**UC – Sistemas Computacionais e Segurança – Atividade Prática 03**

**Proteção de dados e informações Parte I**

INTEGRANTES: Nicholas, Tobias, Victor, Wendel

**Ataques Cibernéticos**

**Colonial Pipeline**

**Data: 7 de maio de 2021**

**Tipo de ataque:** *Ransomware*.

**Descrição do ataque ou de como aconteceu:**

Através de um login comprometido ou uma vulnerabilidade no sistema de segurança, especula-se que foi através de credenciais de funcionários. Dentro da rede, o grupo DarkSide introduziu o ransomware, que iniciou o processo de criptografia de arquivos importantes no sistema de TI da empresa. Isso resultou na inacessibilidade dos dados para a Colonial Pipeline, provocando a paralisação de suas atividades de apoio administrativo.

***Vulnerabilidade explorada (verificar se está no CVE e qual o seu código)***

Não houve a utilização de uma falha técnica específica (CVE) ligada diretamente a problemas de software. No entanto, a razão principal para o ataque foi o uso de credenciais comprometidas.

***Impactos e/ou prejuízo (pode ser estimado)***

**Falta de Combústivel:** A interrupção no fornecimento de combustível gerou medo entre

clientese empresas, resultando em escassez em certos estados americanos.

**Elevação dos Preços:** Os preços dos combustíveis aumentaram consideravelmente enquanto durou a paralisação.  
**Preocupações sobre a Segurança Nacional:** O incidente ressaltou a fragilidade das infraestruturas críticas dos EUA diante de ataques cibernéticos, resultando em alertas globais sobre a urgência de fortalecer a segurança em áreas fundamentais.

***Tipo de Proteção que poderia ter sido aplicada para evitá-lo***

**Autenticação Multifator (MFA):** Acrescenta uma camada adicional de proteção, necessitando de múltiplos métodos de verificação (exemplo: senha e código) para entrar em sistemas, aumentando a dificuldade de acesso para hackers.

**Gerenciamento de Acesso Privilegiado (PAM):** Limita o acesso em sistemas críticos, assegurando que somente indivíduos autorizados tenham permissão e restringindo a movimentação de invasores na rede.

**Segmentação de Rede:** Divide a rede em setor, separando os sistemas cruciais e prejudicando a mobilidade dos invasores dentro da estrutura.