Ataque cibernético a empresa Colonial Pipeline 2021:

Aluno- Leonardo De Grandi; Orientador- Richard Vieira

Analise e desenvolvimento de sistemas, AEMS

**RESUMO**

Na atualidade, com bilhões de dispositivos conectados à Internet, mecanismos capazes de garantir segurança cibernética precisam ser constantemente criados e aperfeiçoados. Dentre as ameaças existentes, os ransomwares têm apresentado crescimento vertiginoso e gerado prejuízos para governos, empresas e indivíduos. Este trabalho tem como objetivo analisar o ataque ocorrido na empresa Colonial Pipeline, mostrando como foi feito, consequências, roubo de dados, etc.

**PALAVRAS-CHAVE**- ransomwares, dados, roubo.

**1 INTRODUÇÃO**

O ataque cibernético à Colonial Pipeline em 2021 representa um marco significativo na história da cibersegurança, destacando a vulnerabilidade das infraestruturas críticas a ameaças digitais e as complexas ramificações que tais incidentes podem ter em nível nacional e global. Uma análise científica desse evento permite uma compreensão mais profunda de suas causas, impactos e implicações para a segurança cibernética e a gestão de crises.

**2 CAUSAS E TÁTICAS DO ATAQUE**

O ataque à Colonial Pipeline foi realizado por meio de um ransomware conhecido como DarkSide, que emprega táticas de dupla extorsão para maximizar os danos e pressionar as vítimas a pagar o resgate. As causas subjacentes ao ataque incluem vulnerabilidades de segurança na infraestrutura de TI da Colonial Pipeline, bem como possíveis lacunas na detecção e resposta a ameaças cibernéticas.

**3 IMPACTOS OPERACIONAIS E ECONOMICOS**

O ataque resultou na interrupção temporária das operações do oleoduto, causando escassez de combustível em várias regiões dos Estados Unidos e aumentando os preços dos combustíveis. Além disso, o incidente teve impactos significativos nas operações da Colonial Pipeline, incluindo custos de recuperação, perda de receita e danos à reputação da empresa.

**4 SEGURANÇA ENERGETICA E RESILIENCIA DE INFRAESTRUTURAS CRITICAS**

O ataque destacou a importância da segurança cibernética na proteção das infraestruturas críticas, como oleodutos, redes de energia e sistemas de abastecimento de água. Revelou também a necessidade de aumentar a resiliência dessas infraestruturas contra ameaças digitais, por meio de investimentos em tecnologias de segurança avançadas, práticas de governança de segurança e colaboração entre o setor público e privado.

**5 INFORMAÇÕES COMPROMETIDAS**

Até onde se sabe publicamente, a Colonial Pipeline afirmou que não houve evidências de que os dados dos clientes foram comprometidos durante o ataque cibernético. No entanto, os detalhes exatos sobre quais informações podem ter sido acessadas ou comprometidas pelo grupo de ransomware DarkSide não foram totalmente divulgados pelas autoridades ou pela empresa. Geralmente, em ataques de ransomware, os invasores criptografam os dados da vítima, impedindo o acesso a eles até que um resgate seja pago. Em alguns casos, os invasores também podem exfiltrar dados antes da criptografia, com a ameaça de vazar essas informações se o resgate não for pago. Portanto, enquanto a Colonial Pipeline não divulgou informações específicas sobre dados comprometidos, é possível que informações operacionais ou internas tenham sido afetadas pelo ataque.

**6 MEDIDAS ADOTADAS PELA EMPRESA**

Após o ataque cibernético à Colonial Pipeline, a empresa tomou uma série de medidas para lidar com a situação e mitigar os impactos do incidente. Algumas das medidas adotadas pela empresa incluíram:

**6.1 Desligamento dos Sistemas Afetados**: A Colonial Pipeline desligou proativamente os sistemas afetados pelo ataque para evitar uma possível propagação do ransomware e proteger os dados restantes de serem comprometidos.

**6.2 Acionamento de Equipes de Resposta a Incidentes**: A empresa mobilizou equipes de resposta a incidentes e especialistas em segurança cibernética para investigar o ataque, avaliar a extensão dos danos e identificar as medidas necessárias para restaurar a segurança dos sistemas.

**6.3 Comunicação com Autoridades:** A Colonial Pipeline colaborou com autoridades governamentais, incluindo o FBI e o Departamento de Segurança Interna dos Estados Unidos, para compartilhar informações sobre o ataque e buscar assistência na resposta ao incidente.

**6.4 Restauração dos Sistemas e Serviços:** A empresa trabalhou rapidamente para restaurar a operacionalidade de seus sistemas e serviços afetados, implementando medidas de mitigação e recuperação de dados para minimizar os impactos do ataque.

