Уметалиев Алишер

Моделирование угроз для Cloud.ru

**Потенциальные Проблемы Безопасности:**

- Неправильная конфигурация хранилища статического контента S3 и PostgreSQL.

- Уязвимое backend-приложение

- Неправомерный доступ пользователей, несоответствующий их ролям.

- Интеграция с внешними сервисами (Telegram Slack) по API

**Последствия Эксплуатации Проблем:**

- Несанкционированный доступ к конфиденциальной информации.

- Компрометация backend-приложения приведет к эксплуатации всей инфраструктуры.

- Пользователь с повышенными привилегиями может эксплуатировать сегменты инфраструктуры.

- Завладев API-ключом, злоумышленник получит доступ к информации, передающейся на внешние сервисы.

**Способы Исправления и Смягчения Рисков:**

- Регулярные обновления ПО.

- Проверка конфигурации служб хранения данных.

- Шифрование SSL/TLS на всем пути следования пакета.

- Контроль привилегий пользователей.

**Уточняющие Вопросы Для Разработчиков:**

- С помощью какой технологии осуществляется передача данных от пользователя до backend-приложения?

- Какие меры безопасности предприняты при транспортировке пакета?

- Конфигурировались ли хранилища данных с учетом современных норм безопасности?

- Какой именно набор микросервисов развернут на backend-е?

- Отключены ли неиспользуемые порты и сервисы от действующей инфраструктуры?

- Какие виды привилегий существуют в секторе Auth и четко ли они соответствуют должностям и ролям сотрудников и пользователей данного сервиса?

- Используется ли двухфакторная аутентификация при проверке доступа пользователя к системе?

- Существует ли защита от brute-force атаки в панели авторизации?

- Как часто происходит контроль обновлений ПО?

- Создаются ли бэкапы данных, содержащихся в хранилище?

- Логируются и отслеживаются ли действия пользователей в системе?