Atividades Professor Calvetti- Davi Emanuel Silva Adriano 823149648

ATIVIDADE LAB3

Ataque de Ransomware à Lojas Renner (Agosto de 2021)

Tipo de Ataque: Ransomware
Descrição: A Lojas Renner sofreu um ataque cibernético que criptografou seus servidores, afetando seus sistemas de vendas e operações online. O ataque impediu que os sistemas funcionassem normalmente, causando instabilidade nos serviços digitais da empresa.
Vulnerabilidade Explorada: Embora a empresa não tenha divulgado detalhes técnicos, é provável que o ataque tenha explorado falhas em sistemas desatualizados, acesso remoto indevido ou credenciais comprometidas.
Impactos: A empresa enfrentou interrupções em suas operações digitais e sofreu danos à reputação. O prejuízo financeiro não foi oficialmente divulgado, mas ataques desse tipo costumam gerar custos elevados com recuperação de dados e reforço da segurança.
Proteção Possível: Atualizações regulares dos sistemas, uso de autenticação multifator para acessos remotos, backup frequente dos dados e treinamento dos funcionários para identificar tentativas de phishing, que são frequentemente usadas para infectar sistemas com ransomware.

Vazamento de Dados do Facebook (Abril de 2021)

Tipo de Ataque: Exposição de dados por coleta automatizada (Scraping)
Descrição: Informações de mais de 500 milhões de usuários do Facebook foram vazadas e disponibilizadas gratuitamente em fóruns da dark web. Os dados incluíam números de telefone, nomes completos, e-mails e datas de nascimento. O ataque explorou um recurso de importação de contatos do Facebook, que permitia coletar dados massivamente sem a devida proteção.
Vulnerabilidade Explorada: A falha explorada já havia sido corrigida antes do vazamento, mas os dados haviam sido coletados anteriormente por meio da

funcionalidade de sincronização de contatos. O CVE específico não foi informado, mas a vulnerabilidade estava relacionada à extração indevida de informações por meio da API da plataforma.

Impactos: Com os dados vazados, milhões de usuários ficaram mais vulneráveis a golpes como phishing, ataques de engenharia social e tentativas de invasão de contas em outros serviços. O incidente também gerou preocupações sobre a privacidade dos usuários e levou a um aumento na desconfiança em relação ao Facebook.

Proteção Possível: O Facebook poderia ter implementado restrições mais rígidas na coleta de dados por meio de sua API, além de monitorar atividades suspeitas de scraping. Usuários, por sua vez, podem se proteger limitando a exposição de informações pessoais e ativando autenticação multifator para evitar acessos indevidos.