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. Otros ejemplos menos comunes incluyen módulos de seguridad de hardware (HSM), los cuales suministran claves criptográficas para funciones críticas tales como el cifrado, descifrado y autenticación para varios sistemas. 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.

Entre los tipos de seguridad informática, este campo de la seguridad de software es relativamente nuevo. Los primeros libros y clases académicas sobre este tema aparecieron en 2001, lo que demuestra que ha sido recientemente cuando desarrolladores, arquitectos de software y científicos informáticos han comenzado a estudiar sistemáticamente cómo construir software seguro.

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.

¿Y cuáles son las amenazas a la red? Muchas amenazas a la seguridad de la red hoy en día se propagan a través de Internet. 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

Hay que entender que no hay una solución única que protege de una variedad de amenazas. 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

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