Ciberseguridad en 2024: más sofisticada y dominada por la IA

La tecnología seguirá progresando en 2024 y con ella los desafíos en áreas como la ciberseguridad. La falta de profesionales del sector, los ciberataques geopolíticos o las vulnerabilidades en aplicaciones móviles o cascos de realidad virtual estarán en el foco y todo ello dominado por la inteligencia artificial.

Las ciberestafas serán cada vez más complejas y sofisticadas, con el ‘ransomware’ entre las principales amenazas, un programa malicioso que toma el control de los equipos del usuario, para luego exigirle el pago de un rescate a cambio de recuperar el control y la información.

Un año más, la primera defensa de los usuarios es mantener el software actualizado, utilizar antivirus y ser escépticos.

La inteligencia artificial, en escena

Los expertos vaticinan para 2024 ‘una nueva era’ del cibercrimen avanzado y sitúan a la IA como una de las grandes transformadoras de las reglas del juego.

Con el crecimiento de las operaciones de ciberdelincuencia como servicio (CaaS) -subcontratación de programas maliciosos a través de la web oscura- y la llegada de la IA generativa, los actores de amenazas tienen más herramientas «fáciles» a su alcance para perpetrar sus ataques, detalla Fortinet.

«Se prevé que aumenten la sofisticación de sus actividades. Lanzarán ataques más selectivos y sigilosos diseñados para eludir los controles de seguridad más estrictos y se volverán más ágiles al hacer más eficiente cada táctica del ciclo de ataque», agrega la compañía.

Llega un nuevo año y la innovación tecnológica no para. «La tecnología del futuro -del presente continuo, más bien- avanza al mismo ritmo para ‘hackers’ y ciberdelincuentes que también estudian, investigan y diseñan maneras de utilizarla para llegar hasta nuestro dinero o datos», apunta por su parte Panda Security.

«Los ciberdelincuentes van a utilizar la IA, nuestros

dispositivos tecnológicos favoritos y mucho más para derribar nuestras defensas y acceder a nuestro datos personales».

Panda vaticina que, entre otros, aumentarán las ventas de herramientas de ‘phishing’ (mensajes suplantando a una entidad legítima) con IA en la internet oscura. «Empezaremos a ver (sufrir) un mercado negro cada vez mayor de herramientas de ‘phishing’ automatizadas que inundarán correos, teléfonos y dispositivos inteligentes».

Además, despegará el ‘vishing’ -‘phishing’ por voz- basado en IA. A través de una llamada, se suplanta la identidad de una empresa, organización o persona de confianza, con el fin de obtener información personal y sensible de la víctima.

Ojo a los cascos de realidad virtual

El «desenfrenado» uso de códigos QR y los cascos de realidad virtual y mixta serán otro de los focos de la ciberseguridad. Panda señala en su web que en 2024 «veremos cómo un investigador o un pirata informático malintencionado encuentra la manera de recopilar o acceder a los datos de los sensores de los auriculares y recrear el entorno en el que juegan los usuarios».

Estos cascos ofrecen una gran cantidad de información nueva y personal que puede ser robada, monetizada y utilizada como arma por los malhechores, por ejemplo, el diseño o ubicación exacta de nuestro hogar.

Si bien sus creadores trabajan para diseñar e incorporar protecciones para evitar que software o actores maliciosos obtengan acceso, «la puerta de la casa está ahí, y los ciberatacantes que tengan interés probablemente acabarán encontrando la manera de entrar».

Las organizaciones son conscientes cada vez más de las consecuencias que un ataque a sus sistemas y redes puede tener, en término de paralización de la actividad, pérdidas económicas o de reputación.

Según Innovery, en 2024 seguirán aumentando en frecuencia y complejidad, con el ‘ransomware’ como una de las principales amenazas, especialmente en la administración pública y los sectores de sanidad y venta al detalle o ‘retail’.

Citando un estudio de IBM, menciona que el 95 % de las empresas en el mundo ha sufrido más de una violación y esta tendencia va a continuar, pues las compañías están migrando a la nube sin implementar una arquitectura de seguridad robusta que evite las

filtraciones.

Otro de los desafíos, además de la ciberguerra que busca neutralizar industrias que son críticas a nivel estratégico y táctico, es la falta de talento. Según Innovery, las empresas se están enfrentando a la escasez de profesionales especializados en ciberseguridad (por ejemplo en España son necesarios más de 25.000).

Aunque las ciberamenazas continúen, los autores de estas «no tienen por qué tener la sartén por el mango», subrayan desde Fortinet. Las organizaciones, entre otros, tienen un papel fundamental en esta lucha, lo que comienza con la creación de una cultura de 'ciberresilencia', hacer de la ciberseguridad un trabajo de todos.

Y es que, apunta Innovery, el factor humano sigue siendo el eslabón más débil de la cadena.

Además del sentido común, desde el Instituto Nacional de Ciberseguridad (Incibe) apuntan algunos consejos para estar protegidos: informarse sobre los principales fraudes que circulan por la red, no proporcionar datos a la ligera, investigar la tienda antes de comprar, utilizar métodos de pago seguro o diversificar las contraseñas.

«El 2024 se presenta como un año emocionante en términos de ciberseguridad. La IA, probablemente, será el perejil de todas las salsas, tanto en el lado de los defensores como en el de los atacantes, por eso es clave seguir investigando, desarrollando y, sobre todo, protegiéndonos», concluye Hervé Lambert, de Panda.

Con información de 800 noticias