**Análise de relatórios de incidentes**

|  |  |
| --- | --- |
| **Resumo** | A empresa foi alvo de um ataque DDoS que comprometeu nossa rede interna por 2 horas antes de ser solucionado. O método de ataque foi uma inundação de pacotes ICMP que impossibilitou o tráfego de acessar recursos na rede. Após investigação foi descoberto que o ataque foi possível devido à um firewall não configurado. |
| Identificar | Um atacante ou atacantes empreenderam um ataque DDoS utilizando de inundação de pacotes ICMP, explorado através de um firewall não configurado, que interrompeu todo tráfego normal dentro da rede interna. |
| Proteger | A equipe de segurança adicionou uma nova regra de firewall com o propósito de limitar a taxa de pacotes ICMP recebidos, interrompeu os serviços de rede não críticos focando em restaurar os serviços críticos e implementou um sistema IDS/IPS para filtrar o tráfego destes pacotes com base em características suspeitas. |
| Detectar | No firewall foi configurado a verificação do endereço de IP de origem para verificar possíveis endereços de IP falsificados nos pacotes recebidos e implementado software de monitoramento para identificar padrões de tráfego anormais. |
| Responder | Para evitar ou mitigar incidentes futuros é necessária verificação periódica de atualização nos softwares de monitoramento, sistema IDS/IPS e regras de firewall, estar atento aos alertas de atividade suspeita emitidos através dos softwares de monitoramento e investigar o quanto antes qualquer atividade suspeita e anormal. No caso de um ataque bem sucedido, isolar os sistemas afetados para evitar propagação do ataque e recuperar sistemas e serviços críticos afetados no incidente. A equipe também se compromete a reportar o incidente à gerência e se necessário às autoridades legais. |
| Recuperar | Para se recuperar de um ataque deste tipo é preciso retornar o tráfego normal e acesso aos serviços de rede para o estado funcional. Todos os serviços não críticos de rede devem ser interrompidos e os serviços críticos devem ser restaurados o quanto antes. Quando a inundação de pacotes for controlada e terminada, os serviços não críticos devem ser restaurados. |

|  |
| --- |
| Reflexões/Notas: |