Análise de relatório de incidente

Resumo	A empresa passou por um evento de segurança quando todos os serviços de rede pararam de responder repentinamente. A equipe de cibersegurança descobriu que a interrupção foi causada por um ataque de negação de serviço distribuído (DDoS) através de uma enxurrada de pacotes ICMP. A equipe respondeu bloqueando o ataque e interrompendo todos os serviços de rede não críticos, para que os serviços de rede críticos pudessem ser restaurados.
Identificado	Um agente malicioso ou agentes maliciosos direcionaram um ataque de inundação ICMP à empresa. Toda a rede interna foi afetada. Todos os recursos críticos da rede precisaram ser protegidos e restaurados ao estado de funcionamento.
Protegido	A equipe de cibersegurança implementou uma nova regra de firewall para limitar a taxa de pacotes ICMP recebidos e um sistema IDS/IPS para filtrar parte do tráfego ICMP com base em características suspeitas.
Detectar	A equipe de cibersegurança configurou a verificação de endereços IP de origem no firewall para verificar endereços IP falsificados em pacotes ICMP recebidos e implementou um software de monitoramento de rede para detectar padrões de tráfego anormais.
Responder	Para futuros eventos de segurança, a equipe de cibersegurança isolará os sistemas afetados para evitar novas interrupções na rede. Eles tentarão restaurar quaisquer sistemas e serviços críticos que foram interrompidos pelo evento. Em seguida, a equipe analisará os logs de rede para verificar atividades suspeitas e anormais. A equipe também relatará todos os incidentes à alta administração e às autoridades legais competentes, se aplicável.

Recuperar	Para se recuperar de um ataque DDoS por inundação de ICMP, o acesso aos serviços de rede precisa ser restaurado ao seu estado normal de funcionamento. No futuro, ataques externos de inundação de ICMP podem ser bloqueados no firewall. Em seguida, todos os serviços de rede não críticos devem ser interrompidos para reduzir o tráfego interno da rede. Depois disso, os serviços de rede críticos devem ser restaurados primeiro. Finalmente, uma vez que a enxurrada de pacotes ICMP tiver expirado, todos os sistemas e serviços de rede não críticos podem ser reativados.

Reflexões e notas: