FUNDAMENTOS DE LA TEORIA DE LA SEGURIDAD INFORMATICA.

Materia: Seguridad Informatica.

Docente: Filiberto Duran García.

Alumno:
Pablo Sánchez Ugalde.

Sistemas 7° A

30/01/2019

La seguridad informática: es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático.

Un sistema informático puede ser protegido desde un punto de vista lógico (con el desarrollo de software) o físico (vinculado al mantenimiento eléctrico). Por otra parte, las amenazas pueden proceder desde programas dañinos que se instalan en la computadora del usuario (como un virus) o llegar por vía remota (los delincuentes que se conectan a Internet e ingresan a distintos sistemas).

Entre las herramientas más usuales de la seguridad informática, se encuentran los programas antivirus, los cortafuegos o firewalls, la encriptación de la información y el uso de contraseñas.

Herramientas todas ellas de gran utilidad como también lo son los conocidos sistemas de detección de intrusos, también conocidos como anti-spyware. Se trata de programas o aplicaciones gracias a los cuales se puede detectar de manera inmediata lo que son esos programas espías que se encuentran en nuestro sistema informático y que lo que realizan es una recopilación de información del mismo para luego ofrecérsela a un dispositivo externo sin contar con nuestra autorización en ningún momento.

Los principales objetivos de la seguridad informática son:

• Confidencialidad: consiste en la capacidad de garantizar que la información, almacenada en el sistema informático o transmitido por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información

• Disponibilidad: la definiremos como la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento

• Integridad: diremos que es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente.

• No repudio: este objetivo garantiza la participación de las partes en una comunicación. En toda comunicación, existe un emisor y un receptor, por lo que podemos distinguir dos tipos de no repudio: a) No repudio en origen: garantiza que la persona que envía el mensaje no puede negar que es el emisor del mismo, ya que el receptor tendrá pruebas del envío. b) No repudio en destino: El receptor no puede negar que recibió el mensaje, porque el emisor tiene pruebas de la recepción del mismo.

Seguridad de Hardware

La seguridad de hardware se puede relacionar con un dispositivo que se utiliza para escanear un sistema o controlar el tráfico de red. Los ejemplos más

comunes incluyen cortafuegos o firewalls de hardware y servidores proxy. De entre los diferentes tipos de seguridad informática, son los sistemas de hardware los que pueden proporcionar una seguridad más robusta, además de que también pueden servir como capa adicional de seguridad para los sistemas importantes. La seguridad de hardware también se refiere a cómo podemos proteger nuestros equipos físicos de cualquier daño. Para evaluar la seguridad de un dispositivo de hardware, es necesario tener en cuenta las vulnerabilidades existentes desde su fabricación, así como otras fuentes potenciales, tales como código que se ejecuta en dicho hardware y los dispositivos entrada y salida de datos que hay conectados en la red.

Seguridad de Software

La seguridad de software se utiliza para proteger el software contra ataques maliciosos de hackers y otros riesgos, de forma que nuestro software siga funcionando correctamente con este tipo de riesgos potenciales. Esta seguridad de software es necesaria para proporcionar integridad, autenticación y disponibilidad. Los defectos de software tienen diversas ramificaciones de seguridad, tales como errores de implementación, desbordamientos de buffer, defectos de diseño, mal manejo de errores, etc. Con demasiada frecuencia, intrusos maliciosos pueden introducirse en nuestros sistemas mediante la explotación de algunos de estos defectos de software. Las aplicaciones que tienen salida a Internet presentan además un riesgo de seguridad más alto. Se trata del más común hoy en día. Los agujeros de seguridad en el software son habituales y el problema es cada vez mayor. La seguridad de software aprovecha las mejores prácticas de la ingeniería de software e intenta hacer pensar en la seguridad desde el primer momento del ciclo de vida del software.

Seguridad de red

La seguridad de red se refiere a cualesquiera actividades diseñadas para proteger la red. En concreto, estas actividades protegen la facilidad de uso, fiabilidad, integridad y seguridad de su red y datos. La seguridad de red efectiva se dirige a una variedad de amenazas y la forma de impedir que entren o se difundan en una red de dispositivos. Los más comunes incluyen:

Virus, gusanos y caballos de Troya

Software espía y publicitario

Ataques de día cero, también llamados ataques de hora cero

Ataques de hackers

Ataques de denegación de servicio

Intercepción o robo de datos

Robo de identidad

Es necesario varios niveles de seguridad. Si uno falla, los demás siguen en pie. Seguridad de la red se lleva a cabo a través de hardware y software. El software debe ser actualizado constantemente para lograr protegerse de amenazas emergentes. Un sistema de seguridad de la red por lo general se compone de muchos componentes. Idealmente, todos los componentes trabajan juntos, lo que minimiza el mantenimiento y mejora la seguridad. Los componentes de seguridad de red incluyen:

Antivirus y antispyware

Cortafuegos, para bloquear el acceso no autorizado a su red

Sistemas de prevención de intrusiones (IPS), para identificar las amenazas de rápida propagación, como el día cero o cero horas ataques

Redes privadas virtuales (VPN), para proporcionar acceso remoto seguro

Referencias

- **1.2- OBJETIVOS DE LA SEGURIDAD INFORMÁTICA | SEGURIDAD INFORMÁTICA**

  En el texto: ("1.2- Objetivos de la seguridad informática | Seguridad Informática", 2019)

  Bibliografía: 1.2- Objetivos de la seguridad informática | Seguridad Informática. (2019). Retrieved from https://infosegur.wordpress.com/category/1-conceptos-basicos-de-la-seguridad-informatica/1-2-objetivos-de-la-seguridad-informatica/

DEFINICIÓN DE SEGURIDAD INFORMÁTICA — DEFINICION.DE

En el texto: ("Definición de seguridad informática — Definicion.de", 2019)

Bibliografía: Definición de seguridad informática — Definicion.de. (2019). Retrieved from https://definicion.de/seguridad-informatica/

TRES TIPOS DE SEGURIDAD INFORMÁTICA QUE DEBES CONOCER | VIU

En el texto: ("Tres tipos de seguridad informática que debes conocer | VIU", 2019)

Bibliografía: Tres tipos de seguridad informática que debes conocer | VIU. (2019). Retrieved from https://www.universidadviu.com/tres-tipos-seguridad-informatica-debes-conocer/