El 60% de las pymes europeas que son ciberatacadas tienen que cerrar al cabo de seis meses

El avance de la Inteligencia Artificial, la perfección de las técnicas, y la deficiencia en la prevención han provocado el incremento de ataques en pequeñas y grandes empresas

Roberto Gravili, ex coronel de la OTAN, o Rafael García, comandante del Mando Conjunto del Ciberespacio, analizarán en DES 2023 el nuevo orden mundial basado en las guerras híbridas y las ofensivas virtuales

Madrid, 02 de junio de 2023. – La eclosión de las tecnologías exponenciales, siendo de gran referencia la Inteligencia Artificial Generativa, ha traído consigo un sinfín de oportunidades para la competitividad de los negocios, pero también ha abierto la puerta a nuevas amenazas. Los ciberataques están registrando un aumento de casos a nivel global, con un total de 1.248 ataques por semana, lo que supone un incremento del 7% en comparación con el primer trimestre de 2022. En este sentido, y de acuerdo con el informe 'Panorama actual de la Ciberseguridad en España' de Google, las consecuencias de estos ciberataques pueden ser muy negativas para, por ejemplo, las pymes europeas, un 60% de las cuales desaparecen en los siguientes seis meses de recibir el ataque porque no pueden afrontar las pérdidas que esto representa.

Es por este motivo que el tejido empresarial actual, independientemente del tamaño de su actividad, tiene que estar preparando para hacer frente al desafío que implican los robos de datos o la manipulación de la información. Así, **DES – Digital Enterprise Show 2023**, el mayor evento europeo sobre transformación digital y tecnologías exponenciales que tendrá lugar del **13 al 15 de junio en Málaga**, dedicará una gran parte de su agenda a abordar las ciberamenazas surgidas en los últimos años, cómo prevenirlas, y qué hacer cuando el asalto ya ha sucedido.

He sido ciberatacado, ¿qué hago?

Los secuestros informáticos y de datos están afectando a miles de empresas, que han visto peligrar la protección de la información de usuarios, clientes y consumidores. Aunque el objetivo es evitar que la acción suceda, la realidad es que el 66% de las organizaciones a nivel mundial han sido atacadas mediante "ransomware", es decir robo de datos a cambio de una compensación económica, solo en el primer trimestre de 2023. Por ello, DES2023 desgranará, de la mano de **Jorge Fernández**, IT Sales Manager & CTO de VMWare, y **Agustín Gallego**, director de Administración Pública y Mercado Empresarial en Intel Corporation, cuáles son los pasos a seguir una vez se ha sido víctima de un ciberataque y cómo recuperarse.

Al respecto, una de las metodologías que se ha convertido en un modelo fundamental de ciberseguridad en red es la estrategia de "zero trust", la cual tiene por objetivo asegurar las conexiones mediante la comprobación de la identidad y la autorización individual. En este contexto, **Ralph Wanders**, SE Manager EMEA en la empresa de ciberseguridad, Colortokens, abordará por qué "zero trust" es la arquitectura que creará una mejor resistencia contra los ciberataques en constante evolución. A su vez, **Alberto**

Sempere, Global Director for Product & Innovation de Cybersecurity & Cloud en Telefónica Tech; **Pedro Galdón**, CIO & CISO de EMASA; **José de la Cruz**, analista internacional; y **Paul Toal**, OCI Security Specialist Senior Director en Oracle EMEA, ahondarán en cómo esta estrategia garantiza el nuevo paradigma del mundo hiperconectado.

Riesgos y desafíos en la nueva era digital

Los ataques a datos o a las redes informáticas cada vez presentan aspectos más diversos, de modo que la gestión de los ciberriesgos se ha dinamizado para adaptarse a los diferentes 'malware', es decir virus de software maliciosos, los episodios de phishing, o los 'deepfakes', que engañan con imágenes falsas creadas a partir de la Inteligencia Artificial. Con este contexto, **Miguel Ángel Cañada**, Head of Institutional Relations & Strategy en el Instituto Nacional de Ciberseguridad; **Fernando Fernández Lázaro**, Inspector Jefe de la Policía Nacional con una amplia experiencia en la ciberdelincuencia y más de 7 años trabajado para la Interpol; y **Enrique Rando**, consejero técnico de la Agencia Digital de Andalucía, analizarán el panorama de amenazas a corto plazo que presenta este 2023.

Un hecho significativo de la era actual es la interconectividad global, que induce a que las ofensivas híbridas estén sentando las bases de un nuevo orden mundial donde la geoestrategia marca la diferencia en el mundo tecnológico. **Roberto Gravili**, excoronel de la OTAN, y doctor en derechos humanos, demografía y justicia internacional, junto a expertos de la talla de **Federico Aznar**, comandante en el Ministerio de Defensa; **Ignacio García**, capitán retirado de la Marina; **Rafael García**, comandante del Mando Conjunto del Ciberespacio del Estado Mayor de la Defensa de España; o **Juan Díaz Nicolás**, Chair, Social Development and Director Centre for Research in Social Values de la Universidad de Camilo José Cela, reflexionarán sobre la compleja interacción entre la política global, la guerra y los avances tecnológicos.

Aunque los ciberataques están a la orden del día, el análisis de la industria muestra que la perspectiva defensiva aún tiene que madurar, mostrando que el 47 % de las alertas se ignoran. Por ello, es fundamental contar con un servicio de detección y respuesta rápida. En este marco, **Abel González**, director técnico de Cybersecurity Services & Solutions en Grupo SIA, compartirá la necesidad de obtener una protección, garantizar la identificación y asegurar una reacción ágil en el camino hacia la digitalización de las organizaciones.

El perfil del 'Chief Information Security Officer'

La cumbre internacional también ahondará en el perfil del CISO, Chief Information Security Officer, una figura esencial en la empresa para frenar las amenazas en la esfera virtual y velar por la protección de la organización. Responsables de seguridad de la información de compañías líderes como Iberia, Kyndryl, el Museo Thyssen o Codere, explicarán la manera que tratan los peligros cibernéticos, además de los riesgos y desafíos empresariales que suponen. Por su parte, **Javier Astiz**, Chief Technology Officer en Laboratorios CINFA, y **Álvaro Fraile**, Director, Cybersecurity Services en Ibermática, darán a conocer sus casos de éxito en cuanto a la ciberseguridad dentro de

la estrategia de negocio con una gestión más eficiente y la detección temprana de posibles ataques virtuales.