Denegación de servicio

- **Descripción de la amenaza.**

  La denegación de servicio es un ataque con el propósito de interrumpir el correcto funcionamiento de una máquina o red, dejándola inaccesible para los usuarios. Los atacantes consiguen el objetivo mediante la inundación del objetivo con tráfico de red, o enviando información que provoca la caída del servicio.

  Las víctimas habituales de ataques DoS son servidores web de organizaciones importantes como las bancarias, de comercio, medios de comunicación y gubernamentales. Aunque los ataques DoS normalmente no resultan en el robo o la pérdida de información importante u otros recursos, sí que pueden costar a la víctima una gran cantidad de dinero y tiempo para solucionar el problema.

  Hay 2 métodos geneales de realizar un ataque DoS: inhunda servicios o provocar un "crash" del servicio. Los ataques de inhundación ocurren cuando el sistema recive demasiado tráfico, causando que se ralentize e incluso deje de funcionar al completo.

  Los ataques de inundación populares son:

  - **Ataques de buffer overflow**: es el ataque DoS más común. El concepto consiste en enviar más tráfico a una dirección de red del que los programadores del sistema establecieron en su momento como tráfico previsto. Incluye los otros tipos de ataque, además de otros que están diseñados para abusar bugs específicos de ciertas aplicaciones o redes.

  - **Inhundación ICMP**: se aprovecha de los dispositivos de red mal configurados mediante el envío de paquetes falsificados que realizan un ping a cada sistema de la red de destino, en lugar de solo a una máquina específica. Esto provoca que la red se active para amplificar el tráfico. Este tipo también se conoce como ataque smurf o ping de la muerte.

  - **Inhundación SYN**: envía una petición para conectarse a un servidor, pero nunca completa el *handshake.* Continúa hasta que todos los puertos están saturados con peticiones y ninguno está disponible para que se conecten a él los usuarios legítimos.

- **Riesgos que supone.**

  - **Falta de disponibilidad**: los usuarios legítimos podrían no tener acceso a los recursos a los que esperan acceder y no serán capaces de encontrar la información que necesitan o llevar acabao las acciones que requerían.

  - **Pérdidas económicas**: la organización afectada podría no ser capaz de continuar con alguna de sus actividades críticas, sobretodo aquellas que requieren ser ejecutadas rápidamente. Por otra parte, para solucionar el problema, los empleados de TI de la empresa podrían ser necesitados durante un tiempo extra al habitual, resultando en más costes.

  - **Reputación afectada**: cuando ocurre un incidente de este tipo, la imagen de la empresa se ve afectada negativamente y esto puede afectar a la relación con los clientes.

  - **Pérdida de clientes**: los clientes, al conocer la existencia de un ataque de este tipo, podrían optar por escoger a un competidor de la empresa afectada para llevar acabo los servicios que requieren de ahora en adelante.

- **Medidas correctivas.**

  - **Adquisión de un nuevo producto:** adquisión de software y hardware de monitorización y análisis de tráfico de red. Se debería supervisar el tráfico mediante sistemas IDS (Intrusion Detection System). Los administradores de red deben establecer reglas para crear alertas para tráfico inusual, identificar las fuentes del tráfico y descartar paquetes de red que encajen con un criterio decidido.

  - **Contratación de un nuevo servicio:** contratar servicio cloud para los sistemas más críticos. El cloud generalmente proporciona más ancho de banda que los recursos on-premise y la naturaleza del cloud significa que muchos servidores no estarán situados en el mismo espacio físico, de esta manera es más difícil para el atacante interrumpir el correcto funcionamiento de los sistemas de información de la organización.

  - **Ejecución de un cambio interno:** establecer un plan de respuesta ante un ataque DoS. Debe incluir aspectos de comunicación, mitigación y recuperación. Se debe practicar de manera simulada en lugar de esperar a que ocurra un ataque real.