Incident report analysis

Summary	Recentemente a empresa sofreu um ataque distribuído de negação de serviço (DDoS) que comprometeu a rede por 2 horas até ser resolvido. O ataque foi caracterizado como um “ICMP flood attack” que é quando um ou mais agentes maliciosos inundam a rede com o tráfego de pacotes ICMP sobrecarregando os recursos do servidor. O ataque foi controlado pela equipe de segurança que bloqueou o fluxo de pacotes ICMP e restaurou serviços de rede críticos.
Identify	A equipe de segurança cibernética da empresa investigou o incidente de segurança. Descobriu-se que um invasor malicioso 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 malicioso sobrecarregasse a rede da empresa por meio de um ataque de negação de serviço distribuído (DDoS).
Protect	Para lidar com esse evento de segurança, a equipe de segurança de rede implementou: - Uma nova regra de firewall para limitar a taxa de pacotes ICMP recebidos - Verificação do endereço IP de origem no firewall para verificar endereços IP falsificados em pacotes ICMP recebidos
Detect	Para detectar futuros ataques a equipe implementou: - Software de monitoramento de rede para detectar padrões de tráfego anormais - Um sistema IDS/IPS para filtrar parte do tráfego ICMP com base em características suspeitas
Respond	Para responder o incidente, paramos todos os serviços não críticos e

	bloqueamos o tráfego ICMP.
Recover	A equipe restaurou os serviços críticos e a normalidade do sistema.

Reflections/Notes: