Incident report analysis

Summary	Recentemente a organização sofreu um ataque DDoS, comprometendo a rede interna por cerca de duas horas até ser corrigido totalmente, foi identificado que o autor havia enviado ataque de flood de pings ICMP para rede da empresa no meio de um firewall não configurado e essa vulnerabilidade permitiu que a rede ficasse vulnerável e sobrecarregasse com o ataque DDoS.
Identify	Um ator ou mais atacaram a rede interna da corporação com ataque de inundação de ICMP, causando sobrecarga e fazendo a rede ficar indisponível por duas horas e precisavam ser protegidos e restaurados para um estado funcional.
Protect	A equipe de segurança implementou a nova regra do firewall para limitar o pacote de ICMP e IDS/IPS para monitorar e proteger o tráfego e deixar mais seguro.
Detect	A equipe de segurança cibernética configurou a verificação de endereço IP de origem no firewall para verificar endereços IP falsificados em pacotes ICMP recebidos e implementou software de monitoramento de rede para detectar padrões de tráfego anormais.
Respond	Para futuros eventos de segurança cibernética isolará os sistemas afetados para evitar interrupções na rede, tentará restaurar quaisquer sistemas e serviços que foram prejudicados no evento e a equipe analisará os logs da rede para verificar atividades e reportará todos os incidentes.
Recover	Para se recuperar de um ataque DDoS por inundação de ICMP, o acesso aos serviços de rede precisa ser restaurado para um estado de funcionamento normal. No futuro, os ataques externos de inundação ICMP poderão ser bloqueados no firewall. Então, todos os serviços de rede não críticos devem

	ser interrompidos para reduzir o tráfego da rede interna. Em seguida, os serviços críticos de rede devem ser restaurados primeiro. Finalmente, quando o fluxo de pacotes ICMP expirar, todos os sistemas e serviços de rede não críticos poderão ser colocados online novamente.

Reflections/Notes: