ATIVIDADE 03

Docente: Robson Calvetti
UC: Sistemas Computacionais e Segurança – SCS

MARIANA HILDEBRAND DANTAS
RA: 824118462
Análise e Desenvolvimento de Sistemas - ADS

sãojudas universidade

ATIVIDADE 3:

Pesquisar 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 evita-lo.

ATAQUE DO TWITTER:

Data: Julho de 2020

Tipo de ataque: spear phishing (Quando o hacker tem uma empresa como alvo e realiza pesquisas detalhadas para criar uma mensagem que pareça verdadeira, com o objetivo de obter informações sensíveis).

Descrição: Hackers enganaram funcionários do Twitter, obtendo acesso às ferramentas internas e controlando contas de figuras públicas como Elon Musk e Barack Obama, postando tweets enganosos sobre criptomoedas.

Vulnerabilidade: Falha humana. Sem código CVE específico.

Impacto: 130 contas foram comprometidas e arrecadaram cerca de 120 mil dólares em criptomoedas.

Proteção: Autenticação multifator (MFA), que adiciona uma camada extra de segurança ao processo de login, exigindo mais de uma forma de autenticação para acessar contas, e treinamento em engenharia social, para ajudar os funcionários a identificar e evitar tentativas semelhantes.

ATAQUE AO JBS FOODS

Data: Maio de 2021

Tipo de ataque: Ransomware (Quando o malware criptografa os dados da vítima e exige um resgate para descriptografá-los.)

Descrição: Em maio de 2021, a JBS Foods foi atacada por ransomware, afetando suas operações na América do Norte e na Austrália. O ataque interrompeu a produção e comprometeu a cadeia de suprimentos.

Vulnerabilidade: Falhas em segurança de TI e práticas inadequadas de gerenciamento. Código CVE específico não foi divulgado.

Impacto: Interrupção nas operações e perdas financeiras, incluindo um resgate pago estimado em 11 milhões de dólares.

Proteção: Atualizações de software, segmentação de rede, soluções de backup e treinamento em segurança cibernética.