

Amenazas contra la ciberseguridad más comunes en 2022

Nadie se salva de poder ser víctima de un ciberataque, prueba de ello es el sufrido por el CSIC español proveniente de Rusia.

FUENTE: REDACCIÓN COMPUTING

Tras años de descenso en la cifra de denuncias por ciberataques informáticos, durante las vacaciones de verano, donde aumentan las descargas de apps para jugar al casino online con dinero, ocio, o el tráfico en plataformas de contenido digital, de compras o reservas hoteleras, han hecho que los ciberdelincuentes vuelvan estar en la mira del cuerpo de delitos informáticos al observarse un repunte de casos de ataques informáticos desde el inicio de las vacaciones veraniegas.

Nadie se salva de poder ser víctima de un ciberataque, prueba de ello es el sufrido por el CSIC español (Consejo Superior de Investigación Científica) proveniente de Rusia y que dejó a la mayoría de centros de investigación del Ministerio de Ciencia e Innovación sin conexión a internet durante 15 días.

El ataque en esta ocasión fue de los llamados ransomware, de las más utilizados durante los últimos años por ciberdelincuentes. Este ataque en concreto hace que tras acceder el ciberdelincuente al equipo mediante una descarga encripte la información para pedir posteriormente un rescate.

Junto al ransomware son muchas las puertas que un ciberdelincuente puede abrir para hacerse con los datos de sus víctimas, por eso es importante tener en cuenta cuales son los posibles ataques que podemos sufrir y como protegernos de ellos.

¿Cómo se pueden evitar ciberataques?

Uno de los recursos más utilizados en los ciberataques son las descargas de aplicaciones maliciosas, que son las que dan acceso al dispositivo de quien las descarga.

Por ello siempre es recomendable realizar las descargas desde un programador verificado o de una app store oficial. Aunque por desgracia esto último no asegura al 100% estar libre de aplicaciones maliciosas. Como pasa en Google Play donde luchan por eliminar de su catálogo de aplicaciones las que puedan resultar sospechosas.

En los últimos meses se han llegado a eliminar aplicaciones con malware como Joker, Coper o Facestealer.

Otro de los objetivos principales para lanzar un ataque son la base de datos de empresas. Sin importar el número de empleados o sus cifras de facturación.

Los ciberdelincuentes saben de sobra de que el tráfico de datos internos de millones de empresas de todo el mundo pasa por la nube de ahí que se hayan convertido en las víctimas más atacadas, sobre todo en datos almacenados en Google Drive.

Para evitar riesgos siempre se recomienda verificar el remitente, no descargar nunca un archivo externo de un remitente externo a la empresa y sobre todo contar con un backup de todo el contenido almacenado en la nube.

Hay que añadir que no hay que descuidar el mantenimiento de la seguridad de los equipos y contar con toda la información manteniéndose al día sobre cómo hacer frente al momento de ser víctimas de un ciberataque o cómo reaccionar si creemos que podemos sufrirlo.

Para ayudar con eso, ya son muchas las empresas que ponen a disposición de sus empleados cursos gratuitos sobre ciberseguridad.

Una evaluación continua de la red, nuestros equipos y sistemas de acceso seguro les hará la vida más difícil a los ciberdelincuentes y nos ahorrará más de un dolor de cabeza.

Fuente: *COMPUTING*