**Aula 03 – Atividade proteção de dados e informações**

Nome: Bruno Rodrigues Reis

RA: 8222243147

**Pesquisa sobre ataques ciberneticos**

**1. Ataque ao Bybit Exchange**

* **Data do ataque:** Fevereiro de 2025​
* **Tipo de ataque:** Roubo de criptomoedas​
* **Descrição do ataque:** Hackers, supostamente associados ao grupo Lazarus da Coreia do Norte, conseguiram invadir a exchange de criptomoedas Bybit, sediada em Dubai, e roubaram 400.000 Ethereum, avaliados em aproximadamente US$ 1,5 bilhão.
* **Vulnerabilidade explorada:** Embora os detalhes específicos não tenham sido divulgados, ataques desse tipo frequentemente exploram falhas em protocolos de segurança, credenciais comprometidas ou vulnerabilidades em contratos inteligentes.​
* **Impactos e/ou prejuízo:** Este ataque é considerado o maior roubo de criptomoedas até o momento, resultando em uma perda substancial para a Bybit e seus clientes, além de afetar negativamente a confiança no mercado de criptomoedas. ​
* **Tipo de proteção que poderia ter sido aplicada para evitá-lo:** Adoção de medidas de segurança robustas, como autenticação multifator, auditorias regulares de segurança, monitoramento contínuo de transações suspeitas e implementação de protocolos de segurança avançados para proteger contra acessos não autorizados.

**2. Ataque de Ransomware ao Governo da Costa Rica**

* **Data do ataque:** Abril de 2022​
* **Tipo de ataque:** Ransomware​
* **Descrição do ataque:** O grupo de ransomware Conti lançou uma série de ataques contra várias agências governamentais da Costa Rica, incluindo o Ministério das Finanças. Os invasores criptografaram dados críticos e exigiram um resgate de US$ 20 milhões, ameaçando derrubar o governo caso não fosse pago. ​
* **Vulnerabilidade explorada:** Os detalhes específicos das vulnerabilidades exploradas não foram amplamente divulgados, mas ataques de ransomware geralmente se aproveitam de sistemas desatualizados, falta de patches de segurança e credenciais comprometidas.​
* **Impactos e/ou prejuízo:** O ataque paralisou serviços essenciais, afetou o pagamento de funcionários públicos e interrompeu sistemas de importação e exportação, causando prejuízos econômicos significativos e instabilidade governamental. ​
* **Tipo de proteção que poderia ter sido aplicada para evitá-lo:** Implementação de políticas rigorosas de atualização de sistemas, realização de backups regulares e seguros, treinamento de funcionários para identificar tentativas de phishing e adoção de soluções avançadas de detecção e resposta a ameaças.