MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

GOBIERNO DE COSTA RICA

GUÍA DE ACCIÓN ANTE INCIDENTES DE DENEGACIÓN

PROCESO DE GESTIÓN DE INCIDENTES

Octubre - 2023

TABLA DE CONTENIDO

Concepto de Denegación de Servicio: ataque cibernético diseñado para sobrecargar un sistema, servicio o red, impidiendo que los usuarios legítimos accedan o utilicen los recursos.

Detalles: el objetivo principal de estos tipos de ataque es reducir o anular la capacidad de servidores o recursos informáticos para ofrecer su servicio.

Los ataques de denegación de servicio pueden originarse de dos formas:

- ✓ **DoS (Denial of Service):** ataques llevados a cabo por un solo dispositivo o dirección IP.
- ✓ **DDoS (Distributed Denial of Service):** ataques que involucran múltiples dispositivos o direcciones IP, lo que dificulta su mitigación y bloqueo. Los atacantes utilizan una gran cantidad de dispositivos comprometidos, conocidos como "botnets", para enviar un flujo masivo de solicitudes o tráfico al objetivo. Estos dispositivos son típicamente computadoras, servidores o dispositivos IoT que han sido infectados con malware y controlados por los atacantes sin el conocimiento de sus propietarios.

Entre los tipos de ataques de denegación de servicio más comunes se incluyen:

- ✓ **Ataques de saturación de ancho de banda:** los atacantes inundan el objetivo con un volumen masivo de tráfico, agotando el ancho de banda disponible y dejando poco o ningún espacio para el tráfico legítimo.

- ✓ **Ataques de agotamiento de recursos:** los atacantes explotan vulnerabilidades en el software o configuración del objetivo para consumir todos sus recursos, como CPU, memoria o conexiones, hasta que el sistema se colapse.
- ✓ **Ataques de capa de aplicación:** los atacantes apuntan a vulnerabilidades específicas en aplicaciones y servicios, enviando solicitudes maliciosas o tráfico falso para agotar los recursos del servidor o provocar errores que afecten su disponibilidad.
- ✓ **Ataques de amplificación:** los atacantes utilizan servicios mal configurados para enviar paquetes más grandes de lo necesario como respuesta a solicitudes más pequeñas, amplificando la cantidad de tráfico dirigido al objetivo.

Impacto: este tipo de ataques pueden causar pérdidas económicas, interrumpir la disponibilidad y el funcionamiento de servicios en línea, afectar la reputación de una organización o distraer a los equipos de seguridad mientras se llevan a cabo otros ataques más sofisticados.

1. Fase de Identificación

El objetivo de esta fase es tener la capacidad de identificar o detectar cualquier ciber incidente que pueda sufrir un organismo o entidad, y notificarlo a la brevedad para tomar acciones ante el incidente.

El objetivo de esta fase es tener la capacidad de identificar o detectar cualquier ciber incidente que pueda sufrir un organismo o entidad, y notificarlo a la brevedad para tomar acciones ante el incidente.

- ✓ Utilizar herramientas de monitoreo de red y tráfico para detectar patrones de tráfico inusuales o sospechosos que puedan indicar un ataque de denegación de servicio.
- ✓ Confirmar si el aumento del tráfico o las solicitudes es el resultado de un ataque de denegación de servicio y no de un evento legítimo o un pico de tráfico normal.
- ✓ En caso de tener la certeza de estar sufriendo un DoS o DDoS, se recomienda:
    - Notificar al equipo de seguridad y a los responsables del sistema o servicio afectado sobre la detección del ataque.
    - Comunicar internamente a los equipos pertinentes, como el equipo de tecnología de la información, para coordinar la respuesta y garantizar una acción rápida.

- En caso de disponer de procedimientos de gestión de crisis y continuidad de negocio, considerar la posibilidad de activarlos.

2. Fase de Contención

La máxima prioridad en esta fase es contener el impacto negativo que el ataque, de DoS o DDoS, está causando sobre la organización para restablecer la continuidad normal.

