**Análise de relatório de incidentes**

**Instruções**

À medida que você continua 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 encontrar.

|  |  |
| --- | --- |
| **Resumo** | A nossa empresa de multimídia sofreu um ataque distribuído de negação de serviço (DDoS) que comprometeu a rede interna por duas horas. O ataque ocorreu devido a um fluxo de entrada de pacotes ICMP, fazendo com que os serviços de rede da organização parassem de responder. O tráfego normal da rede interna não conseguia acessar nenhum recurso da rede. A equipe de gerenciamento de incidentes respondeu bloqueando a entrada de pacotes ICMP, interrompendo todos os serviços de rede não críticos e restaurando os serviços de rede críticos. Uma investigação revelou que um agente mal-intencionado enviou um ataque flood de pings ICMP à rede da empresa por meio de um firewall não configurado, permitindo a sobrecarga da rede. |
| Identificar | O tipo de ataque sofrido pela empresa foi um ataque distribuído de negação de serviço (DDoS), a causa raiz do ataque foi um firewall não configurado que permitiu o fluxo de entrada pacotes ICMP. O sistema afetado foi a rede interna da empresa, incluindo todos os recursos de rede. Os serviços de rede críticos foram interrompidos. A origem do ataque foi um agente mal-intencionado externo e o impacto que o ataque teve foi a indisponibilidade dos serviços de rede por duas horas, impedindo o acesso a recursos da rede. |
| Proteger | Para proteger ainda mais os ativos da organização, as seguintes medidas devem ser implementadas ou reforçadas, complementando as já tomadas:  **Atualização e configuração do firewall:**  Deve-se implementar uma nova regra de firewall para limitar a taxa de entrada de pacotes ICMP (já realizado). Deve-se implementar a verificação do endereço IP de origem no fireall para verificar se há endereços IP falsos nos pacotes ICMP (já realizado). É recomendado realizar auditorias regulares de configuração de todos os firewalls para garantir que estejam alinhados com as políticas de segurança e melhores práticas.  **Seguimentação de rede:**  Implementar a segmentação da rede para isolar sistemas críticos, limitando o impacto de futuros ataques.  **Gerenciamento de vulnerabilidades:**  Estabelecer um programa contínuo de varredura e gerenciamento de vulnerabilidades para identificar e corrigir proativamente as fraquezas de segurança em todos os sistemas e dispositivos da rede.  **Controle de acesso:**  Revisar e reforçar as políticas de controle de acesso para garantir que apenas usuários e serviços autorizados tenham os níveis de acesso necessários.  **Treinamento e conscientização:**  Conduzir treinamentos regulares para a equipe de TI e funcionários sobre ameaças cibernéticas, como ataques DDoS, e os procedimentos para identificá-los e reportá-los.  **Manutenção:**  Garantir que todo hardware, sistema operacional ou software afetado ou relevante para a segurança de rede seja atualizado regularmente.  **Tecnologia de proteção:**  Continuar utilizando e atualizando tecnologias de proteção como firewalls e sistemas de prevenção de intrusão (IPS) |
| Detectar | Para monitorar e analisar o tráfego de rede, softwares de aplicativos, rastrear usuários e detectar atividades incomuns:  **Monitoramento Contínuo de Segurança:**  Utilizar software de monitoramento de rede para detectar padrões de tráfego anormais (já implementado).  Implementar um sistema IDS/IPS para filtrar algum tráfego ICMP com base em características suspeitas (já implementado).  Implantar uma ferramenta de Sistema de Gerenciamento de Eventos e Informações de Segurança (SIEM) para agregar e analisar logs de diversos dispositivos de rede, servidores e aplicativos, permitindo a detecção de anomalias e eventos de segurança.  **Análise de Tráfego de Rede:**  Configurar ferramentas para inspecionar o tráfego de entrada e saída, procurando por padrões suspeitos, como um volume excessivo de pacotes ICMP de fontes não confiáveis.  **Auditoria de Contas de Usuário:**  Implementar auditorias regulares de contas de usuário e seus privilégios para identificar atividades anormais ou não autorizadas.  **Alertas:**  Configurar alertas em tempo real para a equipe de segurança de TI sobre anomalias e eventos de segurança detectados.  **Processo de Detecção:**  Definir claramente os processos e ferramentas para detectar eventos de segurança. |
| Responder | Para conter, neutralizar e analisar incidentes de segurança e implementar melhorias:  **Planejamento de Resposta:**  Manter um plano de resposta a incidentes atualizado que detalhe os procedimentos para diferentes tipos de ataques, incluindo DDoS. Este plano deve incluir etapas para conter o ataque (ex: bloqueio de IPs maliciosos, desvio de tráfego).  **Comunicações:**  Definir canais de comunicação claros para a equipe de resposta a incidentes e para informar as partes interessadas (gestão, outros departamentos, clientes, se necessário) sobre o incidente e as ações tomadas.  **Análise:**  Após a contenção, realizar uma análise forense detalhada para entender completamente o vetor de ataque, a extensão do comprometimento e as vulnerabilidades exploradas.  Documentar todas as ações tomadas durante a resposta ao incidente.  **Mitigação:**  Implementar etapas de resposta para mitigar o impacto do ataque, como isolar os recursos afetados ou desviar o tráfego malicioso. Neste incidente, isso foi feito bloqueando pacotes ICMP e desativando serviços não críticos.  **Melhorias:**  Após cada incidente, realizar uma revisão pós-incidente para identificar lições aprendidas e áreas de melhoria nos processos de segurança, configuração de ferramentas e no próprio plano de resposta.  **Contenção:**  A equipe de gerenciamento de incidentes já demonstrou capacidade de contenção ao bloquear pacotes ICMP e desativar serviços não críticos. Este procedimento deve ser formalizado e, se possível, automatizado. |
| Recuperar | Para retornar os sistemas afetados à operação normal e restaurar dados e ativos:  **Planejamento de Recuperação:**  Manter um plano de recuperação de desastres (DRP) que detalhe os procedimentos para restaurar serviços e sistemas críticos após um incidente.  Priorizar a restauração de serviços de rede críticos, como foi feito no cenário.  **Restauração de Sistemas:**  Garantir que os sistemas sejam restaurados a partir de backups limpos e conhecidos, caso dados ou configurações tenham sido corrompidos (embora neste cenário de DDoS, o foco principal seja a restauração da disponibilidade do serviço).  Verificar a integridade dos sistemas e dados após a restauração.  **Comunicações:**  Comunicar os procedimentos de restauração e o status da recuperação para as partes interessadas relevantes, incluindo usuários finais e equipe de TI.  **Melhorias:**  Revisar e testar regularmente o plano de recuperação para garantir sua eficácia e identificar quaisquer melhorias necessárias nos sistemas ou processos de recuperação. Por exemplo, considerar soluções anti-DDoS baseadas em nuvem que podem absorver e mitigar grandes volumes de tráfego malicioso antes que atinjam a rede da empresa. |

|  |
| --- |
| Reflexões/Notas: |