Ataques Cibernéticos (Últimos Cinco Anos)

A evolução tecnológica trouxe inúmeros benefícios para a sociedade, mas também abriu espaço para ameaças cada vez mais sofisticadas no ambiente digital. Os ataques cibernéticos cresceram significativamente nos últimos anos, atingindo desde usuários comuns até grandes corporações e órgãos governamentais. Esses incidentes causam prejuízos financeiros, comprometem a privacidade e colocam em risco a continuidade de serviços essenciais.

Nesta pesquisa serão apresentados dois ataques cibernéticos ocorridos nos últimos cinco anos, analisando suas características, vulnerabilidades exploradas, impactos gerados e medidas de proteção que poderiam ter evitado os incidentes.

1º Ataque: Caso Colonial Pipeline (EUA – 2021)

- **Data do ataque:** Maio de 2021
- **Tipo de ataque:** Ransomware
- **Descrição:** A Colonial Pipeline, maior operadora de oleodutos dos Estados Unidos, sofreu um ataque de ransomware realizado pelo grupo DarkSide. Os criminosos invadiram a rede corporativa e criptografaram sistemas

críticos, exigindo pagamento em criptomoedas para liberar os dados.

- **Vulnerabilidade explorada:** Acesso indevido por meio de credenciais comprometidas em um sistema VPN sem autenticação multifator. (CVE-2019-11510 foi associado a falhas similares exploradas por grupos de ransomware).
- **Impactos:** A empresa precisou interromper suas operações por vários dias, afetando o fornecimento de combustível em grande parte da costa leste dos EUA. Estima-se que o prejuízo direto e indireto tenha ultrapassado US$ 4 bilhões.
- **Tipo de proteção possível:** Autenticação multifator (MFA), monitoramento de acessos em VPNs, aplicação rápida de patches de segurança e segmentação de redes para impedir movimentação lateral.

Fontes:

https://www.welivesecurity.com/br/2021/05/11/ataque-de-ransomware-a-maior-rede-de-oleoduto-dos-eua-afeta-o-fornecimento-de-combustivel

https://www.cnnbrasil.com.br/internacional/ataque-cibernetico-provoca-fechamento-de-um-dos-principais-oleodutos-dos-eua

2º Ataque: Caso Facebook – Vazamento de dados de 533 milhões de usuários (2021)

- **Data do ataque:** Abril de 2021 (dados coletados entre 2019 e 2020 e divulgados em 2021).
- **Tipo de ataque:** Data Breach (coleta massiva de informações)
- **Descrição:** Um banco de dados com informações pessoais de 533 milhões de usuários do Facebook foi publicado em fóruns de hackers gratuitamente. Entre os dados vazados estavam nomes, números de telefone, e-mails e datas de nascimento. O ataque foi realizado explorando a função de "importar contatos" da plataforma, que permitia coletar informações em larga escala.
- **Vulnerabilidade explorada:** A falha foi catalogada como relacionada a scraping abusivo de dados via API, não corrigida a tempo. Não teve um CVE específico, pois envolvia falha de design na funcionalidade.
- **Impactos:** Vazamento em massa de informações pessoais utilizadas em golpes de phishing, ataques de engenharia social e clonagem de contas. O impacto financeiro direto para o Facebook foi menor, mas a reputação da empresa foi fortemente abalada, com investigações regulatórias em vários países.
- **Tipo de proteção possível:** Limitação de APIs públicas, implementação de limites de requisição, reforço em mecanismos anti-scraping e alertas de segurança aos usuários afetados.

Fontes:

https://www.cnnbrasil.com.br/tecnologia/dados-roubados-de-meio-bilhao-de-usuarios-do-facebook-vazam-na-internet

https://www.jusbrasil.com.br/artigos/vazamento-de-dados-do-facebook-e-suas-repercussoes-em-solo-brasileiro-sob-a-otica-da-lgpd/2519136013