Basque CyberSecurity Centre

Respuesta a ataques DDOS

Checklist

- ☐ Al tratarse de un hecho que pudiera ser constitutivo de delito, interponer la correspondiente denuncia en la comisaría más cercana o notificarlo ante la Sección Central de Delitos en Tecnologías de la Información (SCDTI) enviando un correo electrónico a di@ertzaintza.eus para que tomen las medidas oportunas.

- ☐ Registrar la información relacionada con el ataque, como los flujos de red, o los registros de los servidores y sistemas de seguridad. Estos datos son importantes para un análisis posterior y para poder denunciar los hechos.

- ☐ Asegurarse de poder mantener abierto algún canal de comunicación, como un sitio web en el que pueda proporcionar a los clientes información y datos de contacto alternativos (teléfono, fax, correo electrónico).

- ☐ Analizar el ataque y establecer una estrategia de defensa:

  - ☐ Si el ataque se origina en un número limitado de direcciones IP, puede ser suficiente filtrar estas direcciones en el router o los sistemas de seguridad. Si el volumen de datos excede el ancho de banda disponible, puede ser necesario contactar con su proveedor de servicios de Internet (ISP).

  - ☐ Si la mayor parte de los accesos legítimos a los recursos atacados se encuentran en países específicos, el bloqueo por geolocalización puede ser muy eficaz. Sin embargo, hay que tener en cuenta que algunos usuarios legítimos pueden ser bloqueados.

  - ☐ En el caso de inundaciones SYN, UDP, BGP y SNMP las direcciones IP de origen del ataque pueden ser falsas, por lo que en estos casos no tiene sentido filtrar las direcciones IP, e incluso podría bloquear a usuarios legítimos. En este caso deberá trabajar junto con el ISP para encontrar una solución, desviando y filtrando este tráfico.

- ☐ El ataque podría evolucionar evadiendo las medidas de defensa implementadas. En estos casos habrá que volver a analizar la situación y tomar las contramedidas adecuadas.

Para conocer más información sobre cómo protegerte puedes visitar **https://www.basquecybersecurity.eus/es/**

Si necesitas asesoramiento profesional, puedes consultar el catálogo de proveedores de ciberseguridad de Euskadi disponible en la web.