**Pesquisar**:

• Escolher 2 (dois) ataques cibernéticos de tipos diferentes ocorridos nos últimos 5 anos e fazer um texto com:

1. Data do ataque (pode ser aproximada);

2. Tipo de ataque;

3. Descrição do ataque ou de como aconteceu;

4. Vulnerabilidade explorada (verificar se está no CVE e qual o seu código);

5. Impactos e/ou prejuízo (pode ser estimado); e

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

**EXEMPLOS:**

**1 - Ataque à Change Healthcare**

* **Data do ataque:** Fevereiro de 2024
* **Tipo de ataque:** Ransomware
* **Descrição do ataque:** Em fevereiro de 2024, a Change Healthcare, um dos principais provedores de serviços tecnológicos para o setor de saúde, sofreu um ataque de vírus atribuído ao grupo de cibercrime BlackCat/AlphV. O ataque envolveu a inserção de vírus que criptografou os dados em seus sistemas, tornando-os inacessíveis para a companhia. Os criminosos, então, solicitaram um pagamento em criptomoeda para fornecer as chaves de descriptografia e devolver o acesso às informações. Este ataque foi particularmente prejudicial, já que a Change Healthcare é encarregada de coletar informações médicas e autorizações de pagamento para diversas instituições de saúde nos Estados Unidos.
* **Vulnerabilidade explorada:** Apesar do CVE exato não ter sido revelado publicamente, ataques de ransomware, como o BlackCat, frequentemente exploram vulnerabilidades conhecidas em softwares de gerenciamento de sistemas e redes. O uso de patches desatualizados e a falta de segmentação de rede são comuns em situações como essa, facilitando o acesso dos atacantes ao sistema da vítima. O CVE-2022-30190, uma vulnerabilidade no Microsoft Windows que permite a execução remota de código, foi associado a atividades de ransomware semelhantes, o que pode ter sido a porta de entrada para o ataque.
* **Impactos e/ou prejuízo:** O impacto do ataque foi significativo, com estimativas indicando que cerca de 4 bilhões de informações foram afetadas. A Change Healthcare informou um pagamento de aproximadamente US$ 22 milhões em resgate. Ademais, o ataque causou atrasos significativos nos serviços de saúde, afetando hospitais e clínicas em todo o país. O ataque atingiu diretamente o atendimento aos pacientes, o processamento de autorizações de atendimento e a eficiência financeira da empresa, resultando em prejuízos inestimáveis para as instituições de saúde que dependiam de seus serviços.
* **Tipo de Proteção que poderia ter sido aplicada para evitá-lo:** Para evitar um ataque desse tipo, a Change Healthcare poderia ter adotado diversas medidas de segurança, incluindo:
  + As atualizações regulares de software são fundamentais para evitar vulnerabilidades conhecidas.
  + Treinamento em segurança cibernética: Fazer treinamentos regulares para todos os funcionários sobre como identificar e evitar tentativas de phishing, que são, geralmente, a porta de entrada para ransomware.
  + A configuração da rede pode ter limitado o acesso dos invasores a sistemas críticos.
  + Soluções de backup e recuperação de dados: Implementar políticas de backup rigorosas e testadas com frequência poderia ter permitido à Change Healthcare recuperar dados sem ceder ao pagamento de resgate.

**2 - Ataque ao ChatGPT (OpenAI)**

* **Data do ataque:** Abril de 2024
* **Tipo de ataque:** Ataque de DDoS (Distributed Denial of Service)
* **Descrição do ataque:** Em abril de 2024, os serviços do ChatGPT da OpenAI sofreram um ataque de DDoS, causando intermitências e atraso nos serviços. Os criminosos usaram uma botnet para inundar os servidores da OpenAI com um grande volume de tráfego, prejudicando a performance e impedindo que os usuários acessassem o serviço de forma normal. O ataque foi coordenado e um grupo de cibercriminosos assumiu a responsabilidade, alegando que sua intenção era demonstrar a fragilidade dos serviços de inteligência artificial que se tornaram populares.
* **Vulnerabilidade explorada:** Apesar de o ataque não ter explorado uma vulnerabilidade de software específica, o DDoS frequentemente se aproveita de falhas na capacidade de distribuir os serviços. No contexto deste ataque, a infraestrutura da OpenAI pode não ter sido suficiente para suportar o volume de tráfego gerado, o que resulta em um desempenho ruim. A vulnerabilidade associada a serviços web e protocolos de rede, como o CVE-2020-0601, que explora falhas na validação de certificados, pode ser considerada como um risco adicional de ataques DDoS.
* **Impactos e/ou prejuízo:** O ataque resultou em grandes interrupções no acesso ao ChatGPT, afetando tanto usuários gratuitos quanto corporativos. Apesar de não haver um custo financeiro específico, estima-se que a interrupção de serviços em plataformas de tecnologia possa causar milhões de dólares em perdas de receita e danos à imagem. Ademais, o ataque gerou preocupações em relação à segurança dos serviços de inteligência artificial, o que levou a um aumento nas discussões sobre a segurança digital nesse mercado em ascensão.
* **Tipo de Proteção que poderia ter sido aplicada:** A fim de prevenir um ataque DDoS dessa magnitude, a OpenAI poderia ter adotado diversas medidas de segurança, tais como:
  + Os serviços de mitigação de DDoS devem ser utilizados para identificar e filtrar o tráfego malicioso antes de chegar aos servidores.
  + Redes de distribuição de conteúdo (CDNs): A utilização de CDNs pode distribuir a carga de tráfego e ajudar a lidar com picos de tráfego inesperados.
  + A utilização de ferramentas de monitoramento para identificar padrões de tráfego indesejado e responder prontamente a possíveis ataques.