El 74 % de las empresas españolas reconoce su preocupación ante una posible ciberguerra

MADRID, ESPAñA, January 24, 2023 /EINPresswire.com/ -- Armis, la empresa líder en visibilidad y seguridad de activos, ha dado a conocer hoy los resultados preliminares de su informe Estado de la Ciberguerra, que pone de manifiesto la opinión de los profesionales de la seguridad y las IT a nivel mundial sobre la misma. El estudio está basado en las respuestas de más de 6.000 encuestados en 14 países (incluido España) de múltiples sectores, tales como la sanidad, las infraestructuras críticas, el retail, la cadena de suministro y la logística, entre otros.

La invasión rusa de Ucrania no sólo ha trastornado trágicamente las vidas de innumerables personas, sino que también está provocando ondas geopolíticas de ciberguerra que reverberarán en el futuro inmediato. En este contexto, los objetivos no son únicamente los gobiernos; cualquier organización es una víctima potencial, y tanto las empresas de infraestructuras críticas como las entidades de alto valor ocupan las primeras posiciones de la lista.

"La ciberguerra es el futuro del terrorismo, ya que ofrece un método de ataque asimétrico y rentable, cuya defensa requiere una vigilancia y una inversión constantes", afirma Nadir Izrael, director de tecnología y cofundador de Armis. "La ciberguerra clandestina se está convirtiendo rápidamente en algo del pasado. Ahora vemos ciberataques descarados por parte de los Estados nación, a menudo con la intención de reunir información, interrumpir las operaciones o directamente destruir datos. Basándose en estas tendencias, todas las organizaciones deberían considerarse posibles objetivos de ataques de ciberguerra y, en consecuencia, asegurar sus activos".

Vesku Turtia, director regional de Armis Iberia, explica: “Los actores del Estado nación siguen evolucionando en sus actividades y las infraestructuras críticas se están convirtiendo en su principal objetivo en un entorno de ciberguerra. La amenaza constante de hackeos dirigidos a las redes eléctricas, los sistemas de transporte o las instalaciones de agua son una importante vulnerabilidad de cara al futuro. En 2023, esperamos ver ataques de ransomware y malware más focalizados, así como una mayor convergencia TI/OT, lo que hace imprescindible contar con soluciones diseñadas para identificar, supervisar y proteger los activos digitales de la Industria 4.0, ahora y en el futuro”.

Algunas de las principales conclusiones del estudio Estado de la Ciberguerra de Armis para España son:

 Una de cada cuatro (26 %) organizaciones españolas no se toman en serio la amenaza de la ciberguerra, identificándose como indiferentes o despreocupadas por el impacto de la ciberguerra en su organización, lo que deja espacio para las brechas de seguridad. Esta cifra es aún mayor en países de nuestro entorno como Italia (56 %), Portugal (38 %), Alemania (40 %) o Francia (34 %)
 Más de una cuarta parte de las organizaciones españolas (26 %) se sienten poco preparadas para hacer frente a la ciberguerra. Pese a ello, el elemento de seguridad menos valorado entre los profesionales de TI, no solo de España sino del mundo, es la prevención ante los ataques de Estados nación (22 %). La protección de los datos (67 %) y la detección de intrusiones (58 %) se mantienen como las máximas prioridades en nuestro país.
 Más de dos tercios (67 %) de los profesionales de TI españoles encuestados están de acuerdo con la afirmación: "La guerra en Ucrania ha provocado una mayor amenaza de ciberguerra."
 Casi cuatro de cada diez (39 %) de aquellos profesionales españoles de TI que toman las decisiones sobre seguridad TIC reconocieron haber experimentado más actividad de amenazas en su red entre abril y octubre de 2022 en comparación con los seis meses anteriores, una cifra en línea con la media europea (40 %), pero algo menor si se compara con la media mundial (54 %).
De hecho, un número similar, el 34 % de los ejecutivos españoles con perfil de CTO, CIO y CISO encuestados experimentaron más actividad de amenazas durante el mismo periodo de tiempo, especialmente en el sector de las infraestructuras críticas (70 %), alimentación y bebidas (36 %), o fabricación e ingeniería (35 %).
 Más de la mitad (53 %) de los profesionales de TI españoles encuestados afirman que sus organizaciones han paralizado temporalmente o han abandonado proyectos de transformación digital debido a estas amenazas, siendo Australia (79 %) y EEUU (67 %) los países más afectados, y Japón (32 %) o Portugal (35 %) los que menos.
 El 58 % de los encuestados españoles están de acuerdo en que la amenaza de la ciberguerra puede suponer un freno a la digitalización, una cifra incluso superior a la media europea (51 %).

 El 83 % de los encuestados están de acuerdo en afirmar que existe una carencia de soberanía digital e inversión en la legislación española en referencia a la ciberseguridad. Aproximadamente la mitad (52 %) de los encuestados españoles señalan que confían en la capacidad del gobierno para defenderse en una ciberguerra, cifra algo inferior a la de Francia o Italia (66 % en ambos casos) y similar a la de Portugal.

Más información sobre el estudio aquí: www.armis.com/cyberwarfare

Metodología del estudio
Armis encuestó a 6.021 profesionales de TI en empresas con más de cien empleados en el Reino Unido, Estados Unidos, España, Portugal, Francia, Italia, Alemania, Austria, Suiza, Australia, Singapur, Japón, Países Bajos y Dinamarca. La encuesta se realizó entre el 22 de septiembre y el 5 de octubre de 2022 y describe el estado de la ciberguerra a nivel mundial en diversos sectores.

Sobre Armis
Armis es la empresa líder en seguridad y visibilidad de activos, proporciona la primera plataforma unificada de inteligencia de activos de la industria, diseñada para hacer frente al nuevo panorama de amenazas que crean los dispositivos conectados. Las empresas Fortune 100 confían en nuestra protección continua y en tiempo real para ver con contexto completo todos los activos gestionados y no gestionados en TI, la nube, dispositivos IoT, dispositivos médicos (IoMT), tecnología operativa (OT), sistemas de control industrial (ICS) y 5G . Armis proporciona gestión pasiva de activos cibernéticos, gestión de riesgos y cumplimiento automatizado. Armis es una empresa privada con sede en California. Visita www.armis.com.

por Armis
Grayling
armis@grayling.com
Visit us on social media:
Twitter
LinkedIn
