at_s22_A3_SL13_15redes_segurança

Roteiro de Atividade Prática

1 Título da atividade: Estamos com um grave incidente de segurança

Objetivos

Considerem a seguinte situação: na última sexta-feira à noite, os sistemas da Techsafe foram comprometidos por um ataque de ransomware que resultou na criptografia de dados críticos e na interrupção das operações de negócios. As ameaças e vulnerabilidades identificadas foram:

• Falhas de segurança nos sistemas de TI.
• Ausência de medidas de controle e detecção de ameaças avançadas.
• Falta de backup e planos de recuperação de desastres eficazes.
• Ataque de phishing bem-sucedido que permitiu a entrada inicial dos invasores.

Situação fictícia elaborada especialmente para o curso.

Agora, reflitam:

- Quais seriam as ações iniciais que poderiam ser tomadas?
- E quais seriam as estratégias de mitigação e recuperação?

Crie um e-mail para conscientizar os colaboradores da empresa sobre a atividade e seus riscos.

2 Título da atividade: Caso real: ataque de negação de serviço (DoS) ao Google (2020)

Em junho de 2020, o Google sofreu um ataque de negação de serviço (DoS) recorde que atingiu um pico de 2,56 terabits por segundo (Tbps). O ataque visou os servidores DNS do Google, que são cruciais para direcionar o tráfego da internet para os websites e serviços corretos. O Google mitigou o ataque utilizando técnicas de absorção de tráfego e roteamento inteligente. A empresa também trabalhou com provedores de internet para identificar e bloquear o

tráfego malicioso. O Google publicou um relatório detalhando o ataque e as medidas tomadas para mitigá-lo.

Ação

• Por que é importante que o Google tenha publicado um relatório detalhando o ataque e as medidas tomadas para mitigá-lo?
• Como você se comportaria se fosse o Google?
• Como pode ser classificado o incidente?