Чи захищений ваш бізнес від фішингу?

12 кроків для керівника компанії

Через один скомпрометований обліковий запис зловмисники можуть отримати доступ до договорів, фінансових документів, електронних підписів і комунікацій із контрагентами.

Перевірте, чи впроваджені у вашій компанії основні заходи захисту.

Захист облікових записів і робочих пристроїв

- ☐ **1. Багатофакторна автентифікація.** Для корпоративної пошти, хмарних сервісів і критичних облікових записів увімкнено додаткове підтвердження входу.
- ☐ **2. Унікальні паролі.** Співробітники не використовують однакові паролі для різних робочих сервісів. Для керування ними застосовується менеджер паролів.
- ☐ **3. Обмежені права доступу.** Працівники мають лише ті права, які необхідні для роботи. Звичайні облікові записи не дозволяють безконтрольно встановлювати програми.
- ☐ **4. Захищені робочі комп'ютери.** На пристроях встановлено актуальні оновлення, працюють засоби захисту від шкідливого програмного забезпечення.

Захист фінансових операцій та електронних документів

- ☐ **5. Захист КЕП.** У кожної уповноваженої особи власний електронний підпис. Особисті ключі та паролі не передаються іншим співробітникам.
- ☐ **6. Перевірка платіжних реквізитів.** Будь-яка зміна IBAN або отримувача коштів перевіряється незалежним каналом зв’язку з контрагентом.
- ☐ **7. Подвійне погодження платежів.** Важливі платежі новим отримувачам або на змінені реквізити проходять незалежну перевірку іншою уповноваженою особою. Де доступно, встановлено банківські ліміти й додаткові підтвердження.
- ☐ **8. Захист корпоративної пошти.** Налаштовано фільтрацію підозрілих повідомлень, контроль доступу та механізми SPF, DKIM і DMARC для поштового домену.

Готовність до кіберінцидентів

- ☐ **9. Резервне копіювання.** Важливі документи та облікові дані резервуються. Копії захищені від несанкціонованої зміни, а можливість відновлення регулярно перевіряється.
- ☐ **10. Навчання співробітників.** Команда періодично проходить навчання з фішингу. За потреби проводяться контрольовані фішингові симуляції.
- ☐ **11. План реагування.** Є зрозуміла інструкція: кому повідомляти про підозрілий лист, як діяти після компрометації пароля, ключа КЕП або фінансового акаунта.
- ☐ **12. Моніторинг загроз.** Визначено, хто контролює події безпеки та реагує на підозрілу активність. Для критичних систем розглянуто професійний моніторинг або послуги SOC.

Оцініть результат

10–12: більшість базових заходів впроваджена. Варто перевірити їхню фактичну ефективність.

6–9: є суттєві напрями для посилення захисту.

0–5: доцільно якнайшвидше визначити пріоритетні заходи кібербезпеки.

Що робити далі?

Почніть із систем, компрометація яких може завдати найбільшої шкоди: корпоративна пошта, банкінг, КЕП, фінансові документи та доступи до електронних закупівель.

Якщо ви не впевнені, наскільки ефективно працюють наявні засоби захисту, професійна оцінка кіберризиків допоможе визначити пріоритети.

Дізнайтеся більше: sheriff.com.ua