Análise de Relatório de Incidentes

Resumo	A empresa de multimídia sofreu um ataque de negação de serviço distribuído (DDoS) que causou a interrupção de todos os serviços de rede por cerca de duas horas. O ataque foi realizado com um grande volume de pacotes ICMP (ping flood), que sobrecarregaram a rede interna. O tráfego passou por um firewall que não estava devidamente configurado, permitindo o ataque. A resposta incluiu o bloqueio do tráfego ICMP, desligamento de serviços não críticos e a restauração de serviços essenciais.
Identificar	• Tipo de ataque: Ataque DDoS por meio de flood de pacotes ICMP • Sistemas afetados: Roteadores, switches, servidores de serviços de rede internos • Origem do ataque: Endereços IP externos (possivelmente falsificados) explorando ausência de filtragem no firewall • Impacto: Interrupção dos serviços internos, indisponibilidade para usuários e clientes, perda temporária de produtividade • Vulnerabilidade explorada: Firewall mal configurado, sem regras de limitação ou verificação de pacotes ICMP
Proteger	• Regras atualizadas no firewall para limitar a taxa de pacotes ICMP recebidos • Implementação de verificação de endereço IP de origem no firewall • Treinamento de equipe técnica sobre prevenção de ataques DDoS • Revisão de políticas de acesso e exposição de serviços na rede pública • Agendamento regular de atualizações de firmware e auditorias de segurança em dispositivos de rede
Detectar	• Implementação de sistema IDS/IPS para identificar tráfego ICMP anormal • Utilização de ferramenta de monitoramento de rede para detectar padrões de

	tráfego suspeito • Integração com sistema SIEM para correlação de eventos e geração de alertas em tempo real • Auditoria e revisão periódica de logs de tráfego e eventos de rede • Criação de alertas automáticos para detecção de aumento repentino de tráfego ICMP
Responder	• Contenção imediata do ataque com bloqueio de pacotes ICMP no firewall • Desativação temporária de serviços não críticos para preservar os essenciais • Análise dos logs de firewall para rastreamento dos IPs e volume de pacotes • Desenvolvimento de plano de resposta documentado para ataques DDoS • Comunicação interna com a liderança e equipe técnica sobre o incidente • Planejamento de simulações periódicas de resposta a incidentes como prática de melhoria contínua
Recuperar	• Restauração dos serviços críticos de rede após contenção do ataque • Verificação da integridade dos dados e sistemas de produção • Aplicação de backups, quando necessário, para restaurar serviços impactados • Registro formal do incidente para aprendizado organizacional • Revisão dos processos de recuperação e criação de documentação técnica de referência • Planejamento de comunicação com clientes e partes interessadas, se necessário

---

Reflexões/Notas: Esse incidente demonstrou a importância de aplicar o NIST CSF para manter uma postura de segurança robusta. A vulnerabilidade no firewall mostrou que configurações básicas podem ter grandes impactos se negligenciadas. A resposta rápida foi essencial, mas medidas de prevenção e detecção precoce são fundamentais para evitar futuras interrupções.