Seguridad en Redes de Gobierno

PAULINA RAMOS GATEÑO
JEFA DE CPMPUTACION E INFORMATICA
ESCUELA PDI

Agenda

- Definición
- Seguridad Informática
- Como es el Escenario Actual de las TI y redes
- la Ciberseguridad
- Amenazas globales
- ¿implicancias por fallas en seguridad?
- ¿ Cuáles son las Medidas concretas que se pueden utilizar?
- Conclusiones

Seguridad Informática

Es una parte de la Informática, que procura velar por los activos informáticos, y además, podría definirse como el conjunto de procedimientos y actuaciones destinados al funcionamiento del sistema de información.

Seguridad Informática

Los activos que conforman la seguridad de la información ya sea de una organización o empresa privada son **confidencialidad**, **integridad** y **disponibilidad**.

Seguridad Informática

La **confidencialidad** tiene relación con la protección de información frente a posibles accesos no autorizados.

La **integridad** se refiere a resguardar la información, y métodos de procesamiento afectos a cambios, alteraciones y/u otros que afecten en su estructura o contenido.

La **disponibilidad** es la garantía de que los usuarios autorizados puedan acceder a la información y recursos cuando los necesiten.

Seguridad Informática

La **seguridad** es más que un intangible o producto, son constantes monitoreos, creación de hábitos.

La pérdida de confidencialidad, integridad o disponibilidad pueden ser por diversos motivos, y como consecuencia originan daños económicos, datos erróneos , perdida de oportunidades y lo que mas daño es la **pérdida de imagen pública**.

Seguridad Informática en Redes de Gobierno

Desde un punto de vista de la sociedad, se espera la actuación de buena fe, en cuanto al tratamiento de la información.

Escenario actual – TI y redes

- Las TI son herramientas, que permiten mejorar la gestión de las Instituciones Públicas.
- las TI nos permiten contar con diversas áreas de conocimientos.
- Permiten crear sistemas internos para la administración de la información.
- el acceso a Internet y banda ancha han aumentado constantemente,
- personas con acceso a Internet
- conexiones Banda Ancha.

TI y redes – Escenario actual

Desafíos y Riesgos:

- Portales Informáticos y sistemas desarrollados poco prolijos y con vulnerabilidades.
- Administradores de sistemas no aptos para el cargo
- Rápida disponibilidad de herramientas para construir y para destruir.
- Explosiva aparición de aplicaciones de mensajería instantánea, P2P
- mal uso de las TI
- uso de facebook, chats, entre otros
- descargas que interfieren el derecho de autor.

¿Por qué la ciber seguridad es tema

- Hoy en día, los sistemas, contables, financieros operan sobre sistemas de tecnología de la información e Internet.

- Esto provoca que los sistemas se vuelvan vulnerables a ataques ciberterroristas.

- de acuerdo a los últimos análisis, podemos hablar fehacientemente de grupos de crimen organizado.

Ciber Seguridad

Los ataques terroristas sufridos por Inglaterra, España, Estados Unidos prueban que los ataques a objetivos no militares pueden afectar infraestructura crítica.

Luego del ataque del 9/11 surgió una publicación llamada "Estrategia Nacional" para prevenir y dar seguridad al ciberespacio; ésta es dirigida a empresas e individuos como potenciales objetivos del ciberterrorismo.

Ciber Seguridad

Los atacantes siempre están viendo desde fuera las vulnerabilidades, por lo es necesario tener claro, cuando, como y que proteger.

Amenazas (1)

- En todas las entidades públicas y de Gobierno, aumenta la probabilidad de ataques de crackers, hackers, ociosos y vándalos. El hecho de ingresar a una Red de Gobierno le da status a los crackers.
- Los ataques son internos o desde el extranjeros.
  - Amenazas permanentes:
  - Virus, Gusanos, Troyanos.
  - Spywares.
  - Phishing.
  - Denegación de servicios,.

Amenazas (2)

- por lo general los propios funcionarios de entidades públicas y privadas , utilizan de manera indiscriminada aplicaciones peligrosas (p2p, juegos con virus o malwares).
- No existe control sobre :
- correos extrenos.
- P2P
- dispositivos USB.

- De acuerdo a estudios realizados, los propios usuarios actuan como agentes negativos, ya sea por venganza, problemas personales y /o de trabajo, etc.

Implicancias por fallas de seguridad

Los riesgos asociados a las fallas de seguridad, son diversos y casi siempre significan daños económicos, datos falsos, pérdida de oportunidades, descrédito y pérdida de imagen pública.

Cuales son las implicancias por una falla de seguridad

Hacker

Crackers ……..

Fue posible evitarlo?

- Pueden hacerlo de nuevo?
- Qué aprendió del evento?
- Cuantos sistema similares tiene?
- Mejoró la seguridad desde entonces?
- Esta tomando precauciones adicionales?
- Identificó al responsable?

Algunas causas

- Debilidades estructurales (plataforma, SO).
- Descuido de los usuarios y/o administradores.
- No se persigue a los responsables.
- Se trata de minimizar el evento.

Qué podemos hacer

- Identificar los problemas
- Definir políticas
- Definir protocolos
- Monitoreo constante de los usuarios.
- Capacitar, educar sobre esta temática.
- Invertir en HW y SW especializado para seguridad.

Consejos (1)

- Se aconseja instalar un detector de intrusos (IDS) en sus redes. De esta manera podrá saber que pasa en su red, conocer sus amenazas.
- Para ello revise sus logs de transacción.
  - Definir políticas de seguridad para sus sistemas, redes y usuarios.(manual)
  - Revisar configuraciones de su red.
  - Restringir la capacidad de instalar aplicaciones no necesarias..

Consejos (2)

Realizar administración interna.

Si externaliza el servicio, debe ser auditado constantemente, y evitar conexiones remotas.

Exija auditoria externa.

Revise constantemente la configuración de su corta fuegos, y que sea administrado por un especialista.

Denegación de permisos, salvo cuando sea requerido y supervisado.

Revisar logs del corta fuegos.

Consejos (3)

- Mantener actualizadas sus estaciones de trabajo.
- mantener actualizado el Anti Virus.
- enseñe a sus usuarios a usar un Anti Spyware.
- Haga que su administrador, minimice los riesgos en su propio DNS; que reporte las actividades sospechosas.
- realizar y chequear el inventario de SW
- saber que utilizan e instalan los usuarios .

Consejos (4)

- Quién resguarda que el administrador de la red evite:
- Leer correos
- Leer archivos de terceros.
- Leer información confidencial.
- Haga mal uso de los sistemas y reportería.

TODO LO ANTERIOR SE PUEDE EVITAR, AUDITANDO AL MISMO ADMINISTRADOR.

Reflexiones

- Auditorias
- seguridad
- Palique seguridad a sus sistemas, invierta……y podrá recién prevenir.
- la Seguridad en nuestras Redes no es una opción, es una obligación.

Seguridad en Redes de Gobierno

PAULINA RAMOS GATEÑO
JEFA DE CPMPUTACION E INFORMATICA
ESCUELA PDI