Universidade São Judas Tadeu

Sistemas Computacionais e Segurança

ATAQUES CIBERNÉTICOS

João Vitor Chioatto Serafim – 825133189

Professor: Robson Calvetti

São Paulo – SP

2025

SolarWinds (2020)

Em dezembro de 2020 foi descoberto um dos maiores ataques de supply-chain já registrados, conhecido como caso SolarWinds. Hackers conseguiram comprometer o processo de atualização do software Orion, usado por milhares de empresas privadas e órgãos do governo dos Estados Unidos. Durante a distribuição de updates legítimos, um backdoor chamado SUNBURST foi inserido e acabou instalado em redes críticas no mundo todo. Diferente de uma falha tradicional ligada a um CVE, esse ataque explorou diretamente a cadeia de suprimentos de software, permitindo que os criminosos tivessem acesso remoto prolongado aos ambientes comprometidos. Os impactos foram enormes, com risco de roubo de informações sigilosas, necessidade de reposição de infraestrutura e milhões de dólares gastos em resposta e investigação. Para evitar incidentes semelhantes, são recomendadas medidas como a validação da integridade de atualizações, a segmentação de redes críticas, o monitoramento de tráfego e comportamento anômalo e a exigência de práticas de segurança mais rígidas por parte de fornecedores.

Colonial Pipeline (2021)

Outro incidente marcante ocorreu em maio de 2021, quando a Colonial Pipeline, responsável por um dos maiores oleodutos dos Estados Unidos, foi vítima de um ataque de ransomware realizado pelo grupo criminoso DarkSide. O acesso inicial se deu por meio de credenciais comprometidas de VPN que não estavam protegidas com autenticação multifator (MFA). Uma vez dentro, os atacantes criptografaram dados e sistemas, exigindo pagamento de resgate em criptomoedas. A empresa foi obrigada a interromper totalmente suas operações por vários dias, o que resultou em escassez temporária de combustíveis em algumas regiões e enormes prejuízos financeiros, além de abalar a confiança do público. Embora não tenha sido associado a um CVE específico, o ataque evidenciou falhas operacionais graves no controle de acessos. Como proteção, especialistas indicam o uso de MFA em todos os acessos remotos, o gerenciamento adequado de credenciais, a realização de backups isolados e testados, além da segmentação de redes para reduzir a movimentação lateral dos invasores.