Seguridad informática

Javier Rollán y Jorge Miguel Villarta

Índice:

Seguridad informática:

Qué es:

La seguridad informática, también conocida como ciberseguridad, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras.

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 en un ambiente de red es la habilidad de identificar y eliminar vulnerabilidades, debe también poner atención a la necesidad de salvaguardar la ventaja organizacional, incluyendo información y equipos físicos, tales como los mismos computadores.

En que consiste:

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.

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

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 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.

Los usuarios: son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. Debe protegerse el

sistema 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.

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. Muchas son a menudo imprevisibles o inevitables, de modo que las únicas protecciones posibles son las redundancias y la descentralización.

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 sobredimensionados, no se les han restringido acciones innecesarias, etc.

Programas maliciosos: programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado 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, aunque se dan casos donde el mal desarrollo es, en sí mismo, una amenaza.

Intrusos: personas que consiguen acceder a los datos o programas a los cuales no están autorizados.

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.

Seguridad de software:

Qué es:

El último de los tipos de seguridad informática es el que se encarga de proteger contra ataques de hackers y demás riesgos comunes a nuestro software; es decir, a los programas y aplicaciones que instalamos en nuestros sistemas.

En que consiste:

Muchos de los programas que añadimos a nuestros ordenadores guardan todo tipo de información relevante sobre nosotros. Por eso, impedir que cualquier persona pueda acceder a ellos y robarnos nuestros datos es un campo fundamental de la ciberseguridad. Sin embargo, se trata de uno de los más recientes y por tanto todavía se encuentra en pleno desarrollo.

Al desarrollar programas y aplicaciones, es prácticamente imposible hacerlo de manera perfecta. Por eso, muchas veces el software tiene una serie de vulnerabilidades que cualquier persona que desee atacar nuestros equipos puede explotar. Debido a ello, esta rama de la seguridad se encarga de detectar y subsanar estos errores, así como de desarrollar alternativas más seguras que hayan sido diseñadas con las amenazas informáticas en mente desde el primer momento.

Amenazas/Soluciones:

Troyanos, Virus, gusanos

Antivirus: clamwin, mcaffe, avast antivirus

Limpiadores de programas dañinos: combofix

Seguridad de Hardware:

Qué es:

El segundo tipo de seguridad informática que debes conocer es el que tiene que ver con el hardware, es decir, la parte física de tu equipo. En general, este ámbito se relaciona con ciertos dispositivos que se pueden conectar a un ordenador para hacerlo más seguro.

En que consiste:

De los tres tipos de seguridad que existen, es el que hace más difícil que un atacante pueda acceder a tu información; pero al requerir de elementos externos, también puede ser el más caro y el más difícil de instalar.

Algunos de los dispositivos hardware más conocidos que pueden aumentar la seguridad de tus equipos informáticos son los firewalls de hardware y los servidores proxy. Otros, como los módulos de seguridad de hardware, son menos conocidos, pero pueden realizar algunas funciones muy útiles como encriptar los mensajes que mandes o servir para autenticar que la persona con la que te estás comunicando es realmente quien dice ser.

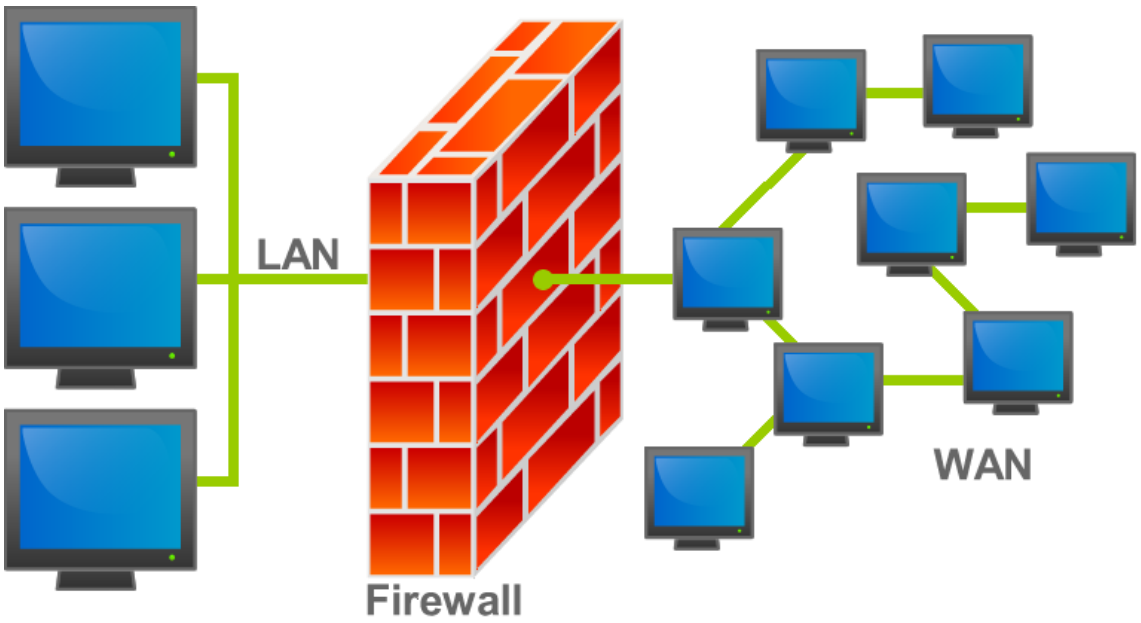
Por último, otra de las áreas de las que se encarga la seguridad de hardware es de detectar y examinar las vulnerabilidades que tiene cada equipo informático. Ningún dispositivo es perfecto; y por eso, esta rama se encarga de mostrarnos la manera en la que podemos volverlos menos accesibles a cualquier tipo de ataque.

