DIGITAL
ENTERPRISE
SHOW

60% of European SMEs that are cyber-attacked have to close after six months

The advance of Artificial Intelligence, the perfection of techniques, and the deficiency in prevention have led to an increase in attacks on small and large companies

Roberto Gravili, former NATO colonel, and Rafael García, commander of the Joint Cyberspace Command, will analyse the new world order based on hybrid warfare and virtual offensives at DES 2023

Madrid, 02 June 2023. – The emergence of exponential technologies, with Generative Artificial Intelligence being a major reference, has brought with it endless opportunities for business competitiveness, but it has also opened the door to new threats. Cyber-attacks are registering an increase in cases globally, with a total of 1,248 attacks per week, an increase of 7% compared to the first quarter of 2022. In this regard, and according to Google's 'Current Cybersecurity Landscape in Spain' report, the consequences of these cyberattacks can be very negative. For example, European SMEs, 60% of which disappear within six months of receiving the attack because they cannot afford the losses.

It is for this reason that the business fabric, regardless of the size of its activity, must be prepared to face the challenge posed by data theft or manipulation of information. Thus, DES – Digital Enterprise Show 2023, the largest European event on digital transformation and exponential technologies that will take place from **13 to 15 June in Malaga**, will devote a large part of its agenda to addressing the cyber threats that have emerged in recent years, how to prevent them, and what to do when the assault has already happened.

I have been cyberattacked, what should I do?

Computer and data hijacking is affecting thousands of companies, which have seen the protection of user, customer and consumer information put at risk. Although the aim is to prevent the action from happening, the reality is that 66% of organisations worldwide have been attacked by "ransomware", i.e. data theft in exchange for financial compensation, in the first quarter of 2023 alone. For this reason, DES2023 will be discussed by **Jorge Fernández**, IT Sales Manager & CTO of VMWare, and **Agustín Gallego**, Director of Public Administration and Enterprise Market at Intel Corporation, which are the steps to follow once you have been a victim of a cyber-attack and how to recover.

In this respect, one of the methodologies that has become a fundamental model of network cybersecurity is the "zero trust" strategy. This model aims to secure connections by verifying identity and individual authorisation. In this context, **Ralph Wanders**, SE Manager EMEA at the cybersecurity company Colortokens, will discuss why zero trust is the architecture that will create the best resilience against ever-evolving cyber-attacks. In turn, **Alberto Sempere**, Global Director for Product & Innovation of Cybersecurity & Cloud at Telefónica Tech; **Pedro Galdón**, CIO & CISO at EMASA; **José de la Cruz**, international analyst; and Paul Toal, OCI Security Specialist Senior Director at Oracle EMEA, will delve into how this strategy guarantees the new paradigm of the hyperconnected world.

Risks and challenges in the new digital era

Attacks on data or computer networks are becoming increasingly diverse. The management of cyber-risks has become more dynamic to adapt to the different 'malware', i.e. malicious software viruses. These are joined by episodes of phishing, or 'deepfakes', which deceive with false images created from Artificial Intelligence. In this context, **Miguel Ángel Cañada**, Head of Institutional Relations & Strategy at the National Institute of Cybersecurity; **Fernando Fernández Lázaro**, Chief Inspector of the National Police with extensive experience in cybercrime and more than 7 years working for Interpol; and **Enrique Rando**, technical advisor of the Digital Agency of Andalusia, will analyse the short-term threat landscape for 2023.

A significant fact of the current era is global interconnectivity, which means that hybrid offensives are laying the foundations for a new world order where geo-strategy makes the difference in the technological world. **Roberto Gravili**, former NATO colonel, and PhD in human rights, demography and international justice, together with experts of the stature of **Federico Aznar**, commander in the Ministry of Defence; **Ignacio García**, retired Navy captain; **Rafael García**, commander of the Joint Cyberspace Command of the Spanish Defence Staff; or **Juan Díaz Nicolás**, Chair, Social Development and Director Centre for Research in Social Values at the University of Camilo José Cela, will reflect on the complex interaction between global politics, war and technological advances.

Although cyber-attacks are the order of the day, industry analysis shows that the defensive perspective has yet to mature, with 47% of alerts being ignored. Therefore, a rapid detection and response service is essential. Within this framework, **Abel González**, technical director of Cybersecurity Services & Solutions at Grupo SIA, will share the need to obtain protection, guarantee identification and ensure an agile reaction on the road to the digitisation of organisations.

The profile of 'Chief Information Security Officer'

The international summit will also delve into the profile of the CISO, Chief Information Security Officer, an essential figure in the company to curb threats in the virtual sphere and ensure the protection of the organisation. Information security managers from leading companies such as Iberia, Kyndryl, the Thyssen Museum and Codere will explain how they deal with cyber dangers, as well as the business risks and challenges they pose. **Javier Astiz**, Chief Technology Officer at Laboratorios CINFA, and **Álvaro Fraile**, Director, Cybersecurity Services at Ibermática, will present their success stories in terms of cybersecurity within the business strategy with more efficient management and early detection of possible virtual attacks.