**Análise Resposta de incidente**

**Análise resposta de incidente de um ataque DDoS aplicando o NIST CSF.**

|  |  |
| --- | --- |
| **Resumo** | Esta manhã, os funcionários relataram à equipe de TI a impossibilidade de acessar a rede interna da empresa. A equipe de TI prontamente identificou uma significativa quantidade de pacotes ICMP provenientes de vários endereços IP. A equipe de segurança foi imediatamente mobilizada para responder ao incidente. Após 2 horas de paralisação das operações comerciais e investigações com base em logs e relatórios de funcionários, a equipe de gerenciamento de incidentes mitigou a situação bloqueando todos os pacotes ICMP. Essa ação temporariamente interrompeu serviços de rede não críticos, mas restaurou com sucesso os serviços de rede críticos.  Pós-incidente, a equipe de cibersegurança conduziu uma investigação para determinar a causa raiz do incidente. A equipe descobriu que um firewall mal configurado foi explorado. Essa vulnerabilidade permitiu que um ator malicioso lançasse um ataque de negação de serviço distribuído (DDoS), inundando a rede da empresa. |
| Identify | A equipe de gerenciamento de incidentes conduziu uma auditoria abrangente de sistemas, dispositivos e configurações para identificar lacunas de segurança. A equipe determinou que a causa raiz do incidente foi um firewall mal configurado, que permitiu que atores maliciosos sobrecarregassem a rede da empresa com pacotes ICMP. O incidente consistiu em um ataque de negação de serviço distribuído (DDoS) que comprometeu a rede da empresa, resultando na interrupção das operações comerciais. |
| Protect | A equipe implementou novas regras no firewall para limitar a taxa de pacotes ICMP. Foi adicionada a verificação do IP de origem no firewall para identificar endereços IP falsificados nos pacotes ICMP de entrada. Um software de monitoramento de rede foi implantado para detectar padrões de tráfego anormais. Além disso, um sistema IDS/IPS foi configurado para filtrar parte do tráfego ICMP com base em características suspeitas. |
| Detect | Para detectar proativamente incidentes futuros potenciais, a equipe empregará as seguintes estratégias:  Monitoramento de Tráfego de Rede:  Utilizar software de captura de pacotes para monitorar continuamente o tráfego de rede. Isso possibilitará a identificação de anomalias ou padrões suspeitos que possam indicar um possível incidente de segurança.  Monitoramento de Alertas do Sistema IDS/IPS:  Monitorar regularmente os alertas gerados pelos Sistemas de Detecção de Intrusão (IDS) e Sistemas de Prevenção de Intrusões (IPS). Essa abordagem proativa garante uma identificação rápida e uma resposta eficaz a possíveis ameaças de segurança.  Análise de Dados de Logs:  Analisar os dados de logs de todas as fontes da rede para identificar atividades ou padrões incomuns. Ao examinar os logs de maneira abrangente, a equipe pode identificar potenciais indicadores de comprometimento e tomar medidas preventivas.  Implementação de SIEM:  Implementar uma solução de Gerenciamento de Informações e Eventos de Segurança (SIEM) para centralizar e correlacionar dados de logs de várias fontes. Essa abordagem integrada aprimora a capacidade da equipe de detectar e responder a incidentes de segurança, proporcionando uma visão holística da rede.  Ao combinar essas técnicas de monitoramento e análise, a equipe visa aprimorar a postura geral de cibersegurança da organização e responder de maneira eficiente a possíveis incidentes futuros. |
| Respond | O plano de resposta da organização envolve os seguintes passos-chave:  Relato e Comunicação de Incidentes:  Inicie o plano de resposta relatando prontamente qualquer incidente potencial para o pessoal responsável e comunique a situação aos stakeholders. Isso garante uma resposta rápida e coordenada.  Utilização de Dados de Logs para Investigação:  Aproveite os dados de logs para facilitar o processo de investigação e determinar a causa raiz do incidente. A análise de logs fornece insights valiosos sobre a natureza e o escopo do evento de segurança.  Não Permissão de Protocolos:  Proativamente não permita protocolos que tenham sido explorados no ataque para proteger a infraestrutura crítica de rede. Essa medida ajuda a prevenir further exploração e mitigar o impacto nos serviços essenciais.  Bloqueio de Endereços IP de Assinatura do Atacante (Ataque DoS):  Em casos de um ataque de Negação de Serviço (DoS), bloqueie prontamente os endereços IP de assinatura do atacante para mitigar o impacto na disponibilidade e desempenho da rede. Essa ação visa interromper a capacidade do atacante de lançar novos ataques.  Sistemas IPS para Marcação de Características de Ataque:  Utilize Sistemas de Prevenção de Intrusões (IPS) para marcar características associadas ao atacante, facilitando a identificação e a quebra de persistência. Isso ajuda a evitar atividades maliciosas contínuas e aprimora a resiliência geral da rede.  Ao implementar essas medidas, a organização visa aprimorar as capacidades de resposta a incidentes, minimizar o impacto de eventos adversos e ativamente dissuadir e frustrar atividades maliciosas. |
| Recover | Para facilitar a recuperação das operações comerciais, a equipe de gerenciamento de incidentes dependerá de processos, diretrizes e tecnologias estabelecidas. Os principais componentes incluem:  Planos de Recuperação de Desastres:  Ativar e seguir os planos de recuperação de desastres estabelecidos para garantir uma restauração sistemática e organizada das funções críticas do negócio. Esses planos devem abranger procedimentos para recuperação de dados, restauração de sistemas e continuidade global dos negócios.  Plano de Resposta a Incidentes:  Consultar o plano de resposta a incidentes para orientar a equipe na execução de ações e procedimentos predefinidos. Isso inclui a identificação do incidente, medidas de contenção, erradicação de ameaças, processos de recuperação e análise pós-incidente.  Medidas Tecnológicas:  Utilizar ferramentas tecnológicas, como firewalls, para bloquear protocolos que foram explorados durante o incidente. Ao restringir o tráfego fora da rede da organização e implementar regras de firewall, a equipe pode evitar novas explorações e garantir a segurança da rede.  Limitação de Tráfego:  Implementar medidas para limitar o tráfego de saída e entrada apenas para comunicações essenciais. Isso ajuda a conter o incidente e reduzir o risco de comprometimento adicional, concentrando-se nas comunicações críticas necessárias para as operações comerciais.  Recursos Tecnológicos:  Aproveitar os recursos tecnológicos, incluindo sistemas de backup e infraestrutura redundante, para acelerar o processo de recuperação. Isso garante que os serviços essenciais possam ser restaurados de maneira eficiente e com tempo de inatividade mínimo.  Ao combinar esses processos, diretrizes e tecnologias, a equipe de gerenciamento de incidentes visa acelerar a recuperação das operações comerciais, garantindo a segurança e integridade da rede e dos sistemas da organização. |

|  |
| --- |
| Reflections/Notes:https://www.nist.gov/cyberframework |