

Ciberataques aumentan en 40% por la pandemia

Los ciberataques, conocidos como acciones que buscan vulnerar los sistemas de información, están registrando un aumento sustancial año tras año y más aún en momentos que el mundo padece de una crisis sanitaria.

Al respecto, el managing director de la consultora Axus Advisory Group, **Claudio Querol**, comentó que si bien es difícil precisar el número de ataques cibernéticos, se estima que en el mundo se dan entre 700.000 a 900.000 reportes diarios, es decir unos 35.000 por hora.

Según el ranking global de **Kaspersky**, entre los países que reciben más ciberataques están los **Estado Unidos**, el Reino Unido, India, Rusia y China. El Perú se ubica en el puesto 20.

El experto en ciberseguridad afirmó, además, que en los últimos cinco años, los ataques cibernéticos han aumentado entre 15% y 20% año a año, y a julio de 2020 se observa un aumento del 40% frente al total del año anterior.

“Los ciberdelincuentes aprovechan el miedo, la curiosidad y la necesidad de las personas para lanzar nuevos ataques a fin de suplantar la identidad y tener acceso a información privilegiada sea de instituciones de salud, bancos, etc.”, remarcó Querol.

Además, señaló que entre los usuarios que reciben mayores ciberataques son los de **Windows** y **Android**, principalmente porque estos dos sistemas operativos tienen 70% o más en mercados los distintos mercados donde operan.

En ese sentido, Querol resalto que es fundamental tener siempre la última actualización del sistema operativo en uso, pues esa versión corrige sus vulnerabilidades.

Por otro lado, indico que esta problemática genera un gran impacto económico en el mundo. La suma total bordea los US\$ 600.000 millones, casi 1% del PBI mundial.

Y más alarmantes son las cifras del **Foro Económico Mundial (WEF)**, por sus siglas en inglés), dadas a fines de 2019, donde los ataques cibernéticos generarían pérdidas económicas de US\$ 5.2 trillones entre 2020 al 2023.

Precisamente el malware y el phishing son los ataques informáticos que generan más costos económicos a las empresas.

El primero es un software malicioso que se introduce para dañar los sistemas operativos y sustraer información, mientras el segundo busca suplantar la identidad de las personas para el robo. Este último ha registrado un aumento significativo del 600% desde febrero.

“Más del 90% de las brechas en ciberseguridad se dan por error humano. Los atacantes buscan explotar el eslabón más débil (las personas) con ingeniería social (manipulación) y ataques de phishing”, manifestó.

Por lo descrito, el experto recomendó a las empresas, instituciones gubernamentales y demás organismos, contar con estrategias que ayuden en sus procesos de digitalización y les garanticen el adecuado respaldo de los datos informáticos.

“Los ataques cibernéticos son cada día más sofisticados y ahora con la modalidad de teletrabajo, los esfuerzos en temas de ciberseguridad debe ser mayores, analizando las conexiones remotas, la seguridad en los dispositivos y sobre todo capacitar al personal”, anotó.