ATIVIDADE 10 de setembro - Luana Oliveira Sousa - Gestão de TI - Robson Calvetti

1. Ataque: SolarWinds (Dezembro 2020)
   - Tipo de Ataque: Ataque à cadeia de suprimentos.
   - Descrição: Os invasores comprometeram o software de monitoramento da SolarWinds (Orion) e distribuíram uma atualização maliciosa para milhares de clientes, incluindo agências governamentais e grandes corporações.
   - Vulnerabilidade Explorada: Não houve uma vulnerabilidade específica registrada no **CVE*, mas o ataque envolveu comprometimento da cadeia de suprimentos.
   - *Impacto*: Afetou cerca de 18.000 clientes, com danos estimados em bilhões de dólares, incluindo espionagem e roubo de dados.
   - Proteção Sugerida: Monitoramento rigoroso da integridade da cadeia de suprimentos e validação criptográfica de atualizações de software.

2. Ataque: WannaCry (Maio 2017)
   - Tipo de Ataque: Ransomware.
   - Descrição: O WannaCry explorou uma vulnerabilidade no sistema Windows (SMBv1), espalhando-se rapidamente por redes globais e criptografando dados dos sistemas afetados, exigindo resgate.
   - Vulnerabilidade Explorada: **CVE-2017-0144* (vulnerabilidade no protocolo SMB do Windows).
   - Impacto: Estimado em US$ 4 bilhões em prejuízos, atingindo organizações como hospitais e empresas de diversos setores.
   - Proteção Sugerida: Aplicação de patches de segurança, desativação de SMBv1, e uso de soluções de backup e recuperação.

Esses ataques destacam a importância de práticas de segurança robustas e atualizações constantes de software para prevenir invasões.