En crímenes digitales, el eslabón débil es humano

Por el Staff de El Inversionista

En el mapa global de la ciberseguridad, México ocupa una posición estratégica que también lo expone a las amenazas. Nuestro país no es un actor secundario en la disputa digital: se ha convertido en un punto de interés constante para grupos delictivos que operan a escala internacional.

Para entender el momento actual y el papel que tendrá la inteligencia artificial (IA) en el corto plazo, Ryan Kalember, director de estrategia de Proofpoint, y Luis Isselin, director regional en México de la misma empresa, describen un escenario claro: la tecnología avanza con rapidez, pero la principal debilidad sigue siendo humana.

En el plano nacional, el panorama no es uniforme. Existen grandes corporativos con sistemas de protección sólidos, pero muchas empresas aún presentan carencias.

"La cultura de ciberseguridad está, digamos, en desarrollo", afirma Isselin.

Esa diferencia ha llevado a que los ataques cambien de forma. En vez de dirigirse de manera directa contra grandes compañías, los delincuentes optan por caminos indirectos, como las cadenas de suministro.

En vez de dirigirse de manera directa contra grandes compañías, los delincuentes optan por caminos indirectos, como las cadenas de suministro

La lógica es sencilla. En vez de enfrentar los sistemas de seguridad de una gran empresa, buscan vulnerar a un proveedor pequeño que cuenta con menos recursos para protegerse.

"Al tercerizar ese acceso, por decirlo, vulnero a una empresa pequeña y puede ser que tenga una relación comercial con la tuya, que es más grande", explica Isselin. Por medio de relaciones comerciales legítimas, logran entrar a redes corporativas de mayor tamaño.

La posición de México como socio comercial clave de Estados Unidos aumenta esa exposición. Su papel como exportador e importador relevante lo coloca "de manera muy visible para ser un objetivo", señala el directivo.

Kalember añade otro elemento que complica el entorno: la existencia de estructuras financieras ilícitas que permiten convertir recursos obtenidos mediante fraudes digitales en dinero utilizable, con vínculos internacionales que facilitan ese proceso.

La información: objetivo

En este contexto, el principal botín no es el equipo físico, sino la información. El robo de credenciales a través de correos falsos, conocido como phishing, sigue entre los métodos más efectivos. "Lo que el ciberdelincuente quiere es tener acceso a la información que tienes a tu disposición", resume Kalember.

La protección de datos enfrenta obstáculos dentro de las propias organizaciones. Isselin explica que algunos empleados intentan evadir controles cuando buscan extraer información antes de cambiar de empleo.

En ocasiones modifican el nombre de documentos confidenciales para intentar superar filtros de seguridad.

A esto se suma un problema adicional: muchas empresas aseguran contar con herramientas para evitar la pérdida de datos, pero no siempre existe certeza de que funcionen como se requiere.

"Hay una disparidad entre la percepción de 'yo ya tengo algo y ese algo está a la altura de lo que se necesita'", advierte.

Kalember aporta un punto práctico que ayuda a entender el fenómeno: "la mayoría de los ataques van a pasar por el correo o el navegador". Si las empresas concentran su vigilancia en herramientas de uso diario, como el correo electrónico y los navegadores, pueden reducir una parte importante del riesgo.