**6.5 Avaliação e Aprimoramento da Segurança Cibernética:** Após o incidente, a Colonial Pipeline realizou uma revisão abrangente de suas práticas de segurança cibernética e implementou medidas adicionais para fortalecer a proteção de seus sistemas contra futuros ataques.

**6.6 Comunicação com o Público e Parceiros:** A empresa forneceu atualizações regulares sobre o status do incidente e suas ações de resposta aos clientes, parceiros e ao público em geral, visando manter a transparência e fornecer orientações sobre medidas de precaução.

Essas medidas demonstram a resposta proativa e coordenada da Colonial Pipeline ao ataque cibernético, destacando a importância da preparação e da capacidade de resposta rápida diante de ameaças cibernéticas cada vez mais sofisticadas e generalizadas.

**7 MEDIDAS PÓS ATAQUE**

Após o ataque cibernético à Colonial Pipeline, a empresa implementou uma série de medidas adicionais para fortalecer sua segurança cibernética e evitar futuros incidentes semelhantes. Algumas das medidas posteriores ao ataque incluíram:

**7.1 Revisão e Reforço das Medidas de Segurança Cibernética:** A Colonial Pipeline conduziu uma revisão abrangente de suas práticas de segurança cibernética, identificando áreas de melhoria e implementando medidas adicionais para fortalecer a proteção de seus sistemas e redes contra ameaças cibernéticas.

**7.2 Atualização de Políticas e Procedimentos de Segurança:** A empresa revisou e atualizou suas políticas e procedimentos de segurança cibernética, garantindo que estivessem alinhados com as melhores práticas do setor e abordassem os desafios específicos identificados durante a investigação pós-ataque.

**7.3 Investimentos em Tecnologias de Segurança Avançadas:** A Colonial Pipeline investiu em tecnologias de segurança cibernética avançadas, como sistemas de detecção de ameaças em tempo real, inteligência de ameaças e proteção de endpoints, para fortalecer sua postura de segurança e aumentar sua capacidade de detectar e responder a ataques cibernéticos.

**7.4 Treinamento e Conscientização dos Funcionários:** A empresa realizou treinamentos adicionais de conscientização em segurança cibernética para seus funcionários, visando educá-los sobre as ameaças cibernéticas mais recentes e promover uma cultura de segurança cibernética em toda a organização.

**7.5 Aprimoramento dos Planos de Resposta a Incidentes:** A Colonial Pipeline aprimorou seus planos de resposta a incidentes, incluindo procedimentos claros e bem definidos para lidar com futuros ataques cibernéticos, garantindo uma resposta rápida e eficaz em caso de emergência.

**7.6 Avaliação de Terceiros e Fornecedores:** A empresa revisou e avaliou a segurança cibernética de terceiros e fornecedores com os quais mantinha parcerias comerciais, garantindo que estivessem em conformidade com os padrões de segurança exigidos e não representassem um risco adicional para a empresa.

Essas medidas posteriores ao ataque demonstram o compromisso contínuo da Colonial Pipeline com a segurança cibernética e sua determinação em fortalecer sua resiliência contra ameaças digitais. Ao implementar essas medidas, a empresa busca reduzir a probabilidade de futuros incidentes cibernéticos e proteger suas operações críticas contra interrupções e danos.

**8 CONSIDERAÇÕES FINAIS**

Em suma, o ataque cibernético à Colonial Pipeline em 2021 representa um ponto de inflexão na conscientização sobre os riscos associados à dependência de infraestruturas críticas altamente conectadas e destaca a necessidade de abordagens proativas na proteção contra ameaças cibernéticas em um mundo cada vez mais digitalizado e interconectado.

**REFERENCIAS**

BBC NEWS BRASIL. O ataque de hackers a maior oleoduto dos EUA que fez o governo declarar estado de emergência. 2021. Disponível em <<[//www.bbc.com/portuguese/internacional-57055618](https://www.bbc.com/portuguese/internacional-57055618)>>

ALECRIM, EMERSON. EUA pagam US$ 10 mi por hackers do ransomware que atacou Colonial Pipeline. Tecnoblog, 2022. Disponível em <<//tecnoblog.net/noticias/eua-oferecem-10-milhes-dolares-informacoes-ransomware-darkside/>>

PETRY, GUILHERME. Ataque á Colonial Pipeline partiu de senha de VPN vazada na dark web. TheHack, 2021. Disponível em <<//thehack.com.br/ataque-a-colonial-pipeline-partiu-de-senha-de-vpn-vazada-na-dark-web/>>