Publicado en Monzón el 21/07/2022

SPI Tecnologías explica los tipos de ataques en ciberseguridad

Diferentes términos desgraciadamente se han instalado en el vocabulario referentes a la ciberseguridad. A muchos les sonará el término troyano, malware, o más recientemente, phishing. Conocerlos puede contribuir a no caer en estos ataques cibernéticos.

Mejorar la seguridad en los dispositivos, o en las cuentas de correo electrónico y navegación es un reto de ciberseguridad al que tanto las empresas como los usuarios deben hacer frente y tomarse muy en serio. Desde SPI Tecnologías, expertos informáticos ubicados en Monzón, explican algunos de los tipos de ataques en ciberseguridad a tener en cuenta para evitar robos y secuestros de datos.

Conocer qué tipos de ataques existen contribuirá a prevenirlos. Los ciberataques, o ataques a los sistemas informáticos, se pueden clasificar en tres grupos:

Phishing attacks, Malware attacks y Web attacks.

Phishing

Los ataques con el método phishing son aquellos dirigidos a robar datos de los usuarios, ya sean contraseñas o números de tarjetas de crédito. Con este sistema, el delincuente se hace pasar por una persona de confianza, ya pueda ser su banco, o el equipo de soporte de una red social o web de confianza, y le manda un email o SMS con un enlace malicioso para que se haga clic en él. Con este enlace se puede causar la congelación de un sistema ransomware, revelar información confidencial o instalar un malware.

Este sistema es relativamente sencillo y fácil de usar, que para el usuario puede suponer el robo de identidad, de fondos o la realización de compras no autorizadas.

Dentro de este grupo, se pueden encontrar dos variantes distintas: el Spearfishing y el Whaling.

El término Spearfishing hace referencia a los ataques informáticos que tienen como objetivo una persona o empleado específico de una compañía en concreto. Estos ataques se llevan a cabo de forma más minuciosa. Los delincuentes recopilan información de los empleados y poco a poco se van ganando su confianza. Son ataques bastante usuales, pues el link en el que se tiene que acceder para robar la información está camuflado entre información que parece real.

Es una técnica que se usa para atacar a influencers, bancos o empresas.

La caza de ballenas, o whaling, hace referencia al tamaño del ataque, pues estos fraudes se focalizan en los altos directivos o CEO de las empresas. El fin es el mismo que en los otros métodos, el robo de información, pero más difíciles de que se lleven a cabo, pues los encargados de la seguridad en las empresas suelen detectarlos rápidamente.

Malware o software malicioso
Hace referencia a los ataques que afectan a los sistemas. Son códigos creados para que se instalen y corrompan el sistema informático de ordenadores, tablets o teléfonos móviles. El objetivo de este ataque suele ser el chantaje.

Éstos ciberataques no acostumbran a dañar los sistemas pero si vulneran los datos y la información.

Existen diferentes software a tal fin como pueden ser spyware, ransomware o troyanos.

- Ransomware. Es un software malicioso que una vez ha penetrado en el equipo, le otorga al hacker la capacidad de bloquearlo desde una ubicación remota y encriptar los archivos quitándole al usuario el control de toda la información y datos almacenados.

Estos softwares se instalan mediante descargas de sitios o webs no seguras. Los hackers acostumbran a pedir un rescate en forma de dinero para eliminar este software y permitir recuperar los documentos y accesos.

- Troyanos. Son softwares diseñados para parecer herramientas útiles y una vez se han instalado, toman el control de la máquina. Son unos de los más peligrosos, pues no se tiene consciencia de su instalación, tiene que acceder y controlar la máquina anfitriona sin ser advertido, bajo una apariencia inocua.

Ataques a la web
Inyección SQL. Es uno de los ataques más conocidos, un método de infiltración de un código intruso que se aprovecha de una vulnerabilidad informática presente en una aplicación, o sea, de errores de diseño en webs.

Estos ataques suponen una vulnerabilidad en la base de datos, lo que permite a los delincuentes robar, destruir y manipular datos.

Ataques XSS. Estos ataques se basan en webs de terceros para ejecutar secuencias de comandos en el navegador web de la víctima. Son comandos maliciosos que se envían a la web para desacreditarlas. Este es un sistema aunque puede resultar devastador, no es difícil de prevenir.

Como se puede ver hay una gran variedad de posibilidades por las que los piratas informáticos podrían

vulnerar la seguridad de los sistemas. Desde SPI Tecnología recomiendan instalar sistemas de prevención, además de consultar siempre con una persona de confianza si se tiene la menor duda de ser atacado.

Datos de contacto:
Enrique Español
974 415 571

Nota de prensa publicada en: Monzón

Categorías: Aragón E-Commerce Ciberseguridad Innovación Tecnológica