Seguridad en sistemas en red

Seguridad

No es un producto que pueda comprarse e instalarse

Proceso continuo que requiere:

- Monitorización
- Actualización permanente
- Definición de políticas de seguridad

- Normas y prácticas
    - Implementadas y cuidadas por responsables de seguridad
    - Establecen procedimientos y rutinas que se crean necesarias

La seguridad debe garantizar

Confidencialidad

Solo entes autorizados tienen acceso a la información que necesiten

Ejemplo: secreto industrial

Competencia no tiene que tener acceso a cierta información

Integridad

Evitar que la información sea modificada

Ejemplo: transferencia bancaria

Disponibilidad

Garantiza que la información estará presente

Siempre que se requiere

Autenticidad

Asegura la identidad u origen

Demuestra que quien genera información no puede retractarse

Ejemplo: acciones de bolsa

Componentes a proteger

Hardware

Software

Información

- Tiene mucha importancia
- Bien intangible no directamente valorable
- Pérdida de información no siempre cuantificable

Clasificación de amenazas

- Interrupción:
    - Pérdida de una parte del sistema
- Interceptación:
    - Acceso no autorizado a un elemento del sistema

- Modificación:
    - Consigue modificar un elemento del sistema
- Fabricación:
    - Modificación no destructiva

Persigue que el sistema trabaje de forma similar

Cambiando alguna parte del objeto final del mismo

Clasificación de seguridad

Física o lógica

Activa o pasiva

Activa:

- Medidas que intentan prevenir y evitar daños en sistemas informáticos
- ACL, contraseñas, encriptación, firmas, cuotas, encriptación

Pasiva:

- Minimizar los efectos ocasionados
- SAI, backups, RAID

Seguridad física

Trata de proteger el hardware de amenazas o desastres naturales.

Muchos de los riesgos y amenazas

De naturaleza física

En sistemas informáticos y también en sistemas en red

Seguridad física

Conjunto de recursos

Orientados a la aplicación de medidas preventivas

Contra amenazas físicas o naturales

Controles y sistemas de seguridad implementados para proteger el hardware

Amenazas según origen

Incendio

Prevención de riesgos

Documentada en plan de prevención de riesgos laborales

Establecidos en los planes de evacuación (con responsables y procedimientos)

Sistemas extintores de fuego por agua o polvo

Provocan daño a los sistemas (inutilizables)

Debe tenerse en cuenta

- Situación de los equipos
- Locales que no posean materiales combustibles
- No cerca de almacenes de material inflamable / explosivo
- Recomendable instalar suelo técnico y puertas o paredes cortafuegos
- Tener copias de información
- Sistemas y servidores duplicados
- En localizaciones diferentes (asegurar disponbilidad)

Inundación

Causa natural o artificial

Acciones posibles:

- No instalar sistemas en sótanos o plantas bajas
- Utilizar techos impermeables

Desastres naturales

Terremotos, condiciones climáticas severas

Suelen existir:

- Planes de contingencia
- Servicio de alerta climática

Construcción de edificios prevee desastres según normativa local (Japón)

Electromagnetismo

Aspectos a destacar

Alimentación eléctrica

Protección TEMPEST

Interferencias electromagnéticas

Protecciones TEMPEST

Medidas de protección frente a emisiones electromagnéticas

Emisiones generadas por los sistemas

Monitor del equipo

Pueden generar agujeros de seguridad

Emisiones pueden recogerse y visualizarse

Protecciones en organizaciones con grandes requisitos de seguridad

Bancos, instituciones militares, gubernamentales, etc.

Pasivas: no intervienen en el sistema

Interferencias electromagnéticas

Las interferencias electromagnéticas orientadas a la denegación de servicio pretenden evitar que una organización lleve a cabo su actividad normal. Para proteger los sistemas de las interferencias en una determinada banda de frecuencias típicas en comunicaciones radio se deben tomar medidas como la emisión con salto de frecuencias y crear un entorno físico libre de interferencias electromagnéticas.

Además, se deben instalar controles de temperatura y humedad, alimentar el sistema con un UPS (SAI) y ubicarlo en un espacio controlado, bajo llave y accesible solo al personal autorizado.

Factores humanos

Amenazas causadas por personas sin un objetivo concreto

Ejemplo: empleados descontentos o despedidos

Medidas a implementar:

- Controles de acceso
- Zonas de seguridad
- Métodos de autenticación

Recomendaciones:

- Exigir garantías personales de seguridad
- Informar de las consecuencias legales del sabotaje o divulgación de información clasificada

Alimentación eléctrica (problemas)

La alimentación eléctrica es un tema crítico en los sistemas de información, ya que una interrupción inesperada puede provocar pérdidas de información y corrupción en los sistemas. Para evitar esto hay varias soluciones, como por ejemplo:

- Disponer de sistemas de alimentación suplementaria o ininterrumpida (UPS/**SAI**)
- **baterías** que suministran energía durante un tiempo y dan tiempo a solucionar una emergencia o realizar cierres ordenados;
- **grupos electrógenos** u otras fuentes que generan electricidad para mantener los sistemas durante un tiempo adicional;
- **sistemas de protección eléctrica** como filtrado para evitar picos de tensión, protección contra sobretensiones y protección contra cortocircuitos.

Amenazas según objetivo

- Recursos

- Utilización
- Información
- Imagen

Riesgos físicos según su objetivo

- Daños físicos a equipos
- Robo o detrucción
- Reducción de la disponibilidad
- Impacto económico
- Acceso a la información
- Modificación y borrado malintencionado de datos

Seguridad lógica:

- Protege el software de los sistemas informáticos

Nivel físico

Nivel enlace

- MAC, protocolo ARP
- Man in the middle
- Defensa
- Vulnerabilidad STP

Nivel de red

- Sniffing o análisis de tráfico
- Spoofing o suplantación de la identidad, falseando algún dato de un PC
- Hijacking
- Denegación de servicio
- Fragmentación
- Inundación
- DDoS

Nivel de transporte

- Escaneo de puertos
- OS fingerprint
- Robos de sesión
- Ataques de repetición
- Parches
- Lista de control de acceso
- DMZ
- Honeypots y honeynets

Nivel de aplicación

Herramientas WAF

DNS spoofing:

- Falsear respuesta del servidor DNS sobre una petición
- Darle una IP diferente a la real

Nivel de meta aplicación

Legislación

- Ley orgánica de protección de datos
- Firma electrónica
- Recomendaciones ISO seguridad informática: ISO 27000