CIMAT

CIMAT

Propuesta sobre aspectos de seguridad en un Equipo de Respuestas ante Emergencias Informáticas (CERT)

Centro de Investigación en Matemáticas

Maestría en Ingeniería de Software

ISC. Heltton Emmanuel Ramírez Luna

Índice

- Introducción
- Objetivos de un CERT
- Servicios de un CERT
- Propuesta
  - Difusión de información
  - Equipo Hardware
  - Sistemas de gestión de información y eventos de seguridad
  - Diagrama
  - Conclusiones y trabajos futuros

Índice

- **Introducción**
- Objetivos de un CERT
- Servicios de un CERT
- Propuesta
  - Difusión de información
  - Equipo Hardware
  - Sistemas de gestión de información y eventos de seguridad
  - Diagrama
  - Conclusiones y trabajos futuros

Introducción

- Un Equipo de Respuestas ante Emergencias Informáticas (CERT, por sus siglas en inglés) es una **organización** dedicada a dar respuesta a incidencias de seguridad en tecnologías de la información. Un CERT está conformado por **un grupo de expertos en seguridad de la información** la cual provee de servicios como alertas y advertencias, tratamiento de incidentes, observatorio de tecnología, auditorías de seguridad, cómputo forense, entre otros. Por lo tanto, **se hace uso de información sensible que deberá tener fuertes métodos de seguridad** tanto físicos como lógicos, es por eso que este artículo habla sobre **una propuesta en su primera etapa de desarrollo**, sin enfocarse a una tipología de CERT en especifico, sobre los aspectos de seguridad que debe tener un CERT abordando las áreas de **Difusión de Información, Equipo hardware y Sistemas SIEM** (Security Information and Event Management).

Índice

Objetivos de un CERT

- Cada usuario sufre 3.56 ataques por malware financiero
- En 2014 duplicaron los troyanos bancarios móviles
- Aumentaron los ataques a carteras bitcoin
- Especialistas en seguridad de las TICs apenas llegan a 1 millón

Índice

- Introducción
- Objetivos de un CERT
- **Servicios de un CERT**
- Propuesta
  - Difusión de información
  - Equipo Hardware
  - Sistemas de gestión de información y eventos de seguridad
  - Diagrama
  - Conclusiones y trabajos futuros

Servicios de un CERT

- Alertas y advertencias
- Tratamiento de incidentes
- Auditorías de seguridad
- Observatorio de tecnología
- Cómputo forense

Índice

- Introducción
- Objetivos de un CERT
- Servicios de un CERT
- Propuesta
  - **Difusión de información**
  - Equipo Hardware
  - Sistemas de gestión de información y eventos de seguridad
  - Diagrama
  - Conclusiones y trabajos futuros

Difusión de información

Acceso a internet

- Alineado a las políticas de gestión de la seguridad del CERT.
- Protección en tiempo real basado en Proxy.

Correo electrónico

- Utilizar el criptosistema PGP (pretty good privacy).
- Contar con un robusto sistema de email.

Página web

- Se podría dañar la reputación del CERT.
- Utilizar balanceo de cargas contra ataques DDOS.

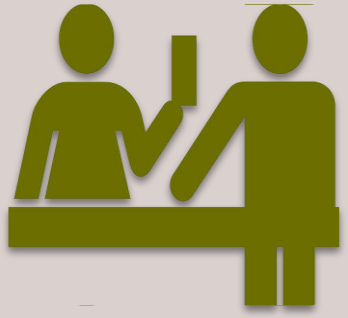
Comunicaciones alternativas

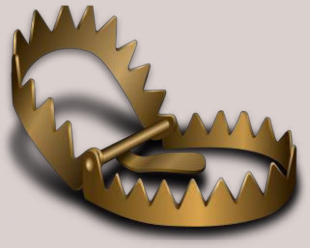
- Siempre tener al menos una fuente redundante de comunicación.
- Radio, wimax, satelite.

Índice

- Introducción
- Objetivos de un CERT
- Servicios de un CERT
- Propuesta
  - Difusión de información
  - **Equipo Hardware**
  - Sistemas de gestión de información y eventos de seguridad
  - Diagrama
  - Conclusiones y trabajos futuros

Equipo Hardware





IPS

- Bloquea ataques conocidos o no.
- Establece políticas de seguridad para proteger el equipo.

Firewall

- Bloqueo de paquetes provenientes de un rango de IP, puertos, dominios, etc.
- Herramienta de análisis del comportamiento.
- Herramienta de análisis forense.

Respaldo de datos

- No solo los ataques malintencionados provocan perdida de información.
- Una opción es establecer un arreglo de discos RAID.

Hardening

- Proceso de reducción de vulnerabilidades al mínimo.
- Eliminando software innecesario.
- Eliminando servicios.
- Cambiando puertos.

Honeypot

- Su función es ser atacado, investigado, comprometido, usado o accedido de forma no autorizada.
- Su objetivo es recabar información.

Índice

- Introducción
- Objetivos de un CERT
- Servicios de un CERT
- Propuesta
  - Difusión de información
  - Equipo Hardware
  - **Sistemas de gestión de información y eventos de seguridad**
  - Diagrama
  - Conclusiones y trabajos futuros

Sistemas de gestión de información y eventos de seguridad

SIM

- Gestión de tasas de información.
- Reporteo de cumplimiento de regulaciones.

SEM

- Monitorización de eventos en tiempo real.
- Gestión de incidentes de seguridad informática.

