Fundamentos de la Gestión de Incidentes

La gestión de incidentes existe como consecuencia de la gestión de la seguridad. ES el proceso para detectar, reportar, valorar, respoder a, tratar con y responder a los incidentes de seguridad. Hay que ser capaz de ver que se está sufriendo un incidente y actuar para eliminarlo o reducirlo. La parte más importante es aprender de los incidentes para saber como reaccionar a futuro o crear contramedidas para estos incidentes. El objetivo es ver que todos los eventos de seguridad e identificar si son maliciosos o no. La gestión de incidentes tiene un enfoque reactivo para manejar incidentes de seguridad.

CSIRT vs CERT

- CSIRT: Equipo de respuestas a incidentes de seguridad en computadores (Mercado Europeo)
- CERT: Equipo de respuesta a incidentes en computadores (Mercado Estadounidense)

Incidente de seguridad

Cualquier evento importante que se produzca de forma intencional o accidentada. Hay varios tipos:

- Contenido abusivo
- Contenido malicioso o malware
- Obtención de información
- Acceso indebido o intrusión
- Disponibilidad
- Seguridad/confidencialidad
- Fraude
- Helpdesk
- Otros

Las amenazas pueden proceder de:

- Crimen organizado
- Agentes gubernamentales
- Hacktivismo
- Amenaza interna

Clasificación de incidentes

- Gravedad: Daño originado a la organización y el caracter de urgencia del mismo
- Orden de prioridad por incidencia.

Respuesta a un incidente

- Controlar y minimizar cualquier tipo de de daño a la organización.
- Coordinar actividades para una recuperación rápida
- Preservación de la evidencia: Logs y evidencias necesarias para trazar los movimientos del atacante.
- Prevenir eventos similares en el futuro, registrando las lecciones aprendidas de estos eventos.
- Compartir información relacionada con estos incidente con otros CSIRT.

Ciber-Resilencia

Capacidad de una organización para resistir ataques y mantenerse en pié. Capacidad de una organización de mantener sus servicios en caso de ataque.

- A nivel europeo,la ENISA (Agencia de Seguridad de las Redes y de la Información de la Unión Europea) creo un programa para mejorar la ciber-resilencia de los estados miembros.
- En 2013 se crea la Estrategia de Ciberseguridad Nacional (ESN)
- También existe un acuerdo entre el ministerio de interior y el ministerio de industria para proteger Infraestructuras Críticas a través del CNPIC (Centro Nacional de Protección de Infraestructuras Críticas).
    - Se apoya en el INCIBE, el CCN y las fuerzas y cuerpos de seguridad del estado.
    - Busca la protección de todas las infraestructuras críticas y servicios esenciales del pais.
- El CCN-CERT es el CERT regulador del Esquema Nacional de Seguridad (ENS), ofreciendo guías, recomendaciones y herramientas para proteger las administraciones públicas.
    - Dispone de guías y medidas para medir la ciber-resilencia de las adminsitraciones públicas.
    - INES: Cuadro de mando donde las adminsitraciones públicas vuelcan el estado de la seguridad, de este volcado se saca un informe con un mapa de estado de las organizaciones.