**Комплексна стратегія захисту даних для «DataSecure Tech»**

**Крок 1: Оцінка наявної безпеки**

***Виявлені вразливості:***

* Відсутнє шифрування даних - як на локальних серверах, так і в хмарі
* Базові брандмауери без правил фільтрації - не захищають від складних атак
* Відсутність IDS/IPS - відсутність механізму виявлення вторгнень.
* Відсутній контроль доступу - ризик несанкціонованого доступу до конфіденційних даних
* Стандартне антивірусні програми не забезпечують захист від складних загроз (APT, zero-day)

***Ризики:***

* Фінансові дані клієнтів під загрозою
* Порушення законодавства (GDPR, ЗУ «Про захист персональних даних»)
* Втрата довіри клієнтів та партнерів
* Штрафи та репутаційні втрати

**Крок 2: Розробка стратегії захисту**

До стратегії захисту в цьому випадку можна включити два напрямки, а саме шифрування та анонімізацію та псевдонімізацію для захисту інформації про клієнтів.

*Шифрування даних*

1. Диск:
   * Використовуємо Bitlocker/LUKS/FileVault
2. При передачі даних:
   * TLS/VPN(IPsec)/HTTPS (сертифікати придбати)
3. При роботі з файлами:
   * AES-256/GPG/TDE

*Анонімізація та псевдонімізація*

1. Анонімізація
   * Данні аналітики: видалити імена, адреси, ID
2. Псевдономізація
   * При транзакціях: використання TOKEN/HASH
3. Диференційована конфеденційність:
   * Статистичні дані: додавання «шуму» до результатів запиту
4. ZKR:
   * Аутентифікація: використовувати «принцип» Zero-knowledge Proof
5. При роботі з хмарними технологіями:
   * Використання NuCypher / Google Private Join Computer

**Крок 3: Відповідність законодавству**

Для відповідності законодавству України та міжнародним нормам потрібно зробити наступні кроки:

*Дотримання ISO/IEC 27001*

* Впровадити ***ISMS***: політики, процедури, оцінка ризиків, моніторинг
* Провести ***аудит безпеки*** та *підготуватися до сертифікації*
* *Забезпечити* ***навчання персоналу*** з інформаційної безпеки

*Дотримання GDPR*

* Призначити ***інспектора з охорони даних (DPO).***
* Впровадити ***процедуру отримання згоди*** та ***право бути забутим***
* Забезпечити ***шифрування та псевдонімізацію*** як технічні заходи
* Вести ***реєстр обробки персональних даних***

Що до Закону України «Про захист персональних даних», ми маємо впроваджувати технічні та організаційні заходи, забезпечувати CIA, пам’ятати про внутрішні політики та оновлювати їх. Призначення відповідальних осіб з роботи та обробки персональних даних.

Додатково треба звернути увагу на такі інструменти IDS/IPS як *Suricata* чи *Snort*, та впровадити їх на підприємстві.

Також для посилення безпеки впроваджувати контроль доступу, сегментацію мережі та автентифікацію на кожному рівні де працюють співробітники.

*Опціонально*

Інструменти для проведення перевірки безпеки

Оцінка:

Nmap, Gobuster, Enum4linux, Hydra, Zap Proxy, Wireshark, Netcat (перевірити на взаємодію з портами)

Для перевірки та розробки стратегії:

OpenSSL, Zap Proxy (BurpSuite), CyberChef (візуально побачити декодування, хешування), JohnTheRipper(hashcat), GPG(локальне шифрування файлів)

**Словник**

*APT (Advanced Persistent Threat)* - це складна, тривала кібератака, зазвичай здійснювана організованими групами. Мета- непомітний доступ до системи для збору даних або саботажу. APT часто використовує соціальну інженерію, zero-day та бекдори.

*Zero-day* - вразливість у програмному забезпеченні, про яку ще не знають розробники. Зловмисники можуть її експлуатувати до випуску патчу. Zero-day атаки є особливо небезпечними через відсутність захисту.

*GDPR (General Data Protection Regulation)* - Європейський регламент захисту персональних даних. Встановлює права осіб (доступ, видалення, згода) і обов’язки компаній. Вимагає технічні та організаційні заходи для захисту даних.

*BitLocker / LUKS / FileVault* - інструменти для шифрування дисків: BitLocker (Windows), LUKS (Linux), FileVault (macOS). Захищають дані у стані спокою від несанкціонованого доступу. Використовують симетричне шифрування з керуванням ключами.

*TLS / VPN (IPsec) / HTTPS* - протоколи для захисту даних під час передачі. TLS - основа HTTPS, забезпечує шифрування вебтрафіку. VPN/IPsec - створює захищене з’єднання між пристроями або мережами.

*GPG (GNU Privacy Guard)* - інструмент для шифрування, підпису та перевірки даних. Заснований на OpenPGP, підтримує асиметричне шифрування. Використовується для захисту файлів, електронної пошти та автентифікації.

*TDE (Transparent Data Encryption)* - шифрує бази даних на рівні файлів без зміни додатків. Застосовується в SQL Server, Oracle, PostgreSQL. Захищає дані у стані спокою, автоматично шифруючи/розшифровуючи.

*Token (токен)* - тимчасовий ідентифікатор, що замінює чутливі дані (наприклад, номер картки). Використовується для автентифікації або псевдонімізації. Знижує ризик витоку конфіденційної інформації.

*DPO (Data Protection Officer)* - Посадова особа, відповідальна за моніторинг відповідності організації вимогам захисту персональних даних. DPO консультує щодо GDPR, проводить оцінку ризиків, взаємодіє з регуляторами. Обов’язковий для компаній, що обробляють великі обсяги чутливих даних.

*Інструменти в розділі опціонально використовуються при тестуванні на проникнення та/або тестуванні додатків.*