Análise de relatório de Incidente

Resumo	Esta manhã, a rede interna da empresa de multimídia sofreu um ataque de Negação de Serviço Distribuído (DDoS) do tipo ICMP flood, que a deixou indisponível por duas horas. O ataque foi caracterizado por um súbito e massivo influxo de pacotes ICMP, que sobrecarregou os serviços de rede, impedindo o acesso a recursos internos. A equipe de gerenciamento de incidentes agiu rapidamente, bloqueando a entrada de pacotes ICMP, desativando serviços não críticos e restaurando os serviços essenciais para mitigar o impacto do ataque.
Identificar	O incidente foi identificado como um ataque DDoS, especificamente um ICMP flood, direcionado à rede interna da organização. A investigação revelou que a vulnerabilidade explorada foi um firewall mal configurado, que permitiu que um agente mal-intencionado sobrecarregasse a rede com pacotes ICMP. Os sistemas afetados foram todos os serviços de rede internos, que ficaram inacessíveis durante o ataque.
Proteger	Para proteger a rede contra futuros ataques semelhantes, as seguintes medidas foram implementadas: - Uma nova regra de firewall foi configurada para limitar a taxa de entrada de pacotes ICMP. - A verificação do endereço IP de origem no firewall foi ativada para identificar e bloquear pacotes ICMP com endereços IP falsos. - Foi implementado um software de monitoramento de rede para detectar padrões de tráfego anormais, indicando possíveis ataques. - Um sistema IDS/IPS foi configurado para filtrar o tráfego ICMP com base em características suspeitas.

Detectar	Para aprimorar a capacidade de detecção de futuros incidentes, as seguintes ações foram tomadas: - O software de monitoramento de rede agora monitora continuamente o tráfego para identificar anomalias e padrões incomuns que possam indicar um ataque DDoS ou outro tipo de intrusão. - O sistema IDS/IPS está configurado para alertar a equipe de segurança sobre tráfego ICMP suspeito e outras atividades maliciosas, permitindo uma resposta rápida.
Responder	Em resposta ao incidente, a equipe de gerenciamento de incidentes seguiu os seguintes passos: - Bloqueio imediato da entrada de pacotes ICMP no firewall para conter o ataque. - Desativação de serviços de rede não críticos para preservar recursos e focar na restauração dos serviços essenciais. - Restauração dos serviços de rede críticos para minimizar o tempo de inatividade. - A equipe de segurança cibernética realizou uma análise pós-incidente para entender a causa raiz e identificar as vulnerabilidades.
Recuperar	Para garantir a recuperação e resiliência da rede, as seguintes ações foram realizadas e planos futuros foram estabelecidos: - Os serviços de rede foram restaurados à operação normal após a mitigação do ataque. - As configurações do firewall foram revisadas e atualizadas para prevenir futuras explorações. - Planos de contingência e recuperação de desastres serão revisados e aprimorados com base nas lições aprendidas com este incidente.

Reflexões/Notas: Este incidente ressalta a importância de configurações de firewall robustas e a necessidade de monitoramento contínuo do tráfego de rede. A rápida resposta da equipe de gerenciamento de incidentes foi crucial para minimizar o impacto do ataque. A implementação de um IDS/IPS e a melhoria das regras de firewall são passos importantes para fortalecer a postura de segurança da organização. É fundamental que a equipe de segurança continue a realizar auditorias regulares e a manter-se atualizada sobre as últimas ameaças e vulnerabilidades para garantir a proteção contínua dos ativos da empresa.