Procedimientos Proactivos de Seguridad

Universidad Autónoma del
Estado de Hidalgo

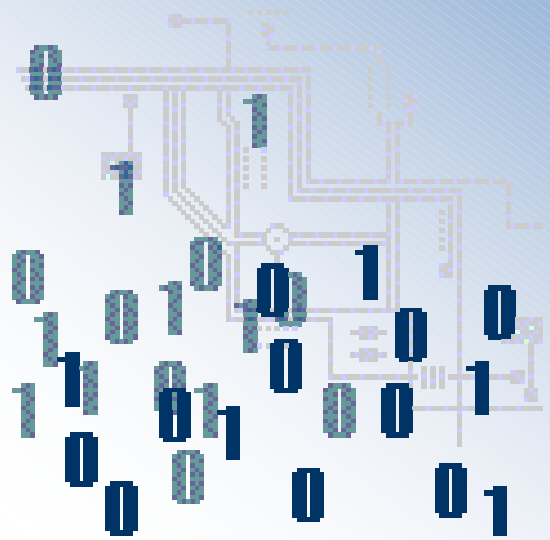
Cudi 2005
Reunion Primavera
Veracruz, Ver.

Contenido

- Sistema de seguridad
- Reto de una Red de Alto Disponibilidad
- Desarrollo de los procedimientos
- Resultados
- Conclusiones

Sistema de Seguridad

- Mecanismos de seguridad a nivel de protocolo y aplicación
- Mecanismos de filtrado de contenido
- Mecanismos de antispam



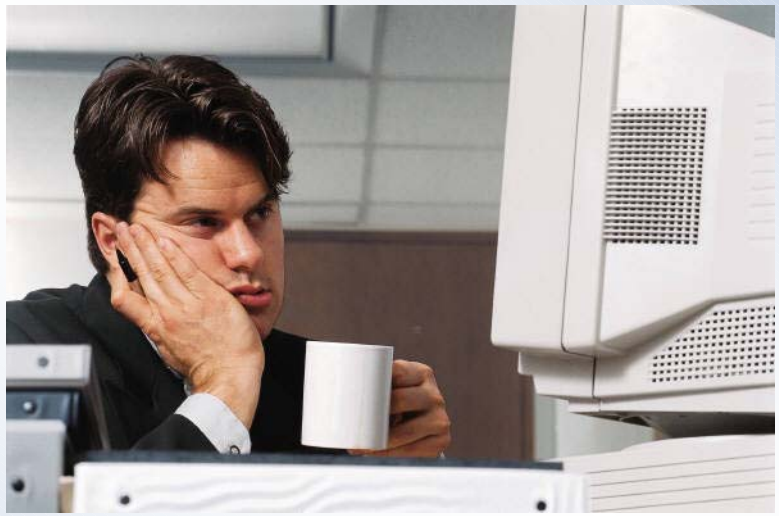
Sistema de Seguridad

- Sistemas de monitoreo en tiempo real
- Políticas de seguridad
- Sistemas de alarma

Sistema de Seguridad

Una red con estas características puede proporcionar a los usuarios un nivel de confianza y seguridad alto

Sistema de Seguridad



¿ Que hay acerca de la administración y mantenimiento del sistema de seguridad?

Sistema de Seguridad

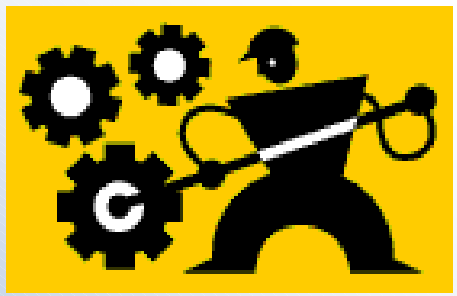
El ataque que mas impacta a los usuarios es la interrupción de los servicios

Reto de una Red de Alta Disponibilidad

Los servicios deben estar funcionando las **24 horas y los 365 días** del año para poder ser utilizados desde todos los nodos **autorizados**

