Empresas frente a los ciberataques: protocolos y respuestas frente a los hackers

En un mundo cada vez más digitalizado, las empresas enfrentan un desafío constante: proteger su información y sistemas frente a los ciberataques.

Desde el robo de datos confidenciales hasta la interrupción de operaciones críticas, los hackers emplean técnicas cada vez más sofisticadas para vulnerar la seguridad corporativa.

Ante esta situación que genera un peligro inminente para los negocios, Kenneth Tovar, Country Manager de Palo Alto Networks para Perú y Bolivia, sostiene que los tipos de amenazas más sofisticadas son el ransomware, el phishing dirigido (spear phishing), ataques a la cadena de suministro y amenazas internas.

Sin embargo, hoy en día se ha visto un incremento en ataques impulsados por la inteligencia artificial (IA), que automatizan y mejoran la efectividad y sofisticación de las campañas maliciosas.

"Esta tendencia amenaza principalmente a las entidades bancarias y financieras. Los ciberdelincuentes pueden 'clonar' el aspecto de una aplicación de un banco para hacer creer a la víctima que está en la aplicación correcta para así sustraer información", indica.

Por otro lado, también manifiesta que se encuentran amenazas avanzadas persistentes (APT), que son ataques sofisticados y prolongados en el tiempo que buscan infiltrarse en las redes de las instituciones para robar información crítica o sabotear

operaciones.

El ataque a las MYPES

Según menciona Tovar, existe la percepción errónea de que solo las grandes corporaciones son objetivos de ataques cibernéticos, lo que hace que muchas micro y pequeñas empresas (mypes) subestimen los riesgos.

“Para una micro o pequeña empresa, lo más importante es comenzar con soluciones que brinden visibilidad y protección en tiempo real. Una prioridad es proteger sus redes, ya que toda empresa en la actualidad trabaja conectada a internet”, dijo.

Otra prioridad es reforzar la seguridad en los Endpoints (PC, laptops, servidores) dentro de la misma plataforma que unifique tanto la seguridad de red como del Endpoint.

Por ello, recomienda capacitar a todo el personal (técnico o tecnológico), ya que una cultura organizacional con conciencia cibernética reduce notablemente el riesgo de ataques exitosos por ingeniería social.

“Una técnica utilizada por ciberdelincuentes que consiste en manipular a los empleados para que revelen información confidencial, como contraseñas o accesos, haciéndose pasar por figuras de confianza”, precisa.

LEA TAMBIÉN: Ciberseguridad para pymes: pasos clave para evitar ataques digitales

La IA contra la IA

Tovar menciona que la rápida integración de la IA ha generado una innovación sin precedentes, pero conlleva una advertencia crítica: los actores maliciosos están buscando formas de aprovecharse de ella, y ya lo hacen, la IA permite incluso a los actores menos experimentados llevar a cabo ciberataques con éxito.

"A medida que tanto los atacantes como los defensores intensifiquen el uso de la IA, el campo de batalla cibernético se convertirá en una carrera armamentista cibernética continua entre IA e IA, donde la velocidad, la adaptabilidad y la sofisticación dictarán el éxito de las futuras operaciones

cibernéticas”, indica.

Recomendaciones

Luis Chávez, líder de Educación en Prevención de Fraudes del BCP, comparte cinco recomendaciones claves para evitar caer en estas trampas.

1. **No tomar decisiones impulsivas:** los estafadores aprovechan momentos de alta expectativa para captar la atención con supuestas promociones limitadas, regalos instantáneos o inversiones que multiplican tu dinero fácilmente.
2. **Verificar siempre la fuente:** revisar con atención el nombre del usuario y asegurarse de que se trate de la cuenta o página oficial de la fuente de información.
3. **Si suena demasiado bueno, probablemente no es real:** desconfiar de las promociones que prometen ganancias rápidas o premios increíbles sin sorteos.
4. **Cuidado con la presión por actuar rápido:** los estafadores suelen crear un falso sentido de urgencia. Si una oferta aparece “solo por hoy” y piden ingresar datos de la tarjeta, clave, token o CVV de manera inmediata, hay que desconfiar. Esa presión es parte del engaño.
5. **Presta atención a las señales:** buscar expresiones faciales que no coinciden con el tono de la voz, parpadeos raros o movimientos desincronizados entre los labios y el audio. Además, las voces generadas por la IA suelen sonar planas, o con una entonación extraña.

Recordemos que las regulaciones, como la Ley de Protección de Datos en Perú, están empujando a las empresas a adoptar buenas prácticas como obtener consentimiento de los usuarios para procesar sus datos, notificar incidentes de ciberseguridad o implementar medidas para proteger datos contra acceso no autorizado. Es por ello que se recomienda que ante el primer

ataque denuncien y apliquen los protocolos de seguridad.

LEA MÁS:

El futuro de la inteligencia artificial en la medicina y la salud

10 usos de la inteligencia artificial que facilitan la vida diaria