Análise de relatório de incidentes.

Resumo	Empresa de multimídia sofreu um ataque DDoS, resultando na interrupção da rede interna por duas horas. O ataque, causado por um fluxo excessivo de pacotes ICMP, impediu o acesso a recursos da rede. A equipe de gerenciamento de incidentes bloqueou esses pacotes, desativou serviços não críticos e restaurou os serviços essenciais. A investigação revelou que o ataque foi facilitado por um firewall não configurado, permitindo que um agente mal-intencionado realizasse o flood de pings ICMP, sobrecarregando a rede da empresa.
Identificar	A equipe de gerenciamento de incidentes auditou os sistemas, dispositivos e políticas envolvidas no ataque para identificar as lacunas na segurança. A equipe descobriu que um invasor 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).
Proteger	Para resolver e proteger a equipe de segurança de rede implementou: • Uma nova regra de firewall para limitar a taxa de entrada de pacotes ICMP • Verificação do endereço IP de origem no firewall para verificar se há endereços IP falsos nos pacotes ICMP recebidos • Software de monitoramento de rede para detectar padrões de tráfego anormais • Um sistema IDS/IPS para filtrar algum tráfego ICMP com base em características suspeitas

Detectar	Para detectar novos ataques como este, a equipe de segurança irá utilizar ferramentas de monitoramento e análise do tráfego de rede como: Wiresshark para monitorar pacotes de dados, utilizar sistemas de prevenção e detecção de intrusões (IDS/IPS), Configurar o firewall para registrar todos os eventos e analisar logs regularmente para detectar tentativas de acesso não autorizadas, realizar varreduras regulares para encontrar possíveis vulnerabilidades, e utilizar gerenciamento de acessos IAM, e MFA.
Responder	A equipe de segurança utilizará o plano de incidentes de segurança: ● Conter o incidente: isolamento rápido para conter os dispositivos afetados para não se propagar por toda rede, e bloquear acessos desconhecidos bem como IP's desconhecidos. ● Neutralizar o incidente: Analisar a causa raiz, entender como o incidente ocorreu e quais vulnerabilidades foram exploradas. Atualizar patches, atualizar sistemas para corrigir vulnerabilidades. ● Aprimorar o processo de recuperação: Documentação e Treinamento: Documentar todos os passos do incidente e realizar treinamentos regulares com a equipe sobre as melhores práticas de resposta, Avaliação de Ferramentas: Revisar e atualizar regularmente as ferramentas de segurança e monitoramento utilizadas
Recuperar	A equipe irá trabalhar para restaurar os bancos de dados do último backup íntegro antes do ataque, visando a recuperação imediata dos dados críticos e sensíveis, Logs de segurança e credenciais de acesso. E posterior a essas recuperações executar monitoramento contínuo, testes pós incidente e atualizações de patches de segurança,

Conclusão:

Ao aplicar o NIST, esse framework, as empresas podem continuamente aprimorar seus processos de segurança, aprendendo com cada incidente e reforçando suas defesas para enfrentar ameaças futuras de forma mais proativa e eficaz.

O NIST não só guia na resposta ao incidente, como também estabelece um ciclo contínuo de melhoria na segurança cibernética, aumentando a resiliência organizacional diante de um cenário de ameaças crescente e dinâmico.