Análisis del informe del incidente

Resumen	La empresa experimentó un evento de seguridad cuando todos los servicios de red dejaron de responder repentinamente. El equipo de ciberseguridad descubrió que la interrupción fue causada por un ataque de denegación de servicio distribuido (DDoS) a través de una inundación de paquetes ICMP entrantes. El equipo respondió bloqueando el ataque y deteniendo todos los servicios de red no críticos, para que los servicios de red críticos pudieran restaurarse.
Identificar	Un agente o unos agentes de amenaza atacaron la empresa con un ataque de inundación ICMP. Toda la red interna se vio afectada. Todos los recursos críticos de la red necesitaban asegurarse y restaurarse a un estado funcional.
Proteger	El equipo de ciberseguridad implementó una nueva regla en el firewall para limitar la tasa de paquetes ICMP entrantes y un sistema IDS/IPS para filtrar parte del tráfico ICMP basado en características sospechosas.
Detectar	El equipo de ciberseguridad configuró la verificación de la dirección IP de origen en el cortafuegos (firewall) para comprobar si había direcciones IP falsas en los paquetes ICMP entrantes, e implementó un software de monitoreo de red para detectar patrones de tráfico anormales.
Responder	Para futuros eventos de seguridad, el equipo de ciberseguridad aislará los sistemas afectados para evitar nuevas interrupciones en la red. Intentarán restaurar cualquier sistema y servicio crítico que hubiera sufrido una interrupción a causa del evento. Luego, el equipo analizará los registros de la red para verificar si hay actividad sospechosa y anormal. También informará sobre todas las incidencias a la alta dirección y a las autoridades legales correspondientes, si procede.

Recuperar	Para recuperarse de un ataque DDoS por inundación de ICMP, el acceso a los servicios de red debe restaurarse a un estado de funcionamiento normal. En el futuro, los ataques de inundación ICMP externos podrán bloquearse en el firewall. En ese momento, todos los servicios de red no críticos deben detenerse para reducir el tráfico de red interno. A continuación, lo primero será restaurar los servicios de red críticos. Finalmente, una vez que el flujo de paquetes ICMP haya agotado el tiempo de espera, todos los sistemas y servicios de red no críticos podrán volver a estar en línea.

Reflexiones/Notas: