# Análise de relatório de incidente

Incidente de segurança modelo NIST

## Introdução

Elaborar um relatório com todo o conhecimento adquirido com o curso 3 da ordem de analista de segurança da google e coursera. Aqui, tudo será aplicado conforme a NIST e análises exclusivamente minhas, pois, dessa forma, o relatório fica mais autêntico e aplicarei a realidade brasileira, o que faz mais sentido para mim e para quem irá analisar esse documento.

## Cenário

Analise o cenário abaixo. Em seguida, conclua as instruções passo a passo.
Você é um analista de segurança cibernética que trabalha para uma empresa multimídia que oferece serviços de web design, design gráfico e soluções de marketing de mídia social para pequenas empresas. Sua organização sofreu recentemente um ataque DDoS, que comprometeu a rede interna por duas horas até que fosse resolvido.
Durante o ataque, os serviços de rede da sua organização pararam repentinamente de responder devido a uma inundação de entrada de pacotes ICMP. O tráfego de rede interno normal não pôde acessar nenhum recurso de rede. A equipe de gerenciamento de incidentes respondeu bloqueando pacotes ICMP de entrada, interrompendo todos os serviços de rede não críticos off-line e restaurando serviços de rede críticos.
A equipe de segurança cibernética da empresa então investigou o evento de segurança. Eles descobriram que um ator mal-intencionado havia enviado uma enxurrada de pings ICMP para a rede da empresa por meio de um firewall não configurado. Essa vulnerabilidade permitiu que o invasor mal-intencionado sobrecarregasse a rede da empresa por meio de um ataque distribuído de negação de serviço (DDoS).
Para resolver esse evento de segurança, a equipe de segurança de rede implementou:

- Uma nova regra de firewall para limitar a taxa de entrada de pacotes ICMP
- Verificação do endereço IP de origem no firewall para verificar se há endereços IP falsificados em pacotes ICMP de entrada
- Software de monitoramento de rede para detectar padrões de tráfego anormais
- Um sistema IDS/IPS para filtrar algum tráfego ICMP com base em características suspeitas

# Análise de relatório de incidente

Incidente de segurança modelo NIST

Como analista de segurança cibernética, você tem a tarefa de usar esse evento de segurança para criar um plano para melhorar a segurança de rede da sua empresa, seguindo o National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). Você usará o CSF para ajudá-lo a navegar pelas diferentes etapas de análise desse evento de segurança cibernética e integrar sua análise em uma estratégia geral de segurança. Dividimos a análise em diferentes partes no modelo abaixo. Você pode explorá-los aqui:

- Identifique riscos de segurança por meio de auditorias regulares de redes, sistemas, dispositivos e privilégios de acesso internos para identificar possíveis lacunas na segurança.
- Proteja os ativos internos por meio da implementação de políticas, procedimentos, treinamentos e ferramentas que ajudam a mitigar ameaças de segurança cibernética.
- Detecte possíveis incidentes de segurança e melhore os recursos de monitoramento para aumentar a velocidade e a eficiência das detecções.
- Responder para conter, neutralizar e analisar incidentes de segurança, implementar melhorias no processo de segurança.

Recupere os sistemas afetados para a operação normal e restaure os dados e/ou ativos dos sistemas que foram afetados por um incidente.

Mateus Breno Soares Silva

# Análise de relatório de incidente

Incidente de segurança modelo NIST

## Resumo

A organização sofreu um ataque DDoS, e isso fez toda a rede ser comprometida por duas horas. esse ataque é oriundo de uma enxurrada de ICMP, ao ponto de fazer tudo parar.
A equipe ao investigar o incidente, descobriram que a enxurrada de IMCP aconteceu devido à má configuração do firewall da empresa, gerando esse ataque.

## Identifique

A causa foi dada pela má configuração do firewall da rede, permitindo inúmeros pacotes ICMP sobrecarregando o tráfego.

## Proteja

A melhor maneira de proteger os dados, é fechando todas as portas de entrada e saída, e depois, permitir portas especificas pra saída, como por exemplo, o HTTPS, HTTP, DNS, entre outras.
Fazendo isso, a segurança fica extremamente mais rígida, fazendo com que seja muito difícil a tentativa de ataques como esse sejam bem-sucedidos.

## Detecte

Ao analisar a origem da enxurrada de pacotes ICMP, a equipe de segurança identificou que a origem partia de uma falha do firewall, provavelmente com recursos SIEM de monitoramento de rede.

## Responda

Nesse caso a melhor resposta é a restrição absoluta de todas as portas, deixando somente as necessárias abertas, e para saída de dados, assim, pode-se evitar ataques como o DDoS e outros piores.

Mateus Breno Soares Silva

# Análise de relatório de incidente

Incidente de segurança modelo NIST

## Recupere

A partir do momento em que as portas formam bloqueadas pelo firewall, para esse tipo de ataque, não há necessidade de depender de backups ou perda de dados, com as portas fechadas do firewall, um ataque DDoS passa a não ser um problema.

## Notas

É importante que a equipe de segurança vá atrás de brechas na empresa, pois esperar que um ataque aconteça para poder agir, pode ser prejudicial a organização e muitas vezes pode dar consequências irreversíveis. Se investigassem falhas, muito provavelmente identificariam o problema com o firewall e não perderiam 2 horas com todo o sistema parado.
Investir em segurança é sempre e sempre será a melhor maneira de evitar e se preparar para a grande maioria dos ataques.

Mateus Breno Soares Silva