Ataque 1 – Ransomware WannaCry (2017, impacto até hoje)

• **Data do ataque**: maio de 2017 (apesar de ter mais de 5 anos, ainda é referência mundial).

• **Tipo de ataque:** Ransomware (sequestro de dados).

• **Descrição**: O malware WannaCry explorou uma vulnerabilidade no Windows (EternalBlue) para se espalhar rapidamente em redes corporativas, criptografando arquivos e exigindo resgate em Bitcoin.

• **Vulnerabilidade explorada**: CVE-2017-0144.

• **Impactos/prejuízo**: Afetou mais de 200 mil computadores em 150 países; prejuízo estimado em mais de 4 bilhões de dólares. Hospitais do Reino Unido tiveram que cancelar atendimentos.

Proteção que poderia ter evitado: Atualização de segurança (patch da Microsoft), firewall, segmentação de rede e backup periódico.

Ataque 2 – Vazamento de dados da Eleição dos EUA (Twitter Hack 2020)

• **Data do ataque**: julho de 2020. Tipo de ataque: Engenharia social / Phishing.

• **Tipo de ataque:** Engenharia social / Phishing.

• **Descrição**: Hackers invadiram contas verificadas no Twitter (incluindo Elon Musk, Barack Obama e Apple) usando phishing contra funcionários da empresa. Postaram mensagens pedindo bitcoins em nome dessas contas.

• **Vulnerabilidade explorada**: Não envolveu falha de software, mas sim engenharia social contra colaboradores (não listado em CVE, pois foi falha humana).

• **Impactos/prejuízo**: Cerca de 120 mil dólares arrecadados em bitcoins, além de um grande abalo na confiança na segurança do Twitter.

• **Proteção que poderia ter evitado**: Treinamento contra phishing, autenticação multifator forte, limitação de acesso administrativo