Sicrom

- Blog

Los tipos de ataques informáticos más comunes – Sicrom

#SICROMTeam 28.Ago.2018Seguridad

Tipos de ataques informáticos – Sicrom

El mundo está viviendo una auténtica **revolución tecnológica**. Todos los sectores están siendo digitalizados, desde la agricultura o la ganadería hasta la industria, el comercio, el turismo, etc. Este aumento en el uso de tecnología también ha provocado un **incremento en la cantidad de ciberataques**.

Hace unos años, los objetivos principales de los hackers eran las personas particulares. En la actualidad, la mayoría de ataques informáticos son **dirigidos a empresas**, y así lo demuestran los datos de los ataques informáticos en 2018.

Estos ataques provocan cuantiosas pérdidas en las empresas. Según el Instituto Nacional de Ciberseguridad (INCIBE), las **pérdidas medias** causadas por los incidentes de seguridad más comunes en las pymes son:

Ciberespionaje: 62.676€

Intrusión en la red de la empresa: 61.768€

DDoS (Denegación de Servicio): 48.122€

Phishing (suplantación de identidad): 43.583€

Vulnerabilidades en el software: 38.130€

Infección por malware: 28.144€

Fuga de información: 29.988€

La mejor manera de evitar ser víctima de estos tipos de ataque es conocerlos, así que en este post trataremos de explicar los más comunes y **cómo funcionan**.

Tipos de ataques informáticos

Existen **numerosos tipos de ciberataques**, cada uno con unas características o unos objetivos diferentes. Debido a la complejidad de sus nombres, la mayoría de ellos en inglés, es **complicado saber de qué se tratan**. Por ello, vamos a describir los principales ataques informáticos:

Malware

También llamado **software malicioso**, por su traducción del inglés (malicious software). Su función principal es **introducirse en un equipo y dañarlo** de diversas formas.

Las más comunes son las siguientes:

- **Virus**. El virus permanece inactivo hasta que un usuario lo ejecuta. En este momento el virus comienza a infectar los archivos extendiéndose por todo el equipo.
- **Worms (gusanos)**. El objetivo de los gusanos informáticos es infectar los archivos del equipo para difundirlos. Tienen la capacidad de extenderse a otros equipos sin necesidad de que un usuario los ejecute.
- **Troyanos**. Los troyanos muestran la apariencia de un programa fiable, pero esconden otro tipo de malware que es instalado automáticamente con el objetivo de tomar el control del equipo.
- **Keyloggers**. Son capaces de registrar todas las pulsaciones del teclado. Esta información es utilizada para conseguir contraseñas y datos de la víctima.
- **Spyware**. El objetivo principal de este malware es el robo de información.
- **Adware**. El adware se encarga de mostrar publicidad al usuario a través de banners, pop-ups, nuevas ventanas en el explorador... En muchos casos, el objetivo secundario también es obtener información sobre la actividad del usuario en la red.
- **Ransomware**. Es el tipo de ataque más común en la actualidad. Se basa en el cifrado de los datos, restringiendo el acceso a los archivos del equipo para pedir un pago por el rescate de los mismos. En la mayoría de los casos en bitcoins.

Denegación de servicio distribuido (DDoS)

Este tipo de ataque informático consiste en **generar una enorme cantidad de tráfico** desde numerosos dispositivos a un sitio web. Debido a este drástico aumento del tráfico, el rendimiento de la red disminuye hasta el punto de que dicha **red se satura** y se interrumpe su funcionamiento normal.

Los ataques DDoS son de los más difíciles de evitar debido a la complejidad que han adquirido durante estos últimos años y a la importancia que han adquirido las transacciones a través de Internet.

Ingeniería social

En la mayoría de los casos, los problemas informáticos son provocados por errores de los propios empleados, por ello es importante **capacitar a los usuarios**.

Muchos de estos ataques informáticos son a través del llamado **phishing**. Este tipo de ataques se basa en una **suplantación de identidad**.

El caso más común es el envío de un correo electrónico aparentemente de una entidad conocida (bancos, netflix, facebook...) en el que de algún modo conduce al usuario a un **enlace malicioso** donde **introduce su usuario y contraseña**.

Por ejemplo, el ataque de phishing sufrido este año suplantando la identidad de Caja Rural tuvo el siguiente procedimiento. El usuario recibía un email, aparentemente de Caja Rural, el cual decía que, debido a una nueva política de seguridad, su cuenta había sido suspendida y que, para restaurar el acceso, debía hacer clic en un enlace donde introducir sus credenciales.

Como podemos ver, existe una **enorme variedad de ataques informáticos**, cada uno con una función o un objetivo concreto.

Conociendo en qué consisten y cómo funcionan, podremos **estar alerta** y **saber detectar cuándo nuestra empresa está siendo víctima de los ciberdelincuentes**.