Ataque 1 – Colonial Pipeline (EUA)

Data do ataque: Maio de 2021.

Tipo de ataque: Ransomware.

O grupo DarkSide invadiu os sistemas da Colonial Pipeline, uma das maiores redes de oleodutos dos EUA. Eles criptografaram arquivos e exigiram resgate em criptomoedas para liberar o acesso. A empresa teve que interromper temporariamente suas operações.

Vulnerabilidade explorada:

O ataque ocorreu devido a credenciais comprometidas (senha reutilizada em contas de VPN). Não há CVE específico, mas foi uma falha de segurança por falta de autenticação multifator (MFA).

Impactos/prejuízo:

Paralisação do transporte de combustíveis em boa parte da costa leste dos EUA.

Escassez de gasolina e aumento nos preços.

A Colonial pagou cerca de US$ 4,4 milhões em Bitcoin como resgate (parte recuperada depois pelo FBI).

Tipo de porteção que poderia ter evitado:

Autenticação multifator (MFA)

Monitoramento de acessos remotos.

Politica de senhas mais fortes e segmentação de rede.

Segundo ataque 2 – LATAM Airlines (América Latina)

Data do ataque: Junho de 2024.

Tipo de ataque: Ransomware (LockBit).

O grupo LockBit anunciou ter roubado dados da LATAM Airlines. A empresa sofreu sequestro de informações críticas, e houve risco de exposição de dados de

passageiros. O ataque interrompeu parte das operações e causou instabilidade nos sistemas internos.

Vulnerabilidade explorada:

Segundo relatórios preliminares, o ataque explorou falhas em sistemas de acesso remoto e má segmentação de redes corporativas. Ainda não foi divulgado um CVE específico, mas o LockBit geralmente explora vulnerabilidades conhecidas em softwares desatualizados.

Impactos/prejuízo:

Voo e reservas afetados temporariamente.

Exposição de dados de clientes.

Dano à imagem da empresa.

Valor do prejuízo não foi divulgado oficialmente, mas estimado em milhões de dólares.

Tipo de proteção que poderia ter evitado:

Atualização constante de sistemas (patch management).

Backup seguro e isolado.

Treinamento de funcionários contra phishing.

Monitoramento constante contra ransomware.