¿Qué es un ciberataque y qué tipos existen?

El confinamiento nos ha hecho aún más dependientes de la tecnología. El ordenador y el móvil no son solo imprescindibles para el ocio, sino que lo son para nuestro trabajo, y contienen en muchas ocasiones información personal sensible. En este contexto, la seguridad informática es más importante que nunca.

Hay que tener en cuenta que prácticamente toda la información que manejamos hoy en día son datos informáticos. Prácticamente ningún autónomo o empresa puede trabajar hoy sin herramientas informáticas. Por eso, para un particular o para una pequeña empresa estar protegidos frente a los ciberataques más comunes resulta casi tan crucial como tener bien protegido el hogar, el local donde desarrollan su negocio o sus oficinas.

Además, las amenazas informáticas no han dejado de crecer en los últimos años. La ciberdelincuencia es un negocio que atrae

cada vez a más criminales, que encuentran en las redes una lucrativa vía de negocio.

Se estima que los ciberataques tienen ya un coste anual de 45.000 millones de dólares para la economía mundial. En España, el Centro Criptológico Nacional publicó un informe en noviembre del año pasado, donde cifraba el número de ataques informáticos en 2018 en 38.192.

Los ciberataques se incrementaron en un 43,95% respecto a 2017. Según un informe que publicó Google el año pasado, las pymes son el principal objetivo de los ciberataques en España. Sin embargo, todavía hay muchas pymes y autónomos que no son conscientes del peligro. Por ejemplo, tan solo un 36% de las pymes encuestadas para el informe tenían protocolos básicos de seguridad informática y el 30% de las webs no disponían de protocolo https.

¿Qué es un ciberataque?

Un ciberataque, es un ataque a cualquier dispositivo remoto para alterar su funcionamiento normal, o bien extraer datos de él de forma ilegal, es decir, sin autorización. Los ciberataques pueden ir contra ordenadores y redes locales (no conectadas a Internet), o bien contra dispositivos conectados a Internet (computadoras, tablets, teléfonos inteligentes, tvs inteligentes, IoTs, etc).

Al igual que en la vida real un ataque es una agresión contra una persona o sus pertenencias (vehículo, casa, etc), en el ámbito elecrónico sucede lo mismo, es una agresión contra tus equipos electrónicos o los datos que hay en ellos. También se aplica el mismo término contra los servicios que están en la nube en Internet (como redes socials, email, etc).

¿Cuáles son los ciberataques más comunes?

Ya hemos definido previamente qué es un ciberataque, pero para no quedarnos solo con esa concepción, ahora vamos a ver qué tipos de ciberataques existen en la actualidad. Lo cierto es que hoy en día hay una gran diversidad de formas de atacar un equipo electrónico local o remoto. Muchas de ellas son nuevas, otras son tradicionales y hasta de antaño, pero que aún hoy siguen con vigencia.

Los ciberdelincuentes generalmente usan métodos manuales o bien bots automatizados para atacar organizaciones o personas, y para esto utilizan numerosas herramientas llamadas “red team toolkit”, o un arsenal de ataque en palabras claras. Ahora veremos algunas de als formas de ataque más comunes que se ven en la actualidad:

Hay muchos tipos de ciberataques, pero en los últimos tiempos han proliferado los de tres tipos:

- **Phishing:** comienza mediante un correo electrónico personal o correo corporativo en el que los delincuentes suplantan la identidad de una institución, una empresa o una persona de confianza. Esta apariencia de familiaridad les permite redirigir al usuario a una página web fraudulenta a través de un enlace o de un archivo adjunto infectado con software malicioso. Una vez allí, consiguen que la víctima introduzca en ella sus datos personales o bancarios.
- **Smishing:** en este caso,la suplantación se produce a través de SMS o de herramientas de mensajería instantánea como WhatsApp. A través de enlaces o adjuntos a los mensajes, los delincuentes solicitan al usuario que facilite datos personales o bancarios.
- **Vishing:** aquí el señuelo es una llamada telefónica, en la cual el delincuente suplanta la identidad de una

institución, empresa o persona. Suele tratarse de personas entrenadas para obtener precisamente la información que necesitan.

- **Malware**: se trata de software malicioso que incluye a otros subtipos como ransomware, troyanos y virus por ejemplo. Se caracterizan por infectar al ordenador y causar diversos daños de todo tipo y tamaño, incluyend desde encriptar parte de tu disco duro, hasta borrar datos, usar tu información a otras redes, usar tu equipo como centro de control remoto, entre otros. Los usuarios suelen infectarse de este tipo de malware haciendo click en páginas con links maliciosos, o en correos que incluyen links a sitios peligrosos.
- **Denegación de Servicio (DOS y DDOS)**: este es otro de los tipos de ciberataque más comunes, donde el objetivo del delincuente informático es saturar los servidores destino, para dejarlos inaccesibles, y asi causar que los usuarios no puedan acceder a dichos servicios. Los DOS (ataque desde una única dirección IP) y DDOS (ataques desde diferentes direcciones IP) suelen durar desde minutos a días, y dependen mucho de la cantidad de paquetes por segundo y Gbps que se envíen a la víctima.

¿Cómo puedo protegerme de un ciberataque?

Por todo esto, resulta de vital importancia protegerse de estos ciberataques siguiendo algunas pautas básicas. Revisar la seguridad de los dispositivos, cambiar la conexión wifi establecida por defecto, utilizar contraseñas diferentes y seguras en los distintos servicios web, fijarse siempre que estamos accediendo a páginas seguras antes de suministrar datos bancarios o evitar la descarga de aplicaciones no seguras o desde sitios no oficiales son algunas claves.

Ten también en cuenta que ningún organismo o entidad oficial

te solicitará datos personales por WhatsApp, correo electrónico o sms, y que nadie debe pedirte una clave por teléfono.

Conclusión

Hoy pudimos analizar en detalle qué es un ciberataque, para qué se utilizan, y los diferentes tipos de ciberataque que utilizan los hackers maliciosos contra la información de tus dispositivos electrónicos, como también contra las diferentes organizaciones y compañias del mundo.
Los ciberdelincuentes siempre suelen estar un paso por delante, por lo que tomar las medidas necesarias para evitar caer presa de sus trampas es algo funadmental tanto en lo personal, como si trabajas en ámbitos corporativos. Adoptar las mejores prácticas básicas de ciberseguridad te asegurará que detengas la mayor parte de los ataques, que no es poco, y es al menos un buen comienzo para tener siempre tus redes y equipos seguros.

Fuente: tecnomagazine.