Reto de una Red de Alta Disponibilidad

- En la actualidad casi todos los servicios son críticos

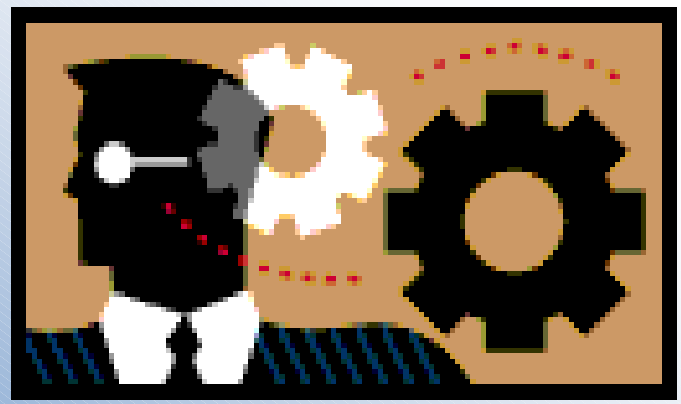


•Las interrupciones se consideran hasta 4 horas sin servicio

- Mayores a cuatro horas se consideran ataques de deshabilitacion y destruccion

Reto de una Red de Alta Disponibilidad

- Un porcentaje de aproximadamente el 20% de las interrupciones de algún servicio son atribuidas al actividades complejas que se deben realizar en la red



Reto de una Red de Alta Disponibilidad

- Pero un 65% del total de las interrupciones de los servicios, son debido a que no se programaron o no llevaron a cabo actividades de rutina

Reto de una Red de Alta Disponibilidad

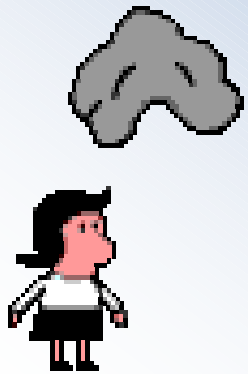
- Las actividades muy sencillas el personal de operación las lleva a acabo eventualmente.

Reto de una Red de Alta Disponibilidad

- Un porcentaje bastante alto tienen que ver de alguna forma con las vulnerabilidades de los equipos, malas configuraciones, ataques de a servicios no administrados y errores humanos

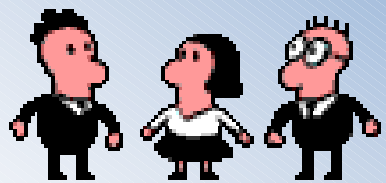
Desarrollo de los procedimientos

El objetivo principal es que deben de ser proactivos



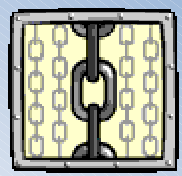
Desarrollo de los procedimientos

- Identificarlos



- Que fueran sencillos de ejecutar
- Debían de tomar en cuenta a los indicadores mas representativos

Desarrollo de los procedimientos



- Sobre todo deberían de ser calendarizados
- Y asegurarse de cumplir con su cometido
- En la medida posible ser automatizados

Desarrollo de los procedimientos

- Procedimiento para la optimización del desempeño de los equipos
- Procedimiento de Seguridad en los Equipos

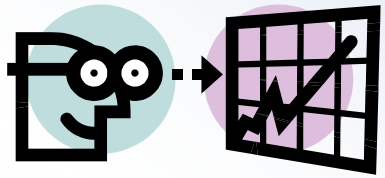
Desarrollo de los procedimientos

- Procedimiento de Monitoreo de la Red
- Implementación de nuevas tecnologías
- Plan de recuperación de desastres

Resultados

El numero de interrupciones se ha decrementazo en un 90%, como consecuencia el numero de acciones correctivas son esporádicas

Resultados



Se han identificado y detenido un mayor numero de ataques a la infraestructura, de igual forma se tiene un control mas exhaustivo del trafico en la red

Conclusiones

La administración y la operación de la red son actividades susceptibles de poderse medir y por lo tanto deben de ser calidad

Preguntas

Miguel Angel Hernandez Vazquez
miguelh@uaeh.edu.mx