Nota de prensa
15/02/2023

Ciberseguridad: riesgos y ataques más comunes que enfrentarán las empresas este 2023

- *Según la Encuesta de Adopción Digital Pymes-Perú realizada por Movistar Empresas, el 63% de las empresas encuestadas aseguró que planea implementar soluciones en ciberseguridad para proteger sus* dispositivos, redes y sistemas informáticos.
- *Entre los riesgos más comunes destacan los vinculados al robo de información, secuestro de datos y los ataques de denegación de servicio, que generan que los usuarios no puedan acceder a la información de sus empresas.*

Lima, 15 febrero de 2023.- Durante estos últimos tres años hemos visto un creciente número de incidentes y amenazas cibernéticas en Perú y en Latinoamérica debido en gran parte a esta dinámica de sociedad cada vez más hiperconectada a raíz de la pandemia. A la par, vemos que las empresas e instituciones han incrementado sus inversiones para proteger sus activos digitales, aplicando políticas y procedimientos internos para salvaguardar la información tanto a nivel de corporaciones como pymes.

Según la Encuesta de Adopción Digital Pymes-Perú realizada por Movistar Empresas, el 63% de las empresas entrevistadas aseguró que planea implementar soluciones en ciberseguridad para proteger en forma integral sus dispositivos, redes y sistemas informáticos. Sin embargo, aún existe un gran desafío para mejorar la capacidad de detección y respuesta ante incidentes de seguridad dada la rápida y continua evolución en las técnicas de los ciber atacantes.

Al respecto, Roberto Igei, Jefe de Productos Digitales B2B de Movistar Empresas, explica: “A medida que las empresas han acelerado su transformación digital, también se han incrementado y sofisticado los tipos de ciberataques. Por ello incidimos en que la ciberseguridad requiere de una estrategia integral a nivel compañía, donde deben estar siempre actualizados y preparados para enfrentar nuevas amenazas cibernéticas con técnicas de ataque cada vez más avanzadas que dificultan su detección”.

En esa línea, Igei comenta cuáles son los riesgos y ataques más comunes que este año continuarán siendo una amenaza para las organizaciones:

- **Robo de información:** entre las formas más frecuentes de ciberataques, destacan los destinados a robar información a través de la ingeniería social para obtener información confidencial de los usuarios. Entre estos se encuentran los engaños por correo electrónico (phishing), por llamadas de voz (vishing) y por mensajes de texto (smishing). En todos estos casos pueden afectar a personas naturales y también a ejecutivos que manejan y acceden a información privilegiada dentro de sus organizaciones.

- **Secuestro de datos y sistemas informáticos:** el ransomware es un tipo de software malicioso ampliamente utilizado por los ciberdelincuentes para bloquear el acceso a un sistema informático o a los datos que se encuentran en él, y solicitar a cambio del desbloqueo sumas cuantiosas de dinero. El ransomware infecta plataformas informáticas o incluso dispositivos personales, con métodos como el envío malicioso de emails y/o SMS (phishing, smishing) para que el usuario acceda al engaño, y una vez infectado el dispositivo los ciberdelincuentes utilizan técnicas de distribución masiva para secuestrar otros equipos dentro de la red.

- **Ataques de denegación de servicio (DDoS):** este es un tipo de ciberataque donde un actor malicioso interrumpe el funcionamiento de un ordenador u otro dispositivo para que no esté

disponible para los usuarios a los que está dirigido. Para lograrlo, sobrecarga las plataformas informáticas (o el servicio) objetivo con solicitudes de acceso provenientes de diversos dispositivos (botnets) ubicados en cualquier lugar, hasta generar un tráfico que no puede ser procesado y así genera una caída del servicio que afecta a cualquier usuario legítimo que quiera acceder.

“Estas nuevas formas de ataque se vienen sofisticando rápidamente con el uso intensivo de la Inteligencia Artificial (IA), lo cual también genera que las organizaciones deban automatizar los procesos de detección y respuesta con el uso de herramientas igualmente potenciadas con esta tecnología. Aquí radica la importancia de contratar servicios especializados de un Centro de Operaciones de Seguridad (SOC) para afrontar adecuadamente esta realidad”, añade Igei.