Análise de resposta a incidente

Resumo	A empresa de multimídia sofreu um ataque **DDoS (Distributed Denial of Service)**, que sobrecarregou a rede interna com um fluxo massivo de pacotes **ICMP (ping flood).** Isso fez com que os serviços de rede parassem de responder por duas horas, impedindo o acesso a recursos críticos. A equipe de gerenciamento de incidentes respondeu bloqueando pacotes ICMP, desativando serviços não críticos e restaurando os serviços essenciais.
Identificar	A investigação revelou que o ataque foi possível devido a um **firewall não configurado corretamente**, que permitiu o tráfego malicioso.
Proteger	Primeiro, o **software de monitoramento de rede** foi instalado para analisar o tráfego em tempo real. Essas ferramentas ajudaram a detectar o pico anormal de pacotes ICMP que estava sobrecarregando a rede. Além disso, um sistema **IDS/IPS (Intrusion Detection System/Intrusion Prevention System)** foi configurado. Esse sistema analisa o tráfego da rede e bloqueia automaticamente atividades suspeitas, como pacotes ICMP em excesso ou de fontes desconhecidas. A empresa também passou a **revisar regularmente os logs de firewall, roteadores e servidores.** Essa análise permitiu rastrear a origem do ataque e entender como ele aconteceu.
Detectar	**Ferramentas de análise de comportamento foram implementadas.** Essas ferramentas usam inteligência artificial para detectar atividades fora do padrão na rede. Por exemplo, se houver um aumento repentino

	no tráfego ICMP, o sistema alerta a equipe imediatamente.
Responder	O plano de resposta ao incidente inclui a **contenção imediata do ataque**, bloqueando o tráfego malicioso com regras de firewall e isolando sistemas afetados para evitar a propagação. Em seguida, a **análise do incidente** é realizada para investigar a origem, os sistemas impactados e o dano causado, documentando todos os detalhes para relatórios e melhorias futuras. A **comunicação clara** com a equipe de TI, a gerência e os clientes é mantida, informando sobre o status da rede e as ações em andamento. Por fim, a **restauração dos serviços críticos** é priorizada, garantindo que os sistemas sejam verificados e colocados novamente online com segurança, minimizando o tempo de inatividade.
Recuperar	O plano de recuperação foca em **restaurar os sistemas e dados afetados** usando backups atualizados, garantindo que os serviços críticos voltem a funcionar rapidamente. Após a restauração, a rede é **monitorada de perto** para detectar resquícios do ataque ou novas ameaças. A empresa também **avalia o impacto** do incidente, analisando os custos operacionais e financeiros, e identifica lições aprendidas para melhorar a segurança. Por fim, as **políticas de segurança são revisadas e atualizadas**, com medidas adicionais implementadas para prevenir futuros incidentes.

Reflections/Notes: