2019

SEGURIDAD INFORMÁTICA

Raúl Pérez y Saúl de la Rosa

Fundamentos del Hardware

10-3-2019

Índice

¿Qué es?	**2**
¿Por qué es tan importante?	**2**
Tipos de seguridad informática.	**3**
¿Qué áreas cubre la seguridad informática?	**3**
¿Qué es un virus?	**4**
Síntomas de que un sistema está infectado.	**5**
Objetivos.	**6**
Amenazas.	**6**
Bibliografía.	**8**

¿Qué es?

Podemos definir qué es la seguridad informática como el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente. La seguridad informática es en realidad una rama de un término más genérico que es la seguridad de la información, aunque en la práctica se suelen utilizar de forma indistinta ambos términos.

¿Por qué es tan importante?

Hemos de tener en cuenta que nuestros sistemas informáticos hoy en día contienen mucha información sobre nosotros, tanto cosas simples como nuestros gustos o aficiones, como datos de tanta importancia como nuestras cuentas bancarias, información de nuestras tarjetas de crédito, contraseñas o dirección de nuestro domicilio. Por eso debemos tener en cuenta la importancia de que tanto dichos datos como las rutas que toman en la red sean lo suficientemente seguros para poder interactuar con nuestro sistema sin correr ningún tipo de riesgo. Un intruso puede modificar y cambiar los códigos fuente de los programas y también puede utilizar tus imágenes o cuentas de correo electrónico para crear contenido perjudicial, como imágenes pornográficas o cuentas sociales falsas. Hay también ciberdelincuentes que intentarán acceder a los ordenadores con intenciones maliciosas como pueden ser atacar a otros equipos o sitios web o redes simplemente para crear el caos.

Tipos de seguridad informática.

Los hackers suelen realizar sus acciones principales en la red, aunque también hay que tener especial cuidado con el software y el hardware, por este motivo, existe seguridad informática para cada uno de estos tres elementos:

- **Seguridad online:** los virus, los robos de identidad, las intrusiones ilegales... todo esto forma parte de los delitos en la red y estos fallos pueden

provocar daños muy graves e incluso irreparables. Para ello existen herramientas que nos ayudarán a mejorar la seguridad de nuestra red que son sencillas de utilizar y además ofrecen unos buenos resultados.

  - Antivirus: McAfee, Panda, Norton…
  - Programas antispyware: ScanGuard, Bit defender…

Cabe decir que muchos de los antivirus, incluso los gratuitos cuentan con antispyware.

- **Seguridad en software:** Este tipo de seguridad ni siquiera se tenía en cuenta hasta hace muy poco, pero recientemente se descubrió que los fallos en el software pueden dañar nuestro sistema y, lo que es peor, ser una puerta abierta para los ciberdelincuentes, debido a la mala instalación de este o a errores en el propio diseño.
- **Seguridad en hardware:** Para combatir este tipo de malware se utilizan cortafuegos de hardware, lo que hacen estas herramientas es controlar de forma exhaustiva el tráfico que se produce en la red, dotando al mismo tiempo al hardware con una seguridad mucho más potente. La seguridad de hardware es una de las más completas.

¿Qué áreas cubre la seguridad informática?

Confidencialidad: Sólo los usuarios autorizados pueden acceder a nuestros recursos, datos e información.

Integridad: Sólo los usuarios autorizados deben ser capaces de modificar los datos cuando sea necesario.

Disponibilidad: Los datos deben estar disponibles para los usuarios cuando sea necesario.

Autenticación: Estás realmente comunicándote con los que piensas que te estás comunicando.

¿Qué es un virus?

Un virus informático es un sistema de software dañino, escrito intencionadamente para entrar en una computadora sin permiso o conocimiento del usuario. Tiene la capacidad de replicarse a sí mismo, continuando así su propagación. Algunos virus no hacen mucho más que replicarse, mientras que otros pueden causar graves daños o afectar negativamente el rendimiento de un sistema. Un virus nunca debe ser considerado como inofensivo y dejarlo en un sistema sin tomar medidas.

Existen diferentes tipos, estos son los más comunes:

- **Adware**: Nos mostrará anuncios donde antes no aparecían y reducirá la agilidad operativa de la memoria RAM.
- **Spyware**: Recopila información de un equipo y los transmite a otra entidad externa sin que el propietario lo sepa y lo que es peor sin su consentimiento.

- **Malware**: Altera el funcionamiento normal de un dispositivo destruyendo archivos o corrompiéndolos.
- **Troyano**: Entra en el quipo porque nosotros mismos lo instalamos. Al ejecutar este software el virus accede por completo al sistema.
- **Phishing**: Consiste en el envío de correos electrónicos para obtener datos confidenciales del usuario haciéndose pasar por fuentes fiables como entidades bancarias.

Síntomas de que un sistema está infectado.

- **Pop-ups/Publicidad de la nada.**
- **Lentitud en el sistema.**
- **Las aplicaciones no inician.**
- **Desconexiones o conexión demasiado lenta.**
- **El navegador abre páginas no solicitadas.**
- **El antivirus desaparece y el firewall se desactiva.**
- **Los archivos y las bibliotecas desaparecen.**

Objetivos.

La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran los siguientes:

1. La infraestructura computacional: es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar por que los equipos funcionen adecuadamente y anticiparse en caso de fallos, robos, incendios, sabotajes, desastres naturales, fallos en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.
2. Los usuarios: son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. Debe protegerse el sistema en general para que el uso por parte de ellos no pueda poner en entredicho la seguridad de la información y tampoco que la información que manejan o almacenan sea vulnerable.
3. La información: esta es el principal activo. Utiliza y reside en la infraestructura computacional y es utilizada por los usuarios.

Amenazas.

No sólo 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 no informáticas que deben ser tomadas en cuenta. 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:

1. **Usuarios**: En la mayoría de los casos es porque tienen permisos sobredimensionados, no se les han restringido acciones innecesarias, etc.
2. **Programas maliciosos**: programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. 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.
3. **Errores de programación**: Pueden 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.
4. **Intrusos**: personas que consiguen acceder a los datos o programas a los cuales no están autorizados (crackers, defacers, hackers, script kiddie o script boy, viruxers, etc.).
5. **Un siniestro (robo, incendio, inundación).**
6. **Personal técnico interno**: técnicos de sistemas, administradores de bases de datos, técnicos de desarrollo, etc. Los motivos que se encuentran entre los habituales son: disputas internas, problemas laborales, despidos, fines lucrativos, espionaje, etc.
7. **Fallos electrónicos o lógicos de los sistemas informáticos en general**.
8. **Catástrofes naturales**.

Existen infinidad de modos de clasificar un ataque y cada ataque puede recibir más de una clasificación:

- **Amenazas por el origen.**

  El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella y hurtar información o alterar el funcionamiento de la red. Sin embargo el hecho de que la red no esté conectada a un entorno externo, como Internet, no nos garantiza la seguridad de la misma. De acuerdo con el Computer Security Institute (CSI) de San Francisco, aproximadamente entre el 60 y 80 por ciento de los incidentes de red son causados desde dentro de la misma. Basado en el origen del ataque podemos decir que existen dos tipos de amenazas:

  - **Amenazas externas:** aquellas amenazas que se originan fuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.
  - **Amenazas internas**: generalmente estas amenazas pueden ser más serias que las externas.

    Si es por usuarios o personal técnico, conocen la red y saben cómo es su funcionamiento, ubicación de la información, datos de interés, etc.

    Los sistemas de prevención de intrusos o IPS, y firewalls son mecanismos no efectivos en amenazas internas por no estar, habitualmente, orientados al tráfico interno. Que el ataque sea interno no tiene que ser exclusivamente por personas ajenas a la red, podría ser por vulnerabilidades que permiten acceder a la red directamente: rosetas accesibles, redes inalámbricas desprotegidas, equipos sin vigilancia, etc.

El tipo de amenazas según el efecto que causan a quien recibe los ataques podría clasificarse en:

- **Robo de información.**
- **Destrucción de información.**
- **Anulación del funcionamiento de los sistemas o efectos que tiendan a ello.**
- **Suplantación de la identidad, publicidad de datos personales o confidenciales, cambio de información, venta de datos personales, etc.**
- **Robo de dinero, estafas,...**
- **Amenazas por el medio utilizado**

  Se pueden clasificar por el modus operandi del atacante, si bien el efecto puede ser distinto para un mismo tipo de ataque:

  - Virus informático: malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Reemplazan archivos ejecutables por otros infectados con el código de este; pueden destruir los datos almacenados en un computadora, aunque o tan solo ser molestos.
  - Phishing.
  - Ingeniería social.
  - Denegación de servicio.
  - Spoofing: de DNS, de IP, de DHCP, etc.

Bibliografía.

- https://definicion.de/seguridad-informatica/
- https://www.obs-edu.com/es/blog-investigacion/sistemas/tipos-de-seguridad-informatica-mas-importantes-conocer-y-tener-en-cuenta-0
- https://www.universidadviu.es/la-seguridad-informatica-puede-ayudarme/
- https://tecnologia-informatica.com/como-saber-computadora-virus-infectada/
- https://vegagestion.es/como-identificar-los-tipos-de-virus-informaticos-mas-comunes/
- https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica#Objetivos