SE ESPERA QUE ESTE AÑO, el mundo invierta casi US$ 500.000 millones en ciberseguridad, pero un solo ataque global cuesta US$ 4,88 millones.

AMENAZAS EMERGENTES:

Las seis tendencias de ataques que ponen en riesgo el escenario actual

Juanita Duque, cofundadora y CEO de Seccuri, enfatizó que se debe pensar "desde el instante" y responder rápidamente a los cibercrímenes.

IVÁN SILVA I.

"El año pasado se registraron 600 millones de ataques diarios a nivel internacional, sumando 219 trillones en todo el planeta. Este año esperamos que el mundo invierta casi US$ 500.000 millones en ciberseguridad, pero solo un ataque global cuesta US$ 4,8 millones.

Con esas cifras, la cofundadora y *chief executive officer* (CEO) de Seccuri, Juanita Duque, graficó los riesgos emergentes en esta materia, en el Cybertech South America 2025.

En todo el orbe, el 70% de las empresas no tiene equipos de ciberseguridad por carecer del conocimiento necesario de este riesgo. "El cibercrimen sigue siendo uno de los más grandes e impresionantes. Le costará al mundo cerca de US$ 24.000 millones en 2027", proyectó.

La experta detalló seis tendencias de ataques que amenazan el presente:

ACCESO A TRAVÉS DE *SINGLE SIGN-ON* (SSO): permite a los usuarios entrar a múltiples cuentas o *apps* con una única autenticación, sin tener que recordar o ingresar diferentes contraseñas repetidamente. Si no están bien protegidas con varios factores de autenticación o no se crea una cultura de conciencia de ciberriesgo, un ciberdelincuente puede acceder fácilmente a los sistemas.

ADVERSARIOS CON IA NO RESTRINGIDA Y *DEEPFAKES:* Se refiere a *hackers* que se hacen pasar por otros para robar información a través de audios, videos e imágenes alteradas digitalmente, creando la impresión de que alguien hace o dice algo que en realidad no sucedió.

***RANSOMWARE* A OT E ICS:** tipo de *malware* que retiene los datos tradicionales, operativos (OT) y de sistemas de control industrial (ICS), amenazando con mantenerlos bloqueados a menos que se pague un rescate. Esto se conoce como secuestro de información. Se están viendo tendencias en *ransomware* a OT, causando riesgos a la infraestructura crítica.

ATAQUES DAÑINOS A OT E ICS: se realizan mediante diversas formas, como *botnets* para internet de las cosas (IoT), que atacan redes eléctricas, sistemas de salud y de transporte. Pueden vulnerar controles industriales.

FALTA DE *LOGGING:* significa que no se está recopilando y analizando información suficiente para identificar actividades sospechosas o no autorizadas.

FALTA DE HABILIDADES DE CIBERSEGURIDAD: apunta a la carencia de profesionales con la formación, experiencia y conocimientos necesarios para proteger los sistemas y datos contra las ciberamenazas.