Evaluación de la situación:

- ✓ Recabar toda la información posible sobre el ataque: o Identificar el tipo de ataque de denegación de servicio que se está llevando a cabo.
  - ✓ Determinar si se es un objetivo principal o, por el contrario, una víctima colateral del ataque.
  - ✓ Determinar el alcance del incidente y si otros sistemas o dispositivos se encuentran siendo afectados.
  - ✓ Evaluar el impacto en los recursos y el rendimiento de los distintos componentes de red de la organización (router, firewalls, servidores y aplicaciones).
  - ✓ Recopilar y analizar el tráfico entrante en búsqueda de patrones que permitan diferenciar el tráfico malicioso del bueno, teniendo en cuenta los siguientes elementos:
    - IP de origen

- IP destino
- Puerto
- Protocolo

✓ Fecha y hora del tráfico, incluyendo información de la zona horaria

✓ Comprobar la repercusión en los medios de comunicación:

- Determinar el alcance del ataque.
- Concretar la cantidad de servicios a los que afecta públicamente.
- Estipular el impacto y cómo afecta a la organización.
- Recabar toda la información externa posible en búsqueda de alguna reivindicación o posible autoría.

✓ Documentar y recopilar evidencias del ataque, como registros de tráfico, registros de firewall y otros datos relevantes para fines de investigación y posibles acciones legales.

✓ Realizar copias de respaldo de la evidencia recopilada para su posterior análisis y referencia.

Contención

- ✓ Ampliar recursos en la medida de lo posible y aplicar restricciones para tratar de paliar el impacto del ataque.
- ✓ Ponerse en contacto con el ISP para evaluar qué medidas tomar y activar un ancho de banda de emergencia temporalmente.

3. Fase de Mitigación

Una vez recopilada y analizada la información obtenida en la fase de contención, deben tomarse medidas reactivas para gestionar el incidente.

- ✓ En caso de tratarse de un ataque en el que las medidas a tomar dependen del ISP, contactar con éste para solicitar que tomen las acciones necesarias y realizar un seguimiento sobre la efectividad de las medidas. Coordinar con el ISP para filtrar el tráfico malicioso antes de que llegue a la red de la organización.
- ✓ En el caso de que el ataque pueda gestionarse mediante los recursos internos de la organización:
    - Configurar las listas de control de acceso (ACL) del Router frontera.
    - Filtrar el tráfico malicioso.

- Configurar reglas de firewall para bloquear o filtrar el tráfico malicioso proveniente de las direcciones IP identificadas como atacantes.
- Activar medidas ante ataques “SYN flood”.
- Deshabilitar los puertos que no sean necesarios.
- Restringir el acceso a la aplicación para mantener la continuidad del negocio y evitar cuellos de botella. Si es necesario, implementar una red de entrega de contenidos (CDN).
- Implementar soluciones de monitoreo de tráfico y análisis de registros para seguir de cerca la evolución del ataque y ajustar las medidas de mitigación según sea necesario.

✓ Establecer comunicación con los usuarios afectados, mediante el uso de medios alternativos, para informarles sobre el ataque.

4. Fase de Recuperación

La finalidad de la fase de recuperación consiste en devolver el nivel de operación a su estado normal y que las áreas de negocio afectadas puedan retomar su actividad. Es importante buscar cualquier signo de actividad sospechosa en los servicios afectados y monitorizarlos temporalmente.

✓ Restablecer los servicios afectados y comprobar el correcto funcionamiento.

- ✓ Realizar un comunicado externo sobre los hechos, con el fin de controlar la repercusión inmediata del incidente.
- ✓ Si se identifica la autoría del ataque, contactar con el equipo jurídico para tomar las acciones legales pertinentes.
- ✓ Implementar medidas para fortalecer la resiliencia y prevenir futuros ataques de denegación de servicio.

5. Fase Post- Incidente

Una vez que el ciber incidente está controlado y la actividad ha vuelto a la normalidad, es necesario reflexionar sobre lo sucedido, analizando las causas del problema, cómo se ha desarrollado la actividad durante la gestión del ciber incidente y todos los problemas asociados a la misma.

La finalidad de este proceso es aprender de lo sucedido y que se puedan tomar las medidas adecuadas para evitar que una situación similar se pueda repetir, además de mejorar los procedimientos.

6. Lecciones aprendidas

Una vez que el ciber incidente está controlado y la actividad ha vuelto a la normalidad, es necesario reflexionar sobre lo sucedido, analizando las causas del problema, cómo se ha desarrollado la actividad durante la gestión del ciber incidente y todos los problemas asociados a la misma.

- ✓ Realizar una revisión exhaustiva del incidente para identificar las lecciones aprendidas y las áreas de mejora en la detección y mitigación de este tipo de ataques.
- ✓ Realizar un informe del ciber incidente que detalle su causa y coste (especialmente, en términos de compromiso de información o de impacto en los servicios prestados), así como las medidas que la organización debe tomar para prevenir futuros incidentes de naturaleza similar.
- ✓ Actualizar las políticas y las medidas de seguridad para fortalecer la resiliencia de la organización contra futuros ataques similares.

7. Diagrama de flujo