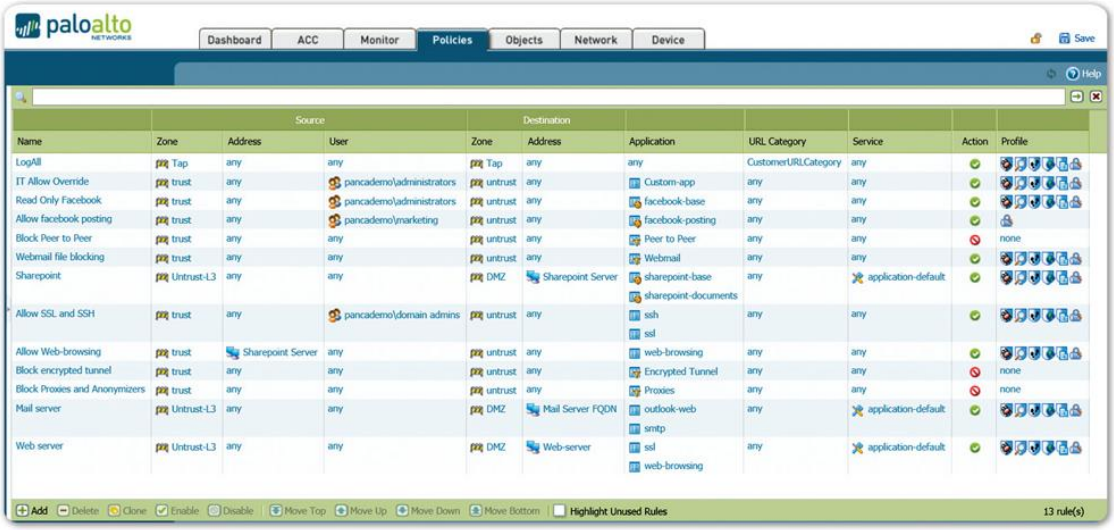
Hardware:

Un cortafuegos (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar o descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

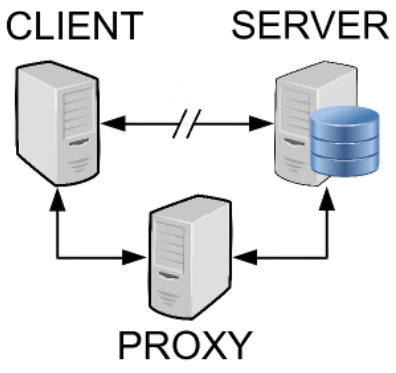
Fabricantes como Cisco, Palo alto, HP.





Servidor proxy, hace de intermediario en las peticiones de recursos que realiza un cliente a otro servidor. Esta situación permite controlo de acceso, registro del tráfico, restricciones, mejora de rendimiento, anonimato, etc.

Varios tipos: proxy nat, inverso, transparentes, abierto, cross-Domain.



Seguridad de Red:

Qué es:

Esta rama de la seguridad informática está compuesta por todo tipo de actividades destinadas a asegurar la fiabilidad, facilidad de uso, integridad y confidencialidad de las redes informáticas que utilizamos y los datos que pasan a través de las mismas.

Virus, troyanos, y gusanos.

Intentos por parte de hackers de controlar nuestro ordenador a distancia.

Robo de datos, como información de tarjetas o cuentas bancarias.

Suplantación de identidad, especialmente en las redes sociales.

Programas de publicidad no deseados (spam).

En que consiste:

Con el auge de Internet, han aparecido todo tipo de amenazas para la integridad de nuestros ordenadores. Una seguridad de red que cumpla su cometido tiene que ser capaz de detectar y detener a tiempo una gran variedad de problemas.

