

И в заключение - безопасность на уровне данных

1. Шифрование данных "в покое" (Data-at-Rest Encryption)

Угрозы:

- Несанкционированный доступ к физическим носителям
- Взлом хранилища данных

Реализация и нюансы:

- Использование AES, TDE (Transparent Data Encryption) для баз данных.
- Регулярное обновление ключей шифрования.

2. Шифрование данных "в передаче" (Data-in-Transit Encryption)

Угрозы:

- Перехват данных
- Man-in-the-Middle атаки

Реализация и нюансы:

- Использование протоколов TLS/SSL для шифрования данных при передаче.

3. Шифрование данных "в использовании" (Data-in-Use Encryption)

Угрозы:

- Взлом оперативной памяти
- Недоверенные исполнительные процессы

Реализация и нюансы:

- Использование технологий, таких как Intel SGX, для обеспечения безопасности данных в оперативной памяти.

4. Маскирование данных (Data Masking)

Угрозы:

- Несанкционированный доступ к конфиденциальным данным
- Утечка данных

Реализация и нюансы:

- Использование методов маскирования для замены идентифицирующей информации.

5. Управление доступом к данным

Угрозы:

- Неавторизованный доступ
- Внутренние угрозы

Реализация и нюансы:

- Принцип наименьших привилегий
- ACLs (Access Control Lists), RBAC (Role-Based Access Control)

6. Бэкап и восстановление

Угрозы:

- Потеря данных
- Физические повреждения

Реализация и нюансы:

- Регулярное создание резервных копий данных.
- Хранение бэкапов в удаленных и безопасных локациях.

7. Аудит и мониторинг доступа к данным

Угрозы:

- Несанкционированный доступ
- Внутренние угрозы

Реализация и нюансы:

- Журналирование всех запросов к данным.
- Использование системы мониторинга для отслеживания необычных паттернов доступа.

8. DLP (Data Loss Prevention)

Угрозы:

- Утечка данных через электронную почту, USB, облако и т.д.

Реализация и нюансы:

- Использование DLP-систем для мониторинга и блокировки попыток несанкционированного копирования, передачи или хранения данных.

9. Immutable Backups and WORM storage

Угрозы:

- Попытки удаления или изменения данных

Реализация и нюансы:

- Создание неизменяемых бэкапов.

- Использование WORM (Write Once, Read Many) хранилищ для предотвращения удаления или изменения критически важных данных.

10. Zero Trust Data Architecture

Угрозы:

- Внутренние и внешние атаки
- Слабые периметры безопасности

Реализация и нюансы:

- Применение стратегии "ноль доверия" к доступу к данным. Проверка каждого запроса, независимо от источника.