# Casos de Ataques Cibernéticos Recentes

## Caso 1: Microsoft (2023 – Espionagem Storm-0558)

1. Data do ataque: junho de 2023.

2. Tipo de ataque: espionagem cibernética (APT – Advanced Persistent Threat).

3. Descrição: o grupo Storm-0558 comprometeu contas de e-mail de cerca de 25 organizações (incluindo agências do governo dos EUA) no Microsoft Exchange Online. O ataque ocorreu por meio de uma chave de autenticação roubada que permitia criar tokens falsos de acesso.

4. Vulnerabilidade explorada: falha no processo de emissão de tokens de autenticação (sem CVE atribuído, erro de design e gerenciamento de chaves).

5. Impactos/prejuízo: espionagem contra órgãos governamentais e empresas privadas estratégicas, afetando a confiança nos serviços cloud da Microsoft. Prejuízo indireto em reputação e possíveis multas.

6. Proteção possível: rotação frequente de chaves de autenticação; auditoria contínua dos sistemas; adoção de modelo Zero Trust.

## Caso 2: Uber (2022 – Acesso Interno Indevido)

1. Data do ataque: setembro de 2022.

2. Tipo de ataque: comprometimento de credenciais + engenharia social.

3. Descrição: um hacker de 18 anos conseguiu acesso à rede interna da Uber usando técnica de MFA fatigue (bombardeio de solicitações de login até que o funcionário aprovasse por engano). Com isso, obteve privilégios elevados e acessou sistemas internos como Slack, dashboards e repositórios de código.

4. Vulnerabilidade explorada: não ligada a CVE, mas sim falhas humanas e configuração fraca de MFA.

5. Impactos/prejuízo: exposição de código-fonte, credenciais internas e grande dano à reputação da Uber. Custos estimados em milhões de dólares para investigação e mitigação.

6. Proteção possível: uso de MFA mais forte (ex.: chaves físicas de segurança); treinamento de funcionários; segmentação da rede e limitação de privilégios.