Cyber-security: the threats of the IoT, Cloud Computing or Artificial Intelligence to the modern world in DES2017

DES2017 is organising a cyber-security forum to debate the new threats that face the new digital and connected world. For employees and citizens, to companies and governments, the expert panels will cover the types of threats that face us now, those that are yet to come, as well as the technologies and practices that could protect us.

Madrid, 18 May 2017- In a hyper-connected market, it is essential to protect information and safeguard its confidentiality to avoid the serious damage that could be caused by improper access to sensitive information or to the different systems of organisations and institutions. For this reason, DES2017 (https://www.des-madrid.com) has organised a **'Cyber-security Forum'** for the morning of **24 May**, to analyse the new threats facing citizens and corporations that continually arise in the current digital landscape.

"Cyber-security has revealed itself to be a "battleground" for companies and governments. The digital transformation also affects the threats and crimes that current society faces, and the latest cyber-attacks, coordinated on a worldwide scale are a good example of this." comments Lluis Altes, DES2017's Strategy Director.

Cyber-security Forum

The R-evolution Theatre, located in pavilion 3 of IFEMA, will host the Cyber-security Forum on 24 May between 11:00 and 14:00.

The cyber-security forum will kick off with Guy Dagan, CAO - the Chief Awareness Officer of Bank Hapoalim - who will underline the importance of the human factor in the cyber-security strategy for public and private organizations in his talk entitled The Last Line Of Defence. Although companies are starting to make their employees aware of the importance of cyber-security and some of the threats that have appeared, there is still a lot to be done to educate and raise awareness of the issue. *"The saying that it is always the weakest link that breaks the chain is more relevant today than ever before; and the weakest link, in terms of cyber-security, is always the human factor. And it is usually due to a lack of awareness."* states Altés.

The forum will continue with the talk ***Cyber Strategies for Organizations*** chaired by Gianluca D'Antonio, GRUPO FCC, followed by the panel debate ***Connected Cars, IoT, Analytics... Are you ready for Digital Transformation?*** Raising the opportunities and risks associated with connected vehicles, IoT and analytics, Mihai Penica, Chief Technology Officer at BEIT SYSTEMS, Román Ramírez, Head of Security in Architecture for FERROVIAL and Marcos Gómez from INCIBE (the National Institute for Cyber-security), together with Daniel Largacha, Head of MAPFRE's Global Control Centre, will lead the debate. *"Data is fundamental to digital transformation, it feeds the system and allows companies that join the digital economy to grow and find new business opportunities. Therefore, its security is of vital importance,"* continues Lluis Altés.

Legislation is of particular relevance in ***EU Data Privacy challenges,*** a debate that will help the attendees to understand European legislation regarding data privacy. Companies are conscious

of the importance of respecting these policies; but, in the era of globalization, things are not so simple, and the risk of new legal challenges arising is ever present. The roundtable will be made up of Carlos Alberto Saiz, Director of the Data Privacy Institute (ISMS FORUM), Isabel González from MINSAIT, Michiel Kemperman from ZIMPERIUM, and Diego Fernández, Director of the Cyber-Security department of EVERIS.

Isaac Gutiérrez, Corporate Director of Cyber-security business at PROSEGUR, will lead the presentation on ***A new approach to Cyber-security is born***; while ***Cloud Security and Artificial Intelligence*** will be the closing conference at this forum dedicated to cyber-security.
Emmanuel Roeseler, IBM's Security Systems Leader for Spain, Israel, Greece & Portugal, will talk about what it means to keep safe while the interconnectivity between all kinds of devices grows.

Wannacry cyberattack statements

Ronen Almog, CO - CEO of Cyberess Ltd, based in Israel and operates globally providing unique cyber services and pro-active defence solutions from Israeli cyber companies.
"The chaos and disruption following the global "WannaCrypt" cyber-attack that hit tens of thousands of organizations in nearly 100 countries is a wake-up call for governments and businesses alike. The attack has shown us once again just how much our day-to-day lifestyle is digitally based and dependent on the continuous normal operation of computer systems, with an emphasis on critical systems such as healthcare systems and others. The ramifications of a large cyber-attack could easily include loss of life and, under certain circumstances, even a large-scale loss of life. Therefore, the nations of the world must now be even more proactive in protecting data on a national scale. Governments must act to create an environment in which attacks like these will be thwarted just as they begin. They must create state-sponsored cyber-defense organizations, as Israel has done, to update laws and regulations to effectively meet the challenges of today's digital reality and require regulators in various critical areas to act more proactively in fortifying cyber defenses and sealing security breaches quickly and effectively in organizations"

Limor Grossman, cyber expert and CEO of Q-Log, an Israeli cyber company that develops and distributes organization-wide systems for simulating and practicing against phishing attacks on a variety of platforms.
"One of the lessons from this cyber-attack, and from other attacks in recent years, is that data protection technologies are relatively effective in stopping attacks that exploit technological weaknesses. However, data protection methods have only limited effectiveness when the attacker exploits a vulnerability among the organization's employees. In the current attack, the first virus malware infected the organization apparently through a phishing attack that targeted human weaknesses. From that entry point, the other computers and systems in the organization and beyond were infected as the virus propagated itself across networks. We are witnessing a growing use of phishing as a preferred attack method, both in the quantity and in the sophistication and complexity of the attacks. The most effective line of defense against these types of cyber-attacks is in raising the cyber-awareness of managers and employees across the organization and by practicing through scheduled simulation attacks throughout the year. Following this method, the organization will know how to identify the tell-tale signatures of these types of attacks and the proper actions to take in avoiding them.
Governments must realize that there is no technological vaccination against attacks exploiting human weaknesses and legislate laws and regulations that require organizations – especially

those providing critical services – to better manage their staff's awareness of cyber threats, and to implement annual plans targeted at raising awareness to these threats.

Almog explains that "an attack on this scale is a turning point for data security that will lead to rethinking the way that organizations – both government and businesses – protect their data. There is no need to wait for the cyber equivalent of 9/11 to implement new processes; this weekend's event was traumatic enough to serve as a catalyst for change. Undoubtedly, cooperation among governments is required to stop hacking groups - whether common criminals, terrorists or other activists – by identifying them, preventing their access to computer resources, and chasing them down – in exactly the same way that governments act against organized crime or terror groups in the physical world.
Alongside these actions, the dialog between government and private sectors must be deepened to strengthen the protective walls around critical services and to protect our normal way of life. We must have greater collaboration and more effective regulations in these fields, not just because governments are able to impose their will on the organizational sectors but out of the common understanding that a cyber-war can only be won