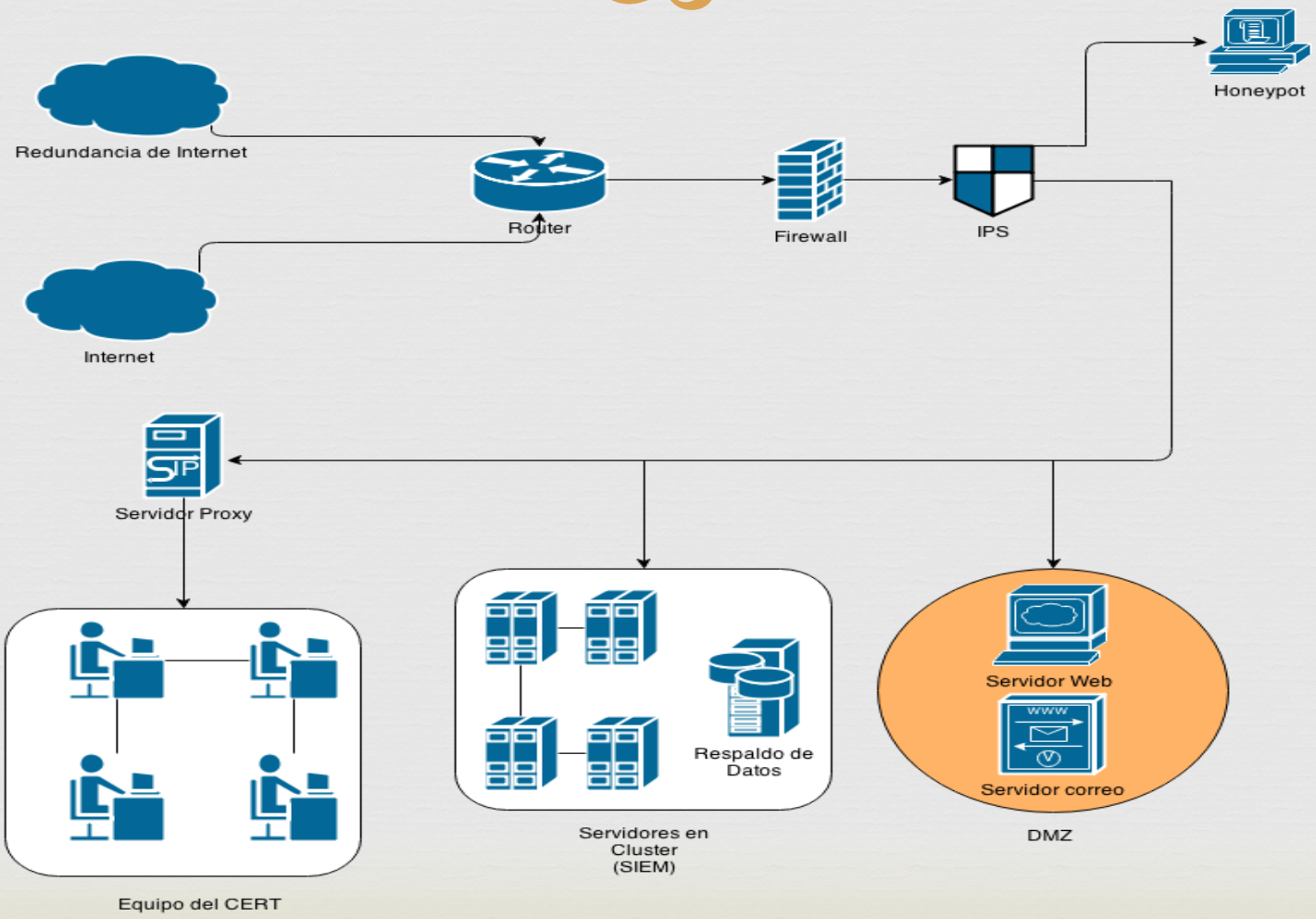
SIEM

- Actúa como un repositorio central para las trazas generadas por las diferentes herramientas.
- OSSIM de AlienVault.
- Arcsight ESM de HP.

Índice

- Introducción
- Objetivos de un CERT
- Servicios de un CERT
- Propuesta
  - Difusión de información
  - Equipo Hardware
  - Sistemas de gestión de información y eventos de seguridad
  - **Diagrama**
  - Conclusiones y trabajos futuros

Diagrama


Redundancia de Internet
Router
Firewall
IPS
Honeypot
Internet
Servidor Proxy
Equipo del CERT
Respaldo de Datos
Servidores en Cluster (SIEM)
Servidor Web
Servidor correo
DMZ

Índice

- Introducción
- Objetivos de un CERT
- Servicios de un CERT
- Propuesta
  - Difusión de información
  - Equipo Hardware
  - Sistemas de gestión de información y eventos de seguridad
  - Diagrama
  - **Conclusiones y trabajos futuros**

Conclusiones y trabajos futuros

- Se buscaba en un principio obtener información acerca del **hardware, software, tecnología y buenas prácticas que utilizan los CERTs en el mundo**, con el fin de dirigir la propuesta hacia una tipología de CERT. Sin embargo, **no se encontró resultados de CERTs** en especifico debido a que tal información es de **carácter sensible** y por lo tanto **la información no es compartida**, únicamente se encontró de manera muy general. Sin embargo, como trabajo futuro, se enfocará la investigación para enriquecer esta propuesta no solo dentro del ambiente de los CERTs, sino en **otras áreas informáticas**.

Gracias