Ataques Cibernéticos Recentes: Estudo de Casos

Nos últimos anos, ataques cibernéticos vêm crescendo em complexidade e impacto, afetando tanto empresas privadas quanto órgãos governamentais. Esses ataques exploram vulnerabilidades técnicas e falhas de segurança, resultando em prejuízos financeiros, interrupção de serviços essenciais e comprometimento de dados sensíveis. Este trabalho apresenta dois casos distintos de ataques cibernéticos ocorridos nos últimos cinco anos, analisando data, tipo, vulnerabilidade explorada, impactos e medidas preventivas que poderiam ter sido aplicadas.

Caso 1: Ataque à SolarWinds (2020)

- **Data do ataque:** Descoberto em dezembro de 2020, mas ocorrido meses antes.
- **Tipo de ataque:** Supply chain attack (ataque à cadeia de suprimentos).
- **Descrição:** Hackers comprometeram o software Orion da empresa SolarWinds, inserindo um backdoor chamado “SUNBURST”. Esse código malicioso foi distribuído por meio de atualizações oficiais do software para milhares de clientes, incluindo órgãos governamentais e grandes empresas privadas. Uma vez

dentro da rede, os invasores podiam realizar espionagem e movimento lateral.

- **Vulnerabilidade explorada:** CVE-2020-10148 – falha de autenticação no Orion, que permitia bypass de login.
- **Impactos:** Mais de 18.000 organizações foram afetadas. O ataque comprometeu dados sigilosos de agências governamentais norte-americanas, além de gerar custos bilionários em investigações e mitigação. É considerado um dos maiores casos de espionagem digital da década.
- **Tipo de proteção que poderia ter sido aplicada:**

Auditoria independente de código de software de fornecedores;

Verificação de integridade em atualizações distribuídas;

Segmentação de rede e monitoramento de tráfego suspeito.

Fontes:

https://www.zscaler.com/br/resources/security-terms-glossary/what-is-the-solarwinds-cyberattack

https://socprime.com/pt/blog/supernova-backdoor-a-second-apt-group-abused-solarwinds-flaw-to-deploy-web-shell-malware

Caso 2: Ataque de Ransomware ao Colonial Pipeline (2021)

- **Data do ataque:** Maio de 2021.
- **Tipo de ataque:** Ransomware.
- **Descrição:** O grupo criminoso DarkSide invadiu os sistemas do Colonial Pipeline por meio de credenciais comprometidas de uma VPN que não possuía autenticação multifator. O ransomware criptografou dados internos e exigiu pagamento de resgate em criptomoedas para liberar o acesso. Como medida de contenção, a empresa desligou temporariamente o maior oleoduto dos Estados Unidos.
- **Vulnerabilidade explorada:** Uso de credenciais comprometidas em VPN sem autenticação multifator (não possui CVE específico, falha relacionada a má configuração de segurança).
- **Impactos:** A interrupção do oleoduto provocou escassez de combustível na costa leste dos EUA, aumento dos preços e prejuízos econômicos significativos. A empresa pagou aproximadamente US$ 4,4 milhões em resgate, embora parte tenha sido recuperada pelas autoridades.
- **Tipo de proteção que poderia ter sido aplicada:**

  Implementação de autenticação multifator (MFA) em acessos remotos;

  Políticas rigorosas de gerenciamento de credenciais;

  Monitoramento de acessos e uso de threat intelligence;

  Estratégias de backup e recuperação em caso de ransomware.

Fontes:

https://pt-br.tenable.com/blog/colonial-pipeline-ransomware-attack-how-to-reduce-risk-in-ot-environments

https://www.rockwellautomation.com/pt-br/company/news/articles/as-licoes-do-ciberataque-a-colonial-pipeline.html