1) Microsoft Exchange Server Breach:

Data do ataque: Janeiro de 2021
Tipo de ataque: exploração de vulnerabilidades de *zero-day* (múltiplas) em servidores Microsoft Exchange, resultando em *data breach* (roubo/exfiltração de emails, credenciais, etc.)
Descrição do ataque:
Um ator malicioso conhecido como "Hafnium", entre outros, explorou pelo menos quatro vulnerabilidades zero-day em instalações do Microsoft Exchange on-premises. Essas vulnerabilidades permitiram que atacantes tivessem acesso completo aos servidores de e-mail e calendário, administradores dos servidores, pudessem instalar backdoors persistentes, e acessar dispositivos.
Vulnerabilidade explorada:
São vulnerabilidades zero-day em produtos de servidor de e-mail Microsoft Exchange (on-premises). Isso inclui falhas que permitem execução remota de código, escalonamento de privilégios, e instalação de backdoors.
Impactos e prejuízos:
Estima-se que ~250.000 servidores foram afetados globalmente.
Organizações impactadas incluíram governos, instituições financeiras, parlamentares, entidades reguladoras etc.
Divulgação e roubo de dados sensíveis (emails, credenciais, possivelmente segredos corporativos ou governamentais) e necessidade de remediação em muitos casos. Custos de auditoria, limpeza de sistemas, mitigação de danos e regulatórios.
Tipo de proteção que poderia ter sido aplicada:
Patch management / atualização rápida de software — se as vulnerabilidades conhecidas fossem prontamente corrigidas por parte dos administradores assim que divulgadas, muitos servidores poderiam ter sido protegidos.

2) Colonial Pipeline Ransomware Attack (DarkSide)

Data do ataque: 7 de maio de 2021.
Tipo de ataque: **ransomware** / extorsão digital. Atacantes criptografaram sistemas de TI da empresa, exigindo pagamento para restaurar acesso. Também paralisou operações físicas por precaução.
Descrição:
O grupo DarkSide obteve acesso aos sistemas da Colonial Pipeline por meio de senha comprometida de conta de VPN que estava inativa, mas sem

autenticação multifator (MFA). Uma vez dentro, os invasores implantaram ransomware, criptografaram dados, e forçaram a empresa a desligar parte de sua infraestrutura para conter o ataque. Como consequência, o transporte de combustíveis ficou interrompido, causando escassez temporária em algumas regiões e pânico na população. A empresa acabou pagando um resgate para retomar o serviço.

Vulnerabilidade explorada:

Senha fraca/comprometida / credenciais vulneráveis.

VPN inativa, mas ainda acessível, sem MFA.

Impactos e prejuízos:

Paralisação total do sistema de oleodutos da Colonial, que transporta ~45% do combustível usado na costa leste dos EUA.

Escassez de combustível em diversas localidades, aumento de preço, efeitos no abastecimento.

Tipo de proteção que poderia ter sido aplicada:

Autenticação multifator (MFA) para todas as contas que permitam acesso remoto (VPN, RDP, etc.). Isso teria impedido que apenas uma senha comprometida fosse suficiente para invasão