Usa el Marco de Ciberseguridad del NIST para responder a un incidente de seguridad

Informe de análisis de incidentes

Resumen del incidente	La empresa multimedia sufrió un **ataque de denegación de servicio distribuido (DDoS)** que comprometió la red interna durante dos horas. El ataque fue causado por una avalancha de paquetes ICMP entrantes, lo que provocó que los servicios de red de la empresa dejaran de responder. El equipo de gestión de incidentes mitigó el ataque bloqueando los paquetes ICMP entrantes, deteniendo los servicios no críticos y restableciendo los servicios críticos. La investigación reveló que la vulnerabilidad explotada fue un firewall mal configurado que permitió el flujo descontrolado de tráfico ICMP.
Identificación	**Riesgo de seguridad**: El ataque fue posible debido a la falta de configuraciones adecuadas en el firewall que permitieron una sobrecarga de tráfico ICMP, saturando la red. Esto se clasificó como un ataque DDoS. **Activos afectados**: • Los servidores y dispositivos de red internos de la empresa, los cuales dejaron de responder. • Los servicios de diseño web y gráfico quedaron inoperativos, afectando a los clientes que dependían de estos servicios.

	Personas: Los administradores de red y el equipo de seguridad son responsables de la configuración y mantenimiento del firewall y la infraestructura de red.
Protección	**Medidas de protección implementadas:** 1. **Configuración adecuada del firewall**: Se configuró una regla de firewall para limitar la tasa de paquetes ICMP entrantes y verificar la autenticidad de las direcciones IP de origen para evitar suplantaciones. 2. **Software de monitoreo:** Se implementó software de monitoreo de tráfico para detectar patrones anómalos y responder de manera proactiva ante tráfico sospechoso. 3. **Sistemas IDS/IPS:** Un sistema de detección y prevención de intrusiones (IDS/IPS) fue instalado para filtrar el tráfico ICMP y bloquear comportamientos anómalos. 4. **Política de acceso**: Reforzar las políticas de acceso a nivel de red, asegurando que solo usuarios y dispositivos autorizados puedan enviar paquetes a la red interna.
Detección	**Sistemas de detección implementados**: 1. **Monitoreo continuo**: El software de monitoreo permite detectar patrones de tráfico anómalos, como una sobrecarga de paquetes ICMP, en tiempo real. 2. **Registro y alertas**: Se configuraron herramientas de registro de firewall para generar alertas automáticas en caso de que se detecten picos inusuales de tráfico, especialmente en protocolos como ICMP. 3. **Análisis de eventos**: El sistema IDS/IPS analizará los paquetes entrantes,

	buscando comportamientos sospechosos que puedan indicar la presencia de ataques DDoS o suplantación de IP.
Respuesta	**Plan de respuesta al incidente**: 1. **Contención**: En caso de un ataque similar, los paquetes ICMP serían bloqueados inmediatamente en el firewall para evitar la saturación de la red. 2. **Neutralización**: Los servicios no críticos serían detenidos para dar prioridad a los servicios esenciales mientras se investiga la naturaleza del ataque. 3. **Análisis post-incidente**: El equipo de seguridad realizaría un análisis exhaustivo de los registros de red y tráfico para determinar el origen del ataque y la magnitud de la intrusión. 4. **Comunicación interna**: Se comunicaría de manera inmediata al equipo técnico y a la alta dirección sobre el ataque y las acciones tomadas para mitigar el daño. 5. **Mejoras continuas**: Después del análisis, se implementarían mejoras en las configuraciones de firewall y otros sistemas de seguridad para evitar ataques futuros.
Recuperación	**Plan de recuperación**: 1. **Restauración de servicios**: Restablecer todos los servicios críticos afectados una vez que la amenaza haya sido mitigada. 2. **Recuperación de datos**: Verificar la integridad de los sistemas y asegurarse de que no haya corrupción de datos como resultado del ataque. Si es necesario, restaurar los datos desde las copias de seguridad más recientes.

	3. **Comunicación post-incidente**: Informar a los clientes sobre el incidente y las medidas tomadas para proteger los servicios en el futuro, asegurando transparencia. 4. **Mejoras a futuro**: Revisar las políticas de recuperación para asegurarse de que sean más eficientes en incidentes futuros, así como realizar simulaciones periódicas de ataques DDoS para evaluar la preparación.

Reflexiones y nota:

El ataque DDoS podría haberse evitado con configuraciones más estrictas en el firewall. La implementación de un sistema IDS/IPS robusto y de un monitoreo continuo es esencial para detectar anomalías tempranamente. A largo plazo, la capacitación del personal en la identificación de amenazas y la simulación periódica de ataques ayudarán a fortalecer la postura de seguridad de la empresa. La documentación y mejora continua de las políticas de respuesta y recuperación son claves para minimizar los impactos de futuros incidentes.