Ризик: Втрата офіційних накладних товару.

Оцінка ризику: Високий

Наслідки: Порушення законодавства щодо оподаткування

Заходи попередження: Впровадження електронних систем замовлення товару та перевірки інтегритету документів.

7. Ризик: Зміна в законодавстві, що впливає на кібербезпеку та обов'язки зі збереження даних.

Оцінка ризику: Середній

Заходи попередження: Постійний моніторинг і адаптація політик безпеки та процедур відповідно до змін у законодавстві.

8. Ризик: Втрата доступу до цифрових активів через технічні збої або стихійні катастрофи.

Оцінка ризику: Високий

Заходи попередження: Розробка та тестування плану відновлення після інциденту та забезпечення резервного сховища даних.

9. Ризик: Атаки на веб-сайт та мережу із метою виведення сайту з ладу (наприклад, через SQL-ін'єкції або крос-сайтові скрипти).

Оцінка ризику: Високий

Наслідки: Фінансові + репутаційні втрати

Заходи попередження: Використання веб-захисту, регулярні аудити на вразливості та патчінг систем.

10. Ризик: Перехоплення конфіденційної інформації під час передачі даних між клієнтами та сервером (наприклад, відсутність TLS/SSL захисту).

Оцінка ризику: Високий

Наслідки: Репутаційні втрати

Заходи попередження: Встановлення SSL-сертифікату, захист передачі даних засобами шифрування.

11. Ризик: Злоумисники, які використовують соціальну інженерію для атак на співробітників та клієнтів (наприклад, фішинг або атаки відомого відправника).

Оцінка ризику: Середній

Наслідки: Можливе втручання зловмисника у систему

Заходи попередження: Навчання персоналу та клієнтів стосовно ідентифікації фішингових спроб, використання антивірусного та антиспамового програмного забезпечення.

12. Ризик: Непередбачувані технічні проблеми, такі як відмова обладнання або програмного забезпечення.

Оцінка ризику: Середній

Заходи попередження: Регулярний технічний обслуговування, моніторинг стану обладнання та готовність до відновлення.

13. Ризик: Зловживання привілеями або внутрішніми загрозами від співробітників.

Оцінка ризику: Високий

Заходи попередження: Встановлення строгого керування доступом, моніторинг дій співробітників та внутрішній аудит безпеки.

14. Ризик: Втрата даних через випадкове видалення або пошкодження.

Оцінка ризику: Середній

Заходи попередження: Регулярні резервні копії, які зберігаються на офсайті, та механізми відновлення даних.

15. Ризик: Зміна в магазинному програмному забезпеченні, яка може призвести до суттєвих недоліків у безпеці.

Оцінка ризику: Середній

Заходи попередження: Ретельне тестування та оцінка безпеки перед оновленням програмного забезпечення.