Breve descripción del CERT-UACh

Erick Rodríguez Arreola

Jefe del CERT-UACh

Definición

"Un equipo de respuesta a incidentes de seguridad informática es una entidad organizativa concreta (es decir, uno o más empleados) a la que se le asigna la responsabilidad de coordinar y apoyar la respuesta a un evento o incidente de seguridad informática. Los CSIRT se pueden crear para estados nacionales o economías, gobiernos locales, organizaciones comerciales, **instituciones educativas** e incluso entidades sin fines de lucro. El objetivo de un CSIRT es minimizar y controlar el daño resultante de los incidentes, proporcionar una guía efectiva para las actividades de respuesta y recuperación, y trabajar para evitar que ocurran incidentes futuros. "

Software Engineering Institute, Carnigie Mellon Univerity

Características

- Planificación y orden

- Minimizar el impacto de incidentes:
  - Ataques informáticos
  - Desastres naturales
  - Accidentes

QUÉ HACE UN CSIRT

Principales funciones

- Coordinar la implementación de estrategias de respuesta.
- Determinar impacto y alcance.
- Comprender las causas técnicas de eventos o incidentes.
- Investigar soluciones.

Principales funciones *(cont…)*

- Diseminar información acerca de riesgos informáticos.
- Colaborar y coordinar actividades con organizaciones externas.
- Mantener un repositorio de incidentes y vulnerabilidades.

PORQUÉ UNA INSTITUCIÓN EDUCATIVA DEBE CONTAR CON UN CSIRT

Motivos

Cuál es el interés de grupos delictivos en la información.

Incremento constante de ataques recibidos.

Incremento en la complejidad y técnicas utilizadas.

Motivos *(cont…)*

- Cumplimiento con normativas (ISO 27001).
- Cumplimiento con lineamientos internos.
- Gestión de incidentes.

TIPOS DE CSIRT

Tipos

CENTRO DE COORDINACIÓN

CSIRT NACIONAL

CSIRT INTERNO

CSIRT COMERCIAL (MANEJADOR DE INCIDENTES)

UNAM CERT

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

ccn-cert centro criptológico nacional

MNEMO

cert UACH

CÓMO OPERA UN CSIRT

Modelos

- Centralizado
- Distribuido
- Coordinador

CERT-UACh

CSIRT Interno

Modelo centralizado

Colaboración con otros CSIRT y organismos judiciales

cert UACH
Equipo de Respuesta a Incidentes de Seguridad Informática

Actividades en el CERT-UACh

- Revisión de registros de actividad
- Búsqueda de avisos importantes (actualizaciones, vulnerabilidades, etc.)
- Generación de comunicados

Actividades en el CERT-UACh *(cont…)*

Procedimiento de atención a incidentes.

Auditorías de seguridad.

Elaboración de guías y manuales.

Monitoreo de tráfico e infraestructura tecnológica.

Actividades en el CERT-UACh *(cont…)*

Interacción recurrente con la Policía Cibernética.

Apoyo a otros organismos.

Campañas de concientización sobre ciberseguridad.

Diplomado de Seguridad Informática.

COMO FORMAR UN CSIRT

Como formar un CSIRT

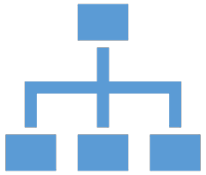
Definir el campo de operación:

Alcance

Tipo

Modelo

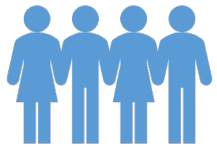
Misión, visión, objetivos



Conocer la organización.

Auditoría de seguridad inicial.

Como formar un CSIRT *(cont…)*



Selección y formación del personal.

Investigar acerca de normativas y regulaciones judiciales pertinentes.

Elaboración de procedimientos principales:

Gestión de incidentes

Gestión de vulnerabilidades

Reporte de incidentes

Como formar un CSIRT *(cont…)*

Definición de roles y tareas.

Cálculo de presupuesto y asignación de recursos para el inicio de operaciones.

Formalización del CSIRT:

Gestión ante instancias de registro como el CERT/CC, FIRST, entre otras.

Comunicación interna.

Generación de convenios con organismos externos.

DOCUMENTOS DE REFERENCIA

Links

https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2016/15551-EC/4B%201.pdf

https://resources.sei.cmu.edu/asset_files/WhitePaper/2007_019_001_294579.pdf

MUCHAS GRACIAS

ERICK RODRÍGUEZ ARREOLA
CERT-UACh
erick.rodriguez@uach.mx