Debido a que las amenazas en la red son tan variadas, no existe una sola forma de protegernos de todas ellas a la vez. Por el contrario, para asegurar la máxima seguridad, es necesario contar con varias capas de protección. En el caso de que una fallase, las demás todavía deberían ser capaces de garantizar la seguridad de nuestra red.

Por lo general, la protección contra ataques de red se realiza por medio de software, es decir, de programas que instalamos en nuestro ordenador. Sin embargo, algunos componentes de hardware también pueden ser efectivos en este sentido. Algunas de las protecciones de red más comunes son las siguientes:

Amenazas/Contramedidas:

Ataques pasivos:

- Escucha telefónica
- Escáner de puertos

Ataques activos:

- Ataques de denegación de servicio:
  Causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad con la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema atacado.
- DNS spoofing:
  Es una situación creada de manera maliciosa o no deseada que provee datos de un servidor de nombres de dominio.
  Esta técnica puede ser usada para reemplazar arbitrariamente contenido de una serie de víctimas con contenido elegido por un atacante.
  Por ejemplo, un atacante envenena las entradas DNS de direcciones IP para un sitio web objetivo, reemplazándolas con la dirección IP de un servidor que él controla. Luego, el atacante crea entradas falsas para archivos en el servidor que él controla con nombres que coinciden con los archivos del servidor objetivo. Estos archivos pueden contener contenido malicioso, como un virus o un gusano
- ARP spoofing:
  Es enviar mensajes ARP falsos a la Ethernet. Normalmente la finalidad es asociar la dirección MAC del atacante con la dirección IP de otro nodo (el nodo atacado), como por ejemplo la puerta de enlace predeterminada.
  Cualquier tráfico dirigido a la dirección IP de ese nodo, será erróneamente enviado al atacante, en lugar de a su destino real. El atacante, puede entonces elegir, entre reenviar el tráfico a la puerta de enlace predeterminada real (ataque pasivo o escucha), o modificar los datos antes de reenviarlos (ataque activo).
  Por lo tanto, en redes grandes es preferible usar otro método: la inspección o *snooping* de DHCP. Mediante DHCP, el dispositivo de red mantiene un registro de las direcciones MAC que están

conectadas a cada puerto, de modo que rápidamente detecta si se recibe una suplantación ARP.

- Inyección de SQL:
  Es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.
- Phishing:
  La mayoría de los métodos de *phishing* utilizan la manipulación en el diseño del correo electrónico para lograr que un enlace parezca una ruta legítima de la organización por la cual se hace pasar el impostor. URLs manipuladas, o el uso de subdominios, son trucos comúnmente usados por *phishers*
- Cross-site scripting:
  Tipo de vulnerabilidad informática o agujero de seguridad típico de las aplicaciones Web, que puede permitir a una tercera persona inyectar en páginas web visitadas por el usuario código JavaScript
- CSRF:
  Un ataque CSRF fuerza al navegador web validado de una víctima a enviar una petición a una aplicación web vulnerable, la cual entonces realiza la acción elegida a través de la víctima. Al contrario que en los ataques XSS, los cuales explotan la confianza que un usuario tiene en un sitio en particular, el cross site request forgery explota la confianza que un sitio tiene en un usuario en particular.

Entre los principales componentes de seguridad de red, destacamos:

Uso de redes privadas virtuales (VPN), que permiten acceder a cualquier página de forma seguro:

- Utiliza una red pública, como Internet, para enlazar dos o más puntos, y permite el intercambio de información empleando criptografía.
- NordVPN, ExpressVPN, CyberGhost, VyprVPN, IPVanish, Hidden24.

Uso de navegadores encriptados, que hacen que nuestros datos no puedan ser rastreados de manera sencilla.

Sistemas de prevención de intrusiones (IPS), que nos ayudan a identificar problemas que se propagan rápidamente.

Un sistema de prevención de intrusos es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

Bibliografía:

https://www.universidadviu.es/la-seguridad-informatica-puede-ayudarme/

https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

https://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica)

http://blog.d-lockbackuponline.com/seguridad/tipos-de-seguridad-informatica-de-software-de-hardware-y-de-red/

https://www.universidadviu.es/tres-tipos-seguridad-informatica-debes-conocer/

https://www.viewnext.com/tipos-de-seguridad-informatica/

https://www.websec.es/seguridad-informatica-en-redes-software-y-hardware/

https://www.ibiblio.org/pub/Linux/docs/LuCaS/Manuales-LuCAS/doc-como-seguridad-fisica/html_out/laseguridadfisicadelhardwar.html

https://seguridadeninformaticablog.wordpress.com/2016/06/09/medidas-de-seguridad-en-software-y-hardware/