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.

Estrategia de la Unión Europea en cuanto a la ciberseguridad

- Ciber-resilencia
- Reducción drástica de la delincuencia en la red
- Desarrollo de una política de ciberdefensa
- Desarrollo de recursos industriales y tecnológicos necesarios en materia de ciberseguridad
- Establecimiento de una política internacional coherente del ciberespacio de la Unión Europea y la promoción de los valores europeos esenciales.

Organismos de Seguridad en España

- INCIBE (Antes INTECO): Organismo de seguridad dependiende del ministerio de economía y empresa, se encarga de pymes y ciudadanos.
- CNPIC (Centro Nacional para la protección de infraestructuras crítcias)

- CCN (Centro Criptológico nacional): Se encarga de la ciberseguridad de las administraciones públicas y empresas estratégicas
- Mando conjunto de ciberdefensa
- CERT Autonómicos
- Grupo de delitos telemáticos de la guardia civil
- Brigada tecnológica de la policia nacional
- AEPD (Agencia Española de Protección de Datos)

Organismos de gestión de incidentes

- CCN-CERT: Centro de coordinación de incidencias y alertas de seguridad para las administraciones públicas
- INCIBE CERT
- IRIS-CERT (Desaparecido): Para las universidades
- CERT-EU: Cert de la unión europea, coordina el resto de certs nacionales.

ISO27001 vs ISO27032

- 27001:
  - Ambito: global
  - Certificable: SI
  - Ibjetivo: ISMS
  - Activos: Proporciona un marco detallado para la identificación y clasificación de activos internos
  - controles: 93
  - Descripción de controles: breve descripción
- 27032:
  - Ambioto: Concreta y especóifica
  - Certificable: NO
  - Objetivo: Ciberseguridad
  - Activos
  - Controles
  - Descripción de controles: detallada

Tratamiento de los incidentes

- ISO27001:
  - Notificar los incidentes
  - Clasificar incidentes en base a su impacto y urgencia
  - Tratar los incidentes: ver como contenerlos, erradicarlos y mitigarlos
  - Cerrar los incidentes: Notificar al que abrió el incidente.
  - Registrar la información de lo que se aprende en los incidentes de seguridad.
  - Base de datos con los conocimientos

Especialidades en la respuesta a incidentes

- Análisis forense digital: Es necesario conocimiento de informatica forense para analizar los sistemas afectados
- Monitorización: Muy importante para la detección de incidentes de seguridad.
    - SIEM:
    - EDR (Endpoint Detection and Response)
- Threat Hunting: Un humano buscando problemas dentro de los logs de los sistemas. Puede llegar a encontrar cosas que igual no detecta un SIEM.
- Ciberinteligencia

Actividades contempladas en un Plan de Respuesta a Incidentes (PRI)

- Constitución de un equipo de respuesta a incidentes (IRT)
    - Denominado como CSIRT (Computer Security Incident Response Team)
    - Personas con experiencia y formación adecuada en desastres de ciberseguridad.
    - Medios técnicos y materiales necesarios para cumplir el objetivo
    - Simulacros periódicos
    - Presente únicamente en grandes organizaciones.
    - SOC vs CSIRT:
        - SOC: detección de comportamientos inseguros por parte de los usuarios
        - CSIRT: Control de incidentes
- Definición de guía de procedimientos
- Detección de un incidente de Seguridad
- Análisis del incidente
- Contención, erradicación y recuperación
- Identificación del atacante y posibles actuaciones legales
- Comunicación con terceros y relaciones públicas
- Documentación del incidente de seguridad
- Análisis y revisión a posteriori del incidente.