Llega la sexta generación de ataques informáticos: más grandes, más rápidos y más sofisticados

La delincuencia informática avanza al mismo ritmo que la tecnología e incluso va por delante. Los ataques van ya por la quinta generación. De los virus de los noventa se pasó a la interferencia de las redes, a la intromisión en las aplicaciones, a los robos de datos y, en los últimos años, a los grandes ataques globales. Pero este año, expertos en seguridad reunidos en el Cybertech de Tel Aviv (Israel), el mayor encuentro internacional del sector, esperan un recrudecimiento de la ofensiva criminal: la sexta generación.

Las puertas de entrada de los ataques informáticos se han multiplicado, se considera que se está produciendo un fenómeno de escala global similar a una carrera armamentística. "Serán más fuertes, más rápidos, más sofisticados. Aprovecharán todo el mundo conectado, desde las nubes de información, los coches o las redes sociales hasta subtítulos, juegos, drones o elementos aparentemente inofensivos como los juegos o las aspiradoras robotizadas".

Ya no vale proteger a una sola organización, sino que también es necesario el control de los proveedores. Un atacante busca el camino más corto, más rápido y más indefenso. Son profesionales, no van en pijama. La seguridad es una necesidad y hay que ir por delante, pasar a la ofensiva. El coste de un error es realmente alto.

La solución global pasa por que las máquinas sustituyan a los hombres" en la prevención, detección y resolución de los ataques. Es la aplicación de la inteligencia artificial con "superpoderes".

El problema, del que se ha hablado en la última cumbre de máximos dirigentes internacionales, se ha situado a la escala del cambio climático o los desastres naturales.

Las cifras avalan la preocupación global. Cada día se registran un

millón de alertas de otros tantos tipos de ataques. Hace una década, las formas de atacar se reducían a unas 50 y las amenazas diarias registradas eran un millar. Se realizan cuatro millones de simulaciones cada jornada para analizar ataques que van desde la nube a cualquier tipo de dispositivo.

"La nube es fundamental porque aporta la seguridad antes de que lleguen a los dispositivos" mencionan expertos. Esta estrategia de ofensiva y actuación rápida ha sido exitosa. Israel ha presentado el pasado año un balance de "cero daños por ataques", de acuerdo con Yigal Unna, director general del directorio israelí de ciberseguridad.

La obsesión del Gobierno israelí por cubrir todos los frentes vulnerables ante los ciberataques, que aseguran que les convierte en el segundo país más amenazado por detrás de Estados Unidos, ha llevado a los responsables de seguridad a crear un teléfono gratuito de emergencias informáticas similar al 112.

El servicio, que cuenta con el número de teléfono 119, recibe unas 540 llamadas diarias y registran unos 40 casos de *phising*, 12 infectaciones pormalware,20 alertas por vulnerabilidad y 40 avisos internacionales.

Cualquier ciudadano que sospeche que ha sufrido una brecha de seguridad en sus sistemas o dispositivos puede solicitar la intervención del equipo de informática, formado por estudiantes en su mayor parte, para solventar la amenaza o la intrusión.

Fuente de información:
https://elpais.com