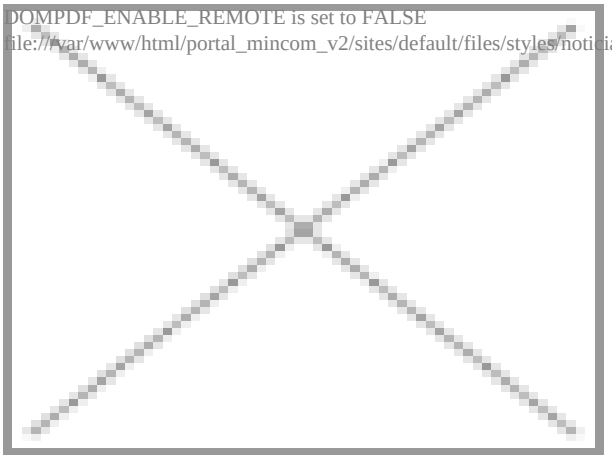

Fuente:
Tomado de CubaSí Omar Pérez Salomón

En lo que va de año han crecido los ciberataques a nivel mundial – en lo fundamental con la presencia de ransomware1, phishing, robos de identidades, ataques a las infraestructuras y entornos en la nube - motivado en lo fundamental por la evolución de la transformación digital, el auge del teletrabajo y la ausencia de una estrategia proactiva en la gestión de vulnerabilidades en las diferentes entidades.

También se ha identificado dificultades en la actualización de los sistemas y soluciones, en la no utilización de empresas especializadas, la resiliencia ante incidentes, insuficiente inversión en materia de ciberseguridad y la preparación de los especialistas, entre otras.

Sobre el panorama actual de la ciberseguridad a escala internacional estaremos hablando con Daniel Ramos Fernández, director de negocios digitales de la Empresa de Telecomunicaciones de Cuba (ETECSA) y experto en sistemas informáticos y ciberseguridad.

DRF: Las previsiones en ciberseguridad para el presente año, expuestas por la compañía rusa de ciberseguridad Kaspersky en diciembre de 2022, de manera general se vienen cumpliendo transcurrido el tercer trimestre del año. Filtraciones de datos de proveedores de servicios públicos, ciberataques por motivos políticos y el robo de datos personales y médicos han tenido un impacto en el presente.

El ransomware ha sido una de las mayores amenazas para las empresas. Entre las principales preocupaciones están el robo o fuga de información, el insuficiente presupuesto asignado al área de ciberseguridad y la búsqueda de soluciones de seguridad eficaces.

A mediados de septiembre varios medios de comunicación informaron sobre un ciberataque de gran magnitud que afectó a entidades públicas y privadas de Colombia, Chile y Panamá. El centro del incidente fue IFX Networks, multinacional de telecomunicaciones, data centers y soluciones TI. Solo en Colombia afectó los sistemas de información y el funcionamiento de plataformas de servicios en más de 40 entidades públicas de los sectores jurídico, cultura, salud, agricultura y comercio exterior, en este último afectando las exportaciones del país.

Recientemente, el Servicio Nacional de Aduanas de Chile informó de un ciberataque a sus equipos informáticos, que afectó la interacción de usuarios importadores y exportadores de ese país con el servicio aduanero. También se han reportado ciberataques al centro de datos de la compañía Air Europa, a la empresa estadounidense 23andMe, especializada en hacer estudios genéticos, al sitio de la Dirección General de Migración de República Dominicana y el del Ayuntamiento de Sevilla.

Los datos del reciente Panorama de Amenazas de Kaspersky revelan que la tasa de ataques de malware

contra computadoras en América Latina se mantuvo estable en el último año en relación con el precedente. En total se registraron 1190 millones de bloqueos, lo que representa un promedio de 37.9 intentos de ataque por segundo en la región. Brasil ha sido el principal objetivo de estos ataques, registrando una media de 1515 bloqueos por minuto, seguido de México (275), Colombia (117) y Perú (107). Los sectores más atacados fueron las entidades gubernamentales (15.49% de los intentos de infección) agrícola (11.82%), comercio minorista/mayorista (11.55%), industria (8.57%), educación (6.92%), salud (5.28%), TI/Telecomunicaciones (4.55%) y el financiero y de seguros (4.55%). 2

OPS: ¿Cuáles son las principales causas de este panorama?

DRF: Entre las principales amenazas detectadas destaca el uso de productos que contienen algún tipo de malware, además de no contar con las correcciones o parches de seguridad correspondientes para atender vulnerabilidades que los ciberdelincuentes podrían aprovechar. En América Latina el 66% del software utilizado es pirata, casi el doble del promedio mundial que es del 35%.

También existen programas maliciosos que muestran publicidad no solicitada por la víctima, direcciones falsas, archivos PDF maliciosos y troyanos. Las técnicas utilizadas por los ciberdelincuentes son siempre las mismas: un mensaje fraudulento para llevar a las víctimas a un sitio web falso, correos electrónicos con un archivo malicioso adjunto para infectar el dispositivo e infecciones durante la navegación.

OSP: Y el escenario cubano, ¿cómo lo valora?

DRF: En nuestro país la cantidad de incidentes en lo que va de año crece en relación a igual período del año 2022. Las causas principales están asociadas a la ocurrencia de ciberataques de denegación de servicios (DoS/DDoS), el envío y recepción de correos no deseados (SPAM), tráfico malicioso generado por códigos malignos, escaneos de servicios y explotación de vulnerabilidades que han comprometido sitios web y otros elementos informáticos y en el caso de las personas naturales, ciberacoso, suplantación de identidad, y estafas a través de las redes sociales digitales y canales electrónicos de pago. Han estado presente ciberataques por motivos políticos, que en lo fundamental modifican el aspecto de la página web total o parcialmente.

A pesar de las limitaciones económicas del país, se trabaja en fortalecer la ciberseguridad en los sectores y actividades estratégicas, mejorar la gestión ante incidentes, incrementar el nivel de preparación de los directivos y especialistas e incrementar las acciones de comunicación para incidir sobre la disciplina y la prevención de riesgos en el uso adecuado de las Tecnologías de la Información y la Comunicación (TIC) en las personas naturales.

Nota

1 Tipo de ciberataque en el que los delincuentes cifran los archivos o sistemas informáticos de una víctima y luego exigen un rescate para proporcionar la clave o herramienta necesaria para desbloquear los archivos o sistemas.

2 https://latam.kaspersky.com [1]. Panorama de amenazas de Kaspersky.

Links
[1] https://latam.kaspersky.com