Conceptos básicos de seguridad

1. Conceptos básicos de seguridad general

- Seguridad: disciplina que se encarga de detectar, evaluar y gestionar los riesgos a los que se encuentra sometido algo. Al se un término muy ambiguo, lo habitual es que se trate la seguridad en campos o ámbitos más concretos (seguridad ciudadana, informática, alimentaria, vial, etc.).

- Riesgo: medida de la magnitud o alcance de los daños que puede provocar una situación peligrosa. Se miden asumiendo que cualquier sistema tiene una o más vulnerabilidades que son susceptibles de ataque, ya sea accidental o intencional.

- Vulnerabilidad: probabilidad de que ocurran daños cuando se presente un peligro.

- Peligrosidad: probabilidad de que ocurra un peligro.

- Medida de seguridad: acción que se toma para prevenir o reducir la peligrosidad o/y vulnerabilidad de un sistema. Se implementan en 4 pasos:

    - Identificación de riesgos: se identifican posibles riesgos o amenazas para el sistema.

    - Análisis de riesgos: se analizan los riesgos para determinar las circunstancias en que se pueden producir (peligrosidad) y el impacto que puedan tener (vulnerabilidad).

    - Toma de medidas: Determinación de las medidas necesarias para protegerse del riesgo e implementación de las mismas.

    - Evaluación de las medidas tomadas: determinar la eficacia de estas y si cumplen las expectativas. Si es baja o incluso contraproducente, se debe considerar su retirada.

Solo cuando seamos conscientes de los potenciales riesgos que existen contra nuestro sistema, podemos tomar las medidas de protección adecuadas.

A la hora de analizar los riesgos y medidas hay que tener un balance entre el conste de la ocurrencia del peligro y el de la medida/s para prevenirlo/paliarlo. Hay que tener el cuenta el mantenimiento y el impacto en la usabilidad del sistema.

2. Seguridad informática

Seguridad orientada a los sistemas informáticos y telecomunicaciones. Tiene los siguientes objetivos:

- Fiabilidad. El sistema debe funcionar correctamente y realizar las funciones para las que se ha diseñado (no puede cometer errores).
- Confidencialidad. Los usuarios sólo tienen acceso a los recursos a los que están autorizados.
- Integridad. Los datos tienen que ser veraces y completos, reflejando la situación real. No se pueden eliminar datos que deban mantenerse.
- Disponibilidad. Cualquier usuario legítimo debe poder utilizar el sistema el momento en el que lo necesite.
- Verificabilidad (no repudio). Cuando se realicen modificaciones a la información se debe conocer quien, cuando y qué información se ha modificado. Persigue el conocer quién ha sido el responsable de cualquier modificación que haya causado algún problema.

Definición formal: área de la informática que se enfoca en la infraestructura informática y todo lo relacionado con ésta, especialmente la seguridad de los datos almacenados o que se comunican al exterior.

No debe confundirse con la seguridad de la información. Esta se encarga de asegurar de asegurar la información esté donde esté, informatizada o no.

3. Tipos de SI

a. Según el momento en que se actúa

i. Activa

Intentan prevenir los problemas. Podemos encontrar:

- Contraseñas fuertes.
- Utilizar y actualizar sistemas anti-malware.
- S.O. actualizado.
- Educación de usuarios.
- Cortafuegos.
- Prohibición de medios extraíbles.
- Configuración del S.O.

ii. Pasiva

Medidas destinadas a reparar o minimizar los daños producidos por un ataque o accidente. Se aplican cuando ya se ha producido, reparando o paliando los efectos. Podemos encontrar:

- Copias de seguridad.
- Sistemas redundantes.

b. Según lo que se proteja

i. Física

Conjunto de medidas destinadas a asegurar la integridad física de los equipos y comunicaciones que forman el sistema -> proteger los elementos tangibles del sistema.

- Incendios
    - Usar elementos ignífugos en las habitaciones de los equipos.
    - Alejar las zonas de los equipos de zonas con materiales inflamables.
    - Sistemas de detección y extinción de incendios: detectores de humo, aspersores, extintores, etc.
- Inundaciones
    - Evitar la instalación de lose equipos en sótanos o plantas bajas
    - Impermeabilización y sellado de puertas
- Robos
    - Cerraduras seguras
    - Cámaras de seguridad
    - Sistemas de detección de presencia e intrusión
    - Personal de vigilancia
- Señales electromagnéticas
    - Evitar la instalación de los centros informáticos cerca de fuentes potentes de S.E.
    - Protecciones como apantallamiento del cableado y los equipos, uso de cables resistentes, apantallamiento completo de las habitaciones o edificios

- Fallos en red eléctrica
    - Utilizar sistemas de alimentación ininterrumpida (SAIs) que almacenan energía y alimentan los equipos en caso de interrupción breve del suministro.
    - En caso de fallos de mayor duración, uso de generadores.
    - Existen empresas que proporcionan generadores móviles que pueden alimentar un edificio ininterrumpidamente el tiempo necesario.
    - Filtros de alimentación que estabilizan la corriente eléctrica en caso de sobrecargas o sobretensiones.

ii. Lógica

Conjunto de medidas destinadas a proteger los datos que contiene o circulan por un sistema informático -> proteger la parte no tangible.

Es el aspecto más importante, puesto que la información es el activo más importante. Si se pierde, la actividad de la organización se resiente más que si se estropea o compromete un equipo.

- Modificaciones no autorizadas a datos o programas:
    - Restringir el acceso mediante identificación
    - Limitar el acceso al los usuarios a los datos/programas estrictamente necesarios
    - Registros de modificaciones con todos lo datos (qué modificación, quién y cuando
- Ataques a través de la red
    - Cortafuegos
    - Sistemas de monitorización de red y detección de intrusiones
    - Registros de accesso
- Pérdidas de información
    - Copias de seguridad
    - Sistemas tolerantes a fallos. Permiten algún nivel de fallo en sus componentes, funcionando de forma degradada hasta que se arregle
    - Discos redundantes. Se almacenan en 2 o más discos que son copias idénticas.

- Malware: sistemas de detección y neutralización de malware.
- Suplantación de identidad: sistemas de autentificación avanzados como sistemas biométricos o de 2 pasos.

4. Amenazas y fraudes a la SI

Según el atacante se pueden clasificar en:

- Hacker. Expertos informáticos que investigan la seguridad de los sistemas pero sin ánimo de dañar u obtener beneficio económico.
- Crackers. Hakcers maliciosos.
- Phreakers. Crackers especializados en las redes de telefonía.
- Sniffers. Expertos en analizar el tráfico de las redes para obtener información.
- Ciberterrorista. Hackers que trabajan para gobiernos/organizaciones como espías o saboteadores.
- Carders. Se dedican al ataque a los sistemas de pago, especialmente tarjetas de crédito o cajeros automáticos.

Según el resultado:

- Interrupción: se dificultan gravemente o interrumpen uno o más servicios.
- Intercepción: se intercepta la información en camino, normalmente en una red.
- Modificación: la información se modifica sin autorización, por lo que deja de ser válida o consistente.
- Fabricación: se crea una construcción informática que suplanta a la original y que puede utilizarse para acceder a la información confidencial de los usuarios.

Según la forma de actuación del ataque:

- Spoofing: suplanta la identidad de un equipo en la red.
- Sniffing: monitoriza el tráfico en la red y lo analiza para obtener información.
- Exploit: se localiza un fallo de seguridad en algún programa y se explota para conseguir acceso no autorizado.

- Malware: se introducen programas malintencionados en el equipo.

- Denegación de servicios: realizar peticiones masivas a un servicio para que se sobrecarge y no pueda proporcionarse. Si se hace desde varios equipos de forma ordenada, es un Ataque distribuido de denegación de servicios.

- Ingeniería social: utiliza engaños para obtener información confidencial de las personas.

- Phising: se engaña al usuario para que proporcione información confidencial suplantando un sitio legítimo de internet.