Incidente análise de relatório

Instruções

À medida que você avança 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 do NIST a diferentes situações que encontrar.

Resumo	No início desta manhã, os serviços de rede da empresa ficaram indisponíveis por aproximadamente duas horas. A equipe de TI identificou que a interrupção foi causada por um ataque de Negação de Serviço Distribuída (DDoS) usando pacotes ICMP (ping flood). O tráfego de entrada sobrecarregou a infraestrutura de rede, impedindo o funcionamento normal do sistema. Após investigação, descobriu-se que o tráfego malicioso passou por um firewall mal configurado, permitindo que o invasor explorasse a vulnerabilidade. Não houve evidências de comprometimento de dados, mas a indisponibilidade temporária impactou diretamente os serviços voltados para o cliente.
Identificar	A equipe de resposta a incidentes auditou sistemas, dispositivos e políticas de acesso para identificar brechas de segurança. A análise revelou que o firewall não estava configurado para limitar ou filtrar pacotes ICMP, o que permitiu que o ataque de inundação ICMP atingisse recursos internos. O ataque interrompeu os serviços de hospedagem web, design gráfico e marketing digital. As permissões de acesso foram revisadas para garantir que apenas pessoal autorizado tenha acesso aos sistemas críticos.
Proteger	**A equipe implementou medidas de proteção imediatas, incluindo:**

	• **Criando uma nova regra de firewall para limitar a taxa de pacotes ICMP de entrada.** • **Habilitando a verificação da origem do IP para detectar falsificação.** • **Fortalecendo a autenticação em dispositivos de segurança.** • **Treinar a equipe de TI e segurança sobre prevenção de DDoS.** • **Atualizando configurações de firewall e políticas de segurança.** • **Avaliando o investimento em ferramentas de mitigação de DDoS mais robustas.**
Detectar	Para melhorar a detecção futura de ataques semelhantes, a equipe tomou as seguintes ações: • Implantou um sistema de monitoramento de rede para identificar padrões de tráfego anormais. • Instalou um IDS/IPS com capacidade de analisar o comportamento de pacotes ICMP. • Alertas automáticos configurados para picos de tráfego incomuns. • Adotou ferramentas SIEM para correlacionar e responder a eventos de segurança em tempo real.

Responder	Durante o incidente: ● O tráfego ICMP foi bloqueado no nível do firewall. ● Serviços não críticos foram retirados do ar para preservar recursos essenciais. ● A equipe de segurança cibernética conduziu análises forenses de tráfego para determinar a origem e o método de ataque. ● O incidente foi relatado formalmente à gerência. ● Os procedimentos de resposta a incidentes foram atualizados com base nas lições aprendidas.
Recuperar	● Os serviços de rede foram gradualmente restaurados depois que o ataque foi mitigado. ● Nenhum dado foi perdido — apenas indisponibilidade temporária foi relatada. ● O plano de recuperação foi revisado e reforçado para garantir uma restauração futura mais rápida.

	• Os departamentos afetados foram notificados e alinhados para normalizar as operações. • Melhorias nos planos de recuperação e continuidade de negócios foram documentadas para implementação.

Reflexões/Notas: Este incidente destacou a importância de configurações proativas e monitoramento contínuo. A falta de uma regra básica de firewall expôs a organização a um ataque evitável. A estrutura CSF do NIST orientou efetivamente a resposta e ajudou a identificar áreas críticas de melhoria, como detecção precoce, resposta coordenada e atualizações de infraestrutura. Como resultado, a empresa emergiu mais forte e resiliente.