Arthur de Sousa Sales 82329334

Ataque 1 – Caso Colonial Pipeline (2021)

1. **Data do ataque:** Maio de 2021
2. **Tipo de ataque:** Ransomware
3. **Descrição do ataque:**
   O grupo de cibercriminosos DarkSide infectou os sistemas da Colonial Pipeline, a maior rede de oleodutos dos EUA. Eles criptografaram dados críticos e exigiram resgate em criptomoeda para liberar o acesso.
4. **Vulnerabilidade explorada:** Uso de credenciais comprometidas de VPN sem autenticação multifator (MFA). CVE relacionado: **CVE-2019-11510** (Pulse Secure VPN).
5. **Impactos/prejuízo:** A empresa interrompeu a distribuição de combustível por vários dias, afetando grande parte da costa leste dos EUA. O prejuízo estimado foi superior a **US$ 4 milhões pagos em resgate**, além do impacto econômico indireto no abastecimento.
6. **Proteção que poderia ter evitado:**

- Uso de autenticação multifator (MFA)
- Monitoramento contínuo de acessos suspeitos
- Segmentação de rede para isolar sistemas críticos

Ataque 2 – Caso Uber (2022)

1. **Data do ataque:** Setembro de 2022
2. **Tipo de ataque:** Engenharia social / Comprometimento de credenciais (phishing + MFA fatigue attack)
3. **Descrição do ataque:**
   Um hacker conseguiu acesso à rede interna da Uber explorando a técnica de **MFA fatigue**, enviando múltiplas solicitações de login para um funcionário até que ele aceitasse por engano. Com isso, o atacante conseguiu acesso ao painel interno da empresa.
4. **Vulnerabilidade explorada:** Não há CVE específico, pois se trata de falha no processo de autenticação multifator. Porém, o ataque explorou o fator humano (engenharia social).
5. **Impactos/prejuízo:** O invasor teve acesso a e-mails, dashboards internos, repositórios de código e outras informações corporativas sensíveis. Não houve prejuízo financeiro direto reportado, mas o impacto reputacional foi significativo.
6. **Proteção que poderia ter evitado:**

- Uso de **MFA mais seguro**, como chaves físicas (U2F / FIDO2)
- Treinamento de funcionários contra técnicas de engenharia social
- Monitoramento em tempo real de tentativas de login suspeitas