Seguridad Informática

La seguridad informática o seguridad de tecnologías de la información es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante.

Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore (activo) y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

La función de la seguridad informática en esta área es velar que los equipos funcionen adecuadamente y anticiparse en caso de fallas, robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

AMENAZAS

No solo las amenazas que surgen de la programación y el funcionamiento de un dispositivo de almacenamiento, transmisión o proceso deben ser consideradas, también hay otras circunstancias que deben ser tenidas en cuenta, incluso «no informáticas». Muchas son a menudo imprevisibles o inevitables, de modo que las únicas protecciones posibles son las redundancias y la descentralización, por ejemplo mediante determinadas estructuras de redes en el caso de las comunicaciones o servidores en clúster para la disponibilidad.

Las amenazas pueden ser causadas por:

Usuarios

Causa del mayor problema ligado a la seguridad de un sistema informático. En algunos casos sus acciones causan problemas de seguridad, si bien en la mayoría de los casos es porque tienen permisos sobre dimensionados, no se les han restringido acciones innecesarias. De igual forma personal de la empresa puede convertirse en un peligro si deciden robar o alterar información importante de la compañía, para su beneficio propio.

Programas maliciosos

programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el ordenador, abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano

informático, un troyano, una bomba lógica, un programa espía o spyware, en general conocidos como malware.

Errores de programación

La mayoría de los errores de programación que se pueden considerar como una amenaza informática es por su condición de poder ser usados como exploits por los crackers, aunque se dan casos donde el mal desarrollo es, en sí mismo, una amenaza. La actualización de parches de los sistemas operativos y aplicaciones permite evitar este tipo de amenazas.

Siniestros

Una mala manipulación de materiales o mala intención derivan a la pérdida del material o de los archivos. De igual forma ocurre con los desastres naturales.

TÉCNICAS PARA ASEGURAR EL SISTEMA

El activo más importante que se posee es la información y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y solo permiten acceder a ellos a las personas autorizadas para hacerlo.

Cada tipo de ataque y cada sistema requiere de un medio de protección o más (en la mayoría de los casos es una combinación de varios de ellos). A continuación se enumeran una serie de medidas que se consideran básicas para asegurar un sistema:

Implantar medidas de seguridad físicas

Sistemas antiincendios, vigilancia de los centros de proceso de datos, sistemas de protección contra inundaciones, protecciones eléctricas contra apagones y sobretensiones, sistemas de control de accesos, etc.

Codificar la información

Criptología, criptografía y criptociencia. Esto se debe realizar en todos aquellos trayectos por los que circule la información que se quiere proteger, no solo en aquellos más vulnerables. Por ejemplo, si los datos de una base muy confidencial se han protegido con dos niveles de firewall, se ha cifrado todo el trayecto entre los clientes y los servidores y entre los propios servidores, se utilizan certificados y sin embargo se dejan sin cifrar las impresiones enviadas a la impresora de red, tendríamos un punto de vulnerabilidad.

Contraseñas difíciles

Que puedan ser deducidas a partir de los datos personales del individuo o por comparación con un diccionario, y que se cambien con la suficiente periodicidad. Las contraseñas, además, deben tener la suficiente complejidad como para que un atacante no pueda deducirla por medio de programas informáticos. El uso de certificados digitales mejora la seguridad frente al simple uso de contraseñas

Vigilancia de red

Las redes transportan toda la información, por lo que además de ser el medio habitual de acceso de los atacantes, también son un buen lugar para obtener la información sin tener que acceder a las fuentes de la misma. Existen medidas que abarcan desde la seguridad física de los puntos de entrada hasta el control de equipos conectados
.

Redes perimetrales de Seguridad (DMZ)

Permiten generar reglas de acceso fuertes entre los usuarios y servidores no públicos y los equipos publicados. De esta forma, las reglas más débiles solo permiten el acceso a ciertos equipos y nunca a los datos, que quedarán tras dos niveles de seguridad.

Tecnologías Repelentes o Protectoras

cortafuegos, sistema de detección de intrusos - antispyware, antivirus, llaves para protección de software, etc.

Actualizaciones

Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.

Respaldos

Copias de seguridad e, incluso, sistemas de respaldo remoto que permiten mantener la información en dos ubicaciones de forma asíncrona.

Permisos

Controlar el acceso a la información por medio de permisos centralizados y mantenidos (tipo Active Directory, LDAP, listas de control de acceso, etc.