**Incident report analysis**

| **Summary** | En resumen, la empresa se dedica a realizar o dar servicios para diseño web, gráfico y soluciones de Marketing en redes sociales a pequeñas empresas. La empresa ha sufrido un ataque DDoS que pone en peligro la integridad de la red privada del negocio. Este ataque ha durado dos horas y se ha basado en el método de inundación de solicitudes ICMP mediante el uso de varios dispositivos para realizar el proceso. Los atacantes pudieron sobrepasar las medidas de seguridad impuestas por el firewall no configurado. Finalmente el departamento IT respondió bloqueando los paquetes ICMP entrantes, deteniendo todos los servicios de red no críticos fuera de línea y restableciendo los servicios de red críticos. | | |
| --- | --- | --- | --- |
| Identify | El tipo de ataque tratado, es un ataque DDoS. Un ataque DDoS se realiza desde varios equipos infectados por un software malicioso y una vez estos están en posesión del atacante comienzan a realizar solicitudes al servidor al que realizan el envío masivo. En este caso se tratará de una botnet que se dedica a enviar solicitudes ICMP y así poder penetrar la red interna saltando controles de seguridad al no estar correctamente operativos.  El firewall de la empresa ha quedado fuera de lugar debido a que no estaban definidas unas reglas de seguridad para este tipo de ataques. Los servicios que han quedado fuera de línea han provocado que no se pudiera acceder a ningún recurso de la red.  Las personas trabajadoras como especialistas en marketing, diseñadores web, creadores de contenido para redes sociales no han podido acceder a los recursos en red de la empresa. | | |
| Protect | Definiremos un conjunto de reglas para mitigar estos tipos de amenazas o vulnerabilidades.   * Controlar las conexiones y solicitudes a nuestros firewall de seguridad mediante reglas actualizadas y evitar cualquier tipo de vulnerabilidad en la red. Por eso estos dispositivos deben tener una configuración correcta. * Accesos y permisos. Saber dividir los permisos y accesos entre los usuarios puede ser un punto a favor para no encontrar cambios en configuraciones de red por usuarios que no están habilitados para ello. * Segmentación de la red. Es importante que nuestra red sea dividida por departamento para evitar que los ataques de red interna afecten a toda la empresa y no a un punto en específico. Para ello, la segmentación de la red es muy importante ya que, organizar nuestra red interna y focalizar los puntos de ataque para poderlos contener evitaremos que el atacante pueda moverse las diferentes secciones de la empresa. * SIEM Tools. El uso de herramientas con panel de control y métricas podrá ayudarnos a mitigar las vulnerabilidades y detener o evadir ataques justo a tiempo. Observar el funcionamiento y comportamiento de nuestros equipos es muy importante para evitar sucesos que podrían costar la economía o reputación de la empresa. * Implementación IPS. Una buena opción sería colocar un dispositivo IPS detrás del firewall correctamente configurado en conjunto para en caso de detección de paquetes que son amenaza para la red puedan ser mitigados por este dispositivos. | | |
| Detect | El equipo de IT, revisa la configuración y la verificación de las IP para que no sean falseadas por los atacantes y saltar las reglas del firewall. | | |
| Respond | Para responder a estos ataques en un futuro, configuraremos reglas y un dispositivo IPS para evitar saltos de reglas de seguridad y mitigar las vulnerabilidades y accesos no controlados.  Las fugas de seguridad de la red, serán comunicadas con los trabajadores y los correspondientes departamentos de la red. Por otro lado, estos hechos deben ser comunicados a las autoridades responsables como;   * Agencia Española de Protección de Datos (AEPD) * Cuerpo Nacional de Policía o Guardia Civil (Brigada de Delitos Tecnológicos) * Centro Criptológico Nacional (CCN-CERT)   Si tenemos un incidente de la misma magnitud deberemos actuar con rápidez centrándonos en el foco del que provienen las vulnerabilidades para poner en cuarentena los dispositivos afectados para que queden limpios y listos, y poder ponerlos en marcha en el menor tiempo posible. Es importante tener en cuenta que la empresa debe funcionar con normalidad cuanto antes.  Una respuesta inmediata protegerá la empresa en confidencialidad, integridad y disponibilidad de los datos. | | |
| Recover | Analizaremos el tráfico de red detectando la IP afectada y los paquetes de datos enviados a los dispositivos de la red. Forzaremos la autenticación de las IP y segmentamos la red en diferentes VLAN dependiendo el departamento en el que estemos, estableciendo rangos de IP por cada una de las VLAN. Haremos un seguimiento de la IP de origen que nos ataca y comunicaremos a las autoridades las acciones del individuo. | | |

| Reflections/Notes: Gracias a las cinco fases de los estándares NIST CSF, hemos podido realizar un seguimiento del proceso sobre cómo dar respuesta a incidentes de seguridad. Completar estas fases es muy importante para la recuperación y protección de los datos de la organización. |
| --- |