**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.

**STUXNET**

**Data: junho de 2010** (acredita-se que tenha começado a infectar sistemas já em 2009 ou até antes)

**Tipo de ataque:** *worm.*

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

O Stuxnet realizou um ataque altamente sofisticado. Ele foi implementado em sistemas desligados da internet (air-gapped), por meio de pendrives infectados. Dentro do sistema, o Stuxnet realizava ataques nos controladores lógicos programáveis (PLCs), aparelhos utilizados para automatizar procedimentos industriais. Um worm conseguiu acessar os sistemas SCADA que monitoravam as centrífugas usadas no enriquecimento de urânio no Irã, modificando suas rotações sem ser detectado pelos operadores, causando danos físicos.

**Vulnerabilidade explorada (verificar se está no CVE e qual o seu código)**O Stuxnet explorou várias vulnerabilidades, algumas das quais eram zero-day (até então desconhecidas pelos desenvolvedores e pela comunidade de segurança). Entre elas, quatro vulnerabilidades principais de segurança foram aproveitadas:

***CVE-2010-2568:*** *Falha no Windows que permitia a execução de código arbitrário através de atalhos (.LNK).*

***CVE-2010-2729:*** *Vulnerabilidade no Windows Print Spooler Service.*

***CVE-2010-3888*** *e* ***CVE-2010-3962****: Falhas relacionadas à elevação de privilégios e execução de código remoto.*

Essas foram as vulnerabilidades utilizadas para infiltrar as redes.

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

O programa nuclear do Irã sofreu um grande impacto em decorrência do **Stuxnet**. É claramente estimado por especialistas que foram mais de 1.000 centrífugas atingidas pelo respectivo ataque. O que trouxe por consequência um atraso muito grande para o programa.

Esse ataque fez com que o mundo inteiro olhasse para tamanha fragilidade dos sistemas de controle industrial, ainda mais em setores que se fazem muito mais necessários em nossa sociedade como de água, energia e indústrias nucleares. Claramente este evento demonstrou que seria necessária a implementação de novas medidas de segurança. Pontualmente, pudemos identificar um **atraso significativo no programa nuclear uraniano**.

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

Para evitar um ataque semelhante ao Stuxnet, várias medidas de segurança poderiam ter sido implementadas.

**Divisão de redes:** Garantir que redes industriais (ICS/SCADA) fiquem separadas da rede corporativa e da internet, diminuindo a chance de contaminação por dispositivos externos.

**Controle em dispositivos removíveis:** proibir o uso de USB e requerer somente o uso de dispositivos verificados.

**Observação e detecção de anomalias:** Utilizar ferramentas avançadas de observação e identificação de comportamento anormal para identificar atividades suspeitas em ambientes industriais.