ATAQUES CIBERNÉTICO

RYAN ROCHA - RA:825155072

ATAQUE AO MICROSOFT EXCHANGE SERVER

Data do ataque: Março de 2021

Tipo de ataque: Exploração de vulnerabilidades de zero-day exploit.

Descrição do ataque: Em janeiro de 2021, foram descobertas quatro vulnerabilidades d ezero-day exploit no Microsoft Exchange Server. Essas falhas permitiam que invasores tivessem acesso total aos e-mails, senhas dos usuários, privilégios de administrador no servidor e acesso a dispositivos conectados na mesma rede. Os atacantes frequentemente instalavam backdoors, garantindo acesso contínuo aos servidores comprometidos, mesmo após a aplicação de patches.

Vulnerabilidades exploradas: As vulnerabilidades exploradas foram identificadas como CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 e CVE-2021-27065.

Impactos e prejuízos: Estima-se que aproximadamente 250.000 servidores globalmente foram afetados, incluindo cerca de 30.000 nos Estados Unidos. Organizações governamentais, empresas privadas e instituições financeiras estiveram entre as vítimas, enfrentando riscos significativos de vazamento de dados sensíveis e interrupções operacionais.

Tipo de proteção que poderia ter sido aplicada: A aplicação imediata de patches fornecidos pela Microsoft teria mitigado as vulnerabilidades. Além disso, a adoção de sistemas de detecção e prevenção de intrusões, juntamente com práticas robustas de monitoramento de segurança, poderia ter ajudado na identificação e resposta rápida a atividades suspeitas.

A exploração de vulnerabilidades de zero-day exploit ocorre quando hackers descobrem e exploram uma falha de segurança em um software antes que o desenvolvedor tenha tempo de corrigi-la. O nome vem do fato de que a empresa responsável pelo sistema não teve nenhum dia para corrigir a falha antes que ela fosse usada em ataques.

ATAQUE DE RANSOMWARE AO GOVERNO DA COSTA RICA

Data do ataque: Abril de 2022

Tipo de ataque: Ransomware

Descrição do ataque: Em 17 de abril de 2022, o grupo de ransomware Conti lançou um ataque cibernético contra várias instituições governamentais da Costa Rica, incluindo o Ministério da Fazenda. O ataque resultou na interrupção de serviços críticos, como sistemas de declaração de impostos e controle de importações e exportações. Os invasores exigiram um resgate de US$ 10 milhões para não divulgarem as informações roubadas.

Vulnerabilidades exploradas: Embora o relatório específico de vulnerabilidades (CVE) exploradas não tenha sido divulgado publicamente, ataques de ransomware frequentemente exploram vulnerabilidades conhecidas em sistemas desatualizados ou utilizam técnicas de phishing para obter acesso inicial.

Impactos e prejuízos: O setor produtivo da Costa Rica sofreu perdas estimadas em US$ 30 milhões diários devido às interrupções nos sistemas governamentais. Além disso, houve exposição de dados sensíveis e uma crise nacional que levou o governo a declarar estado de emergência.

Tipo de proteção que poderia ter sido aplicada: A implementação de backups regulares e offline, políticas de segurança cibernética robustas, treinamento de funcionários para reconhecer tentativas de phishing e a atualização contínua de sistemas e softwares poderiam ter mitigado ou prevenido o impacto desse ataque.

O ransomware é um tipo de malware que sequestra dados ou sistemas, bloqueando o acesso até que um resgate seja pago. Ele geralmente criptografa arquivos ou impede o funcionamento do dispositivo, exibindo uma mensagem exigindo um pagamento, muitas vezes em criptomoedas, para fornecer a chave de descriptografia ou restaurar o acesso.