Стратегія захисту даних і конфіденційності для «DataSecure Tech»

Крок 1. Оцінка наявної безпеки а також ідентифікація вразливостей компанії.

Поточний стан інформаційниої безпеки в даній компанії є критично недостатнім, враховуючи специфіку бізнесу, а саме робота з фінансовими даними клієнтів. Невідповідність жодним стандартам інформаційної безпеки.

В результаті чого можна описати наступні вразливості та ризики для компанії:

1. Відсутність шифрування на будь якому рівні.
- дані під час передачі або транакцій, логіни передаються у відкритому виді, що робить їх вразливими до перехоплення та маніпулювання ними (атака Main-in-the-middle);
- дані які зберігаються у відкритому виді у хмарі та на локальних серверах компанії зберігаються у не зашифрованому виді, у разі витоку даних вся інформація потрапить до зловмисників у четабельному вигляді.

2. Безпека в мережі.
- брандмауери не налаштовані, немає правил фільтрації, в результаті чого не здатні протистояти атакам, ьлокувати шкідливий трафік або вияявляти підозрілу активність в мережі;
- відсутність систем IDS/IPS в результаті чого компанія не може відслідкувати спроби вторгнення у реальному часі.

3. Контроль доступу.
- відсутня політика процесу надання, позбавлення, обмеження прав доступу для співробітників;
- можливо також відсутній принцип найменших привілеїв для працівників

4. Вразливість застосунків
- веб та мобільні застосунки можуть бути першоджерелом для зловмисників.

5. Відсутність відповідності нормативним актам та законодавству
- поточний стан не відповідає GDPR, ISO 27001 та закону України “Про захист персональних даних”, щ в свою чергу загрожує штрафам, позовам клієнтів та втратою репутації.

Крок 2. Пропозиція стратегії захисту

2.1. Стратегі шифрування даних

Щодо інформації в мережі:
Метод шифрування — TLS
Для веб застосунків — HTTPS
Для звязку між серверами — VPN/TLS
Отримати та впровадити **SSL/TLS** сертифікати для всіх доменів та серверів

Щодо інформації у хмарі:
Шифрування на рівні файлів
Використовувати нативні шифрувальні сервіси провайдера

Організувати керування ключами через менеджер ключів (KMS)

Щодо інформації на серверах:
Шифрування на рівні дисків (FDE)
BitLocker(Windows)/ LUKS(Linux)
Шифрування на рівні бази даних
Додатковий зфізичний захист серверів компанії, визначити осіб які мають фізичний доступ до серверів, встановити камери.

2.2. Стретегія анонімізації та псевдонімізації даних

- псевдонімізація на рівні веб та мобільних застосунків
  - Замінити прямі ідентифікатори (email, ID, name) на псевдоніми, випадкові токени в усіх системах де це можливо, крім системи обробки транзакцій
- анонімізація для тестування та аналітики:
  - назавжди видалити можливість ідентифікації особи з даних, що використовується в непродуктових середовищах

2.3. Загальні поліпшення інфраструктури

- впровадження багаторівневої мережевої безпеки:
  - Next-Generation Firewall (NGFW)
  - Системи вторгнення IDS/IPS
  - Сегментація мережі — поділити мережу на сегменти (сервер, користувач, база даних) та суворо обмежити доступ правилами брандмауера
- впровадити систему керування доступом (IAM – Identity and Access Management)
  - принцип найменших привілеїв
  - багатофакторна автентифікація (MFA)
  - впровадити регулярний аудит доступів