Incident report analysis

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

Summary	Um ator malicioso se aproveitou de um firewall mal configurado para fazer um ataque de DoS que comprometeu, por 2 horas, serviços de Web design, design gráfico e soluções de marketing de mídia social da empresa, causando prejuízos financeiros. A equipe de resposta a incidentes respondeu bloqueando a entrada de pacotes ICMP, interrompendo todos os serviços de rede não críticos off-line e restaurando os serviços de rede críticos.
Identify	A equipe de segurança investigou o incidente e percebeu que diversas solicitações ICMP externas à rede passaram por um firewall que não estava corretamente configurado para lidar com esse protocolo, criando uma vulnerabilidade que resultou no sucesso do ataque ocorrido. As diversas solicitações sobrecarregaram os servidores, interrompendo os serviços de Web design, design gráfico e soluções de marketing de mídia social e impedindo que funcionários trabalhassem em entregas para os clientes da empresa.
Protect	Visando prevenir que esse tipo de ataque ocorra de novo futuramente, a equipe de segurança implementou uma nova regra de firewall para limitar a taxa de entrada de pacotes ICMP, a verificação do endereço IP

	de origem no firewall para verificar se há endereços IP falsos nos pacotes ICMP recebidos, um software de monitoramento de rede para detectar padrões de tráfego anormais e um sistema IDS/IPS para filtrar tráfego ICMP com base em características suspeitas
Detect	Para detectar novos ataques de ICMP no futuro, a equipe de segurança irá monitorar pacotes de ICMP que circulam a rede, especialmente os vindos de fora da rede interna, além de verificar os que estão entrando para fiscalizar a eficiência dos filtros configurados no firewall e do sistema IDS/IPS implementado.
Respond	A equipe configurou o firewall vulnerável corretamente e aplicou novos sistemas para filtrar o tráfego que entra na rede. Outros firewalls também tiveram suas configurações revisadas para se adequar às novas regras quanto a pacotes ICMP na empresa. Os clientes serão comunicados de que poderá haver algum atraso nas entregas devido ao incidente que ocorreu na empresa, e também que isso já foi resolvido e devidamente tratado para evitar que aconteça novamente.
Recover	Os serviços afetados foram restaurados seguindo a ordem de prioridade e testados para comprovar a volta do seu funcionamento correto. Regras de firewall foram revisadas. Estabelecemos um monitoramento reforçado pelas próximas 48h para detectar qualquer tentativa de re-ataque. Por fim, será elaborado um relatório de Lições Aprendidas para atualizar o Plano de Continuidade de Negócios da empresa, garantindo que o tempo de inatividade em eventos futuros seja inferior às 2 horas registradas neste incidente.

Reflections/Notes: