Ataques Cibernéticos

Profº Robson Calvetti

Atividade 2

Ataque 1 = SolarWinds / SUNBURST (2020)

Data do ataque: Março a Junho de 2020 (divulgado em dezembro de 2020).

Tipo de ataque: Ataque de cadeia de suprimentos (Supply Chain Attack) com backdoor (malware SUNBURST).

Descrição do ataque: Os invasores comprometeram o processo de atualização do software SolarWinds Orion, inserindo um código malicioso (backdoor SUNBURST) em uma atualização legítima. Assim, milhares de clientes que atualizaram seus sistemas instalaram o malware, que permitiu controle remoto e acesso furtivo aos sistemas afetados.

Vulnerabilidade explorada: CVE-2020-10148 (authentication bypass na API do SolarWinds Orion) entre outras vulnerabilidades relacionadas.

Impactos/prejuízo: Cerca de 18.000 clientes afetados, incluindo agências governamentais dos EUA; prejuízos financeiros e de reputação elevados, além do risco de espionagem e perda de dados sensíveis.

Tipo de proteção: Adoção de práticas rigorosas de segurança no desenvolvimento de software, auditoria e verificação de integridade das atualizações, segmentação de rede, monitoramento de comportamentos anômalos e resposta rápida a incidentes.

Ataque 2 = Colonial Pipeline (2021)

Data do ataque: Maio de 2021 (aproximadamente)

Tipo de ataque: Ransomware

Descrição do ataque: O grupo DarkSide invadiu a rede da Colonial Pipeline explorando uma conta VPN que não tinha autenticação multifator (MFA). Eles instalaram um ransomware que criptografou sistemas críticos, forçando a empresa a suspender temporariamente a operação do oleoduto, que é responsável pelo transporte de grande parte do combustível na costa leste dos EUA.

Vulnerabilidade explorada: Falta de autenticação multifator na VPN, permitindo acesso não autorizado. Não há CVE específico divulgado para essa falha.

Impactos/prejuízo: Paralisação do oleoduto por cerca de 5 a 6 dias, causando escassez e aumento de preços de combustíveis, além do pagamento de resgate de aproximadamente US$4,4 milhões.

Tipo de proteção: Implementação de autenticação multifator (MFA) para acesso remoto, segmentação da rede para limitar danos, monitoramento de atividades suspeitas e políticas de backup para rápida recuperação.

Obrigado!

Realizado Por:

Felipe Pereira do Nascimento - RA: 825126069

Guilherme Dourado Nascimento - RA: 825116419

Bruno de Oliveira Santos - RA: 823223513

Pedro Miranda Rabelo - RA:825243591

Kauane Sandes Brandão - RA: 825113309

Stephanny Ramos Rodrigues - RA: 82512339