**Análise de Relatório de Incidente**

**Resumo do Evento de Segurança**

A empresa enfrentou um incidente de segurança quando todos os serviços de rede pararam de responder repentinamente. Foi identificado que a interrupção foi causada por um ataque de negação de serviço distribuído (DDoS) utilizando pacotes ICMP. O impacto incluiu a indisponibilidade total dos serviços de rede por duas horas, interrompendo operações essenciais. Para mitigar o ataque, a equipe de segurança bloqueou os pacotes ICMP, desativou serviços não críticos e restaurou os serviços essenciais.

**Identificar**

1. **Ativos e Tecnologias Afetados:**
   * Hardware: Firewall com configuração inadequada.
   * Software: Sistemas de rede comprometidos.
   * Ativos: Recursos de rede indisponíveis.
2. **Processos/Negócios Impactados:**
   * Operações de Web design, design gráfico e marketing de mídias sociais ficaram paralisadas.
3. **Pessoas Afetadas:**
   * Funcionários e clientes sofreram impactos pela indisponibilidade dos serviços.

**Proteger**

1. **Ações Imediatas:**
   * Implementação de uma nova regra no firewall para limitar a taxa de pacotes ICMP.
   * Bloqueio de endereços IP falsificados nos pacotes ICMP recebidos.
2. **Políticas e Procedimentos:**
   * Revisão e atualização das políticas de configuração do firewall.
   * Treinamento para a equipe sobre boas práticas de segurança cibernética.
3. **Tecnologias de Proteção:**
   * Aquisição e implementação de sistemas IDS/IPS para filtrar pacotes ICMP suspeitos.
   * Adição de software de monitoramento de rede para detectar padrões anômalos.

**Detectar**

1. **Ferramentas de Monitoramento:**
   * Implementação de um sistema SIEM para correlacionar eventos e gerar alertas.
   * Uso de logs do firewall para monitorar tráfego ICMP.
2. **Análise Contínua:**
   * Estabelecimento de alertas para picos anormais de tráfego ICMP.
   * Auditorias regulares para revisar logs de atividade.
3. **Processos de Detecção:**
   * Configuração de sistemas IDS para identificar padrões de ataques semelhantes.

**Responder**

1. **Plano de Ação:**
   * Contenção imediata do ataque bloqueando o tráfego ICMP no firewall.
   * Desativação temporária de serviços não críticos para reduzir o impacto.
2. **Comunicação:**
   * Notificação da equipe de gestão e comunicação com os funcionários afetados.
   * Registro do incidente para comunicação futura com clientes e autoridades, caso necessário.
3. **Análise e Melhoria:**
   * Realização de uma análise pós-incidente para identificar pontos fracos.
   * Atualização do plano de resposta a incidentes para incluir cenários de ataques ICMP.

**Recuperar**

1. **Recuperação de Sistemas:**
   * Restauração completa dos serviços de rede após a contenção do ataque.
   * Validação de configurações atualizadas no firewall.
2. **Melhorias:**
   * Implementação de backups regulares para garantir a disponibilidade de dados.
   * Testes de estresse periódicos para avaliar a resiliência da infraestrutura de rede.
3. **Comunicação:**
   * Relatório final compartilhado com as partes interessadas, incluindo lições aprendidas.
   * Comunicação com clientes afetados, garantindo transparência e medidas preventivas.

**Aplicação do Framework NIST CSF**

1. **Identificar:**
   * Mal-atores lançaram um ataque ICMP flood contra a organização.
   * Identificação de vulnerabilidades no firewall e serviços impactados.
2. **Proteger:**
   * Configurações aprimoradas no firewall e implementação de IDS/IPS.
   * Procedimentos para limitar tráfego ICMP e treinamento de equipe.
3. **Detectar:**
   * Sistemas de monitoramento e logs para identificar tráfego anômalo.
   * Estabelecimento de alertas para padrões suspeitos.
4. **Responder:**
   * Bloqueio de tráfego malicioso e isolamento de sistemas afetados.
   * Análise de logs para rastrear a origem e avaliar o impacto do ataque.
5. **Recuperar:**
   * Restauração gradual de serviços essenciais.
   * Implementação de medidas para reduzir impacto em eventos futuros.

**Notas e Reflexões:** A aplicação da estrutura NIST CSF proporcionou uma abordagem estruturada e eficaz para lidar com o incidente. A integração de ferramentas de monitoramento e proteção fortaleceu a segurança da rede. Além disso, o uso de análises pós-incidente e melhorias contínuas aumenta a resiliência organizacional e contribui para uma resposta mais rápida e precisa a possíveis ataques futuros. Este modelo será uma base essencial para fortalecer o planejamento de segurança cibernética da organização.