Utilizando o framework NIST para responder à um incidente de segurança de rede

A partir de um incidente de segurança de rede, será elaborado um plano de melhoria seguindo a Estrutura de Segurança Cibernética (CSF) do Instituto Nacional de Padrões e Tecnologia (NIST).

Sumário	Uma empresa de multimídia sofreu recentemente um ataque DDoS que comprometeu a sua rede interna por duas horas, impedindo que qualquer pessoa utilizasse qualquer recurso de rede. O incidente terminou quando a equipe de gerenciamento de incidentes bloqueou a entrada de pacotes ICMP na rede. A causa do incidente se derivou de uma vulnerabilidade no firewall da empresa, que permitiu que o agente mal intencionado inundasse a rede com pings ICMP, realizando um ataque distribuído de negação de serviço. Após o evento, a equipe de segurança implementou uma nova regra de firewall, verificou o IP de origem dos pacotes, implementou dois softwares de monitoramento de rede (IDS e IPS) para analisar, filtrar e bloquear o tráfego ICMP.
Identificar	O agente mal intencionado realizou um ataque de negação de serviço distribuído (DDoS) por meio de uma vulnerabilidade derivada da má configuração do firewall. A vulnerabilidade permitiu que ele realizasse uma inundação de pacotes ICMP na rede da organização, impossibilitando a utilização de todas as ferramentas de rede.
Proteger	A equipe de segurança adotou medidas para conter a situação e melhorar a postura de segurança da empresa, como a implementação de um firewall bom e devidamente configurado e testado, dois sistemas de monitoramento de rede, um IDS para monitorar e relatar ameaças, e um IPS para filtrar e bloquear

	o tráfego ICMP.
Detectar	Para detectar e prevenir possíveis ameaças no futuro, a equipe de segurança configurou uma regra de verificação de IP no firewall para verificar spoofing de IP em pacotes ICMP, além de ter implementado um sistema de verificação de rede para detectar e bloquear tráfego anormal.
Responder	Em resposta a ataques futuros, a equipe de segurança irá isolar os dispositivos afetados, utilizar o sistema de monitoramento de rede para localizar, detectar e bloquear o tráfego suspeito, configurar o firewall para filtrar o tráfego, e restaurar os serviços que foram afetados. Após isso, a equipe irá analisar os logs de rede e utilizará ferramentas forenses para buscar a causa do ataque.
Recuperar	Para se recuperar de um incidente de segurança de rede como este, os pacotes ICMP devem ser urgentemente bloqueados no firewall, os serviços não essenciais de rede devem ser desativados para diminuir o tráfego, os serviços críticos devem ser restaurados e, após a inundação de rede passar, os sistemas e serviços não essenciais devem ser restaurados.
