SISTEMAS COMPUTACIONAIS E SEGURANÇA

Fabrício dos Santos - RA: 825142856

USJT 2025

Exemplo 1 – Ataque ao Grupo JBS (Ransomware – 2021)

Data do ataque: Maio de 2021.

Tipo de ataque: Ransomware (Revil).

- **Descrição:**

Hackers do grupo REvil invadiram os sistemas da JBS, maior processadora de carnes do mundo. Eles criptografaram arquivos importantes e paralisaram operações em diversos países, inclusive no Brasil e nos Estados Unidos, exigindo pagamento em criptomoeda para liberar os dados.

- **Vulnerabilidade explorada:**

Possível exploração de credenciais comprometidas e falhas não corrigidas em servidores internos. O ataque não está associado a um CVE único, mas a práticas de segurança insuficientes e sistemas desatualizados.

- **Impactos/prejuízos:**

Suspensão temporária de operações de frigoríficos nos EUA, Canadá e Austrália. A empresa pagou cerca de 11 milhões de dólares em Bitcoin para recuperar os sistemas. O ataque afetou toda a cadeia de fornecimento de carne.

- **Tipo de proteção que poderia ter evitado:**

Autenticação multifator em todos os acessos, atualização constante de sistemas e softwares, backups offline testados regularmente, segmentação de redes internas e programas de conscientização para funcionários sobre phishing.

Exemplo 2 – Ataque ao TSE (Brasil)

Data do ataque: Novembro de 2020, durante o primeiro turno das eleições municipais.

Tipo de ataque: Vazamento de dados e ataque de negação de serviço (DDoS).

- **Descrição:**

Durante o período eleitoral, hackers publicaram na internet dados antigos de servidores e ex-servidores do TSE. Ao mesmo tempo, realizaram um ataque DDoS que sobrecarregou os sites ligados às eleições, deixando o acesso lento ou indisponível por algumas horas.

- **Vulnerabilidade explorada:**

Exposição de informações antigas sem criptografia adequada e ausência de um sistema anti-DDoS robusto. Não há um CVE específico, pois não se tratou de uma falha de software único, mas de gestão de dados e proteção insuficiente.

- **Impactos/prejuízos:**

Vazamento de dados pessoais, instabilidade temporária nos sistemas online e desgaste para a imagem do TSE, embora o resultado das urnas não tenha sido afetado.

- **Tipo de proteção que poderia ter evitado:**

Uso de criptografia para dados sensíveis, exclusão de dados antigos desnecessários, políticas mais rígidas de segurança (como as previstas na LGPD), firewall de aplicação web e serviços especializados de proteção contra DDoS.