**Análise de relatório de incidente**

**Instructions**

À medida que você avança neste curso, você pode usar este modelo para registrar suas descobertas após concluir uma atividade ou para fazer anotações sobre o que aprendeu sobre uma ferramenta ou conceito específico. Você também pode usar este gráfico como uma forma de praticar a aplicação da estrutura NIST a diferentes situações que você encontrar.

|  |  |
| --- | --- |
| **Summary** | A empresa de multimídia sofreu um ataque DDoS que afetou a rede interna, tornando-a inoperante por duas horas devido ao fluxo excessivo de pacotes ICMP. Esse ataque comprometeu a capacidade dos serviços de rede de atenderem ao tráfego normal, interrompendo operações e afetando o atendimento ao cliente. A resposta ao incidente incluiu o bloqueio temporário dos pacotes ICMP e a desativação de serviços de rede não essenciais para priorizar serviços críticos. Após uma análise do incidente, foi detectado que o ataque explorou uma vulnerabilidade no firewall, permitindo que o tráfego de ping ICMP sobrecarregasse a rede. |
| Identify | Foi descoberto que um agente mal-intencionado havia enviado um ataque flood de pings ICMP para a rede da empresa por meio de um firewall não configurado. Essa vulnerabilidade permitiu que o invasor mal-intencionado sobrecarregasse a rede da empresa por meio de um ataque distribuído de negação de serviço (DDoS). |
| Protect | Para evitar ataques futuros, a equipe de segurança implementou novas medidas, incluindo uma regra de firewall para limitar a taxa de pacotes ICMP recebidos e a verificação de endereços IP para bloquear IPs falsificados. Além disso, reforçamos o treinamento dos colaboradores, enfatizando a importância de políticas de segurança robustas e a atualização contínua dos sistemas para garantir maior resiliência contra DDoS. |
| Detect | Na detecção de atividades suspeitas, foi aumentado a segurança adotando um sistema de detecção e prevenção de intrusões (IDS e IPS), que monitora o tráfego de entrada e sinaliza padrões incomuns. Um sistema de monitoramento em tempo real foi configurado para registrar o tráfego de rede, ajudando na identificação de comportamentos anômalos e na reação a possíveis incidentes futuros. |
| Respond | Durante o incidente, a equipe respondeu desativando temporariamente o tráfego ICMP, permitindo a recuperação parcial dos serviços críticos. Paralelamente, foi feita a comunicação com a alta gerência para mantê-los informados do progresso, além de documentar o incidente e reforçar o treinamento dos colaboradores para assegurar uma resposta ágil a novos incidentes. Após a contenção do ataque, a equipe restaurou os serviços e revisou as configurações de segurança nos dispositivos de rede. Com a atualização das políticas de backup, garantimos uma recuperação mais rápida e confiável em situações semelhantes. |
| Recover | Esse incidente enfatizou a necessidade de práticas de segurança cibernética mais rigorosas e de uma configuração de firewall adequada para proteger a empresa contra ataques DDoS. Com a implementação de novas ferramentas de monitoramento e a resposta rápida da equipe, foi possível mitigar danos e evitar interrupções mais longas. A empresa continuará investindo em segurança e no treinamento dos funcionários para se fortalecer contra futuras ameaças. |

|  |
| --- |
| Reflections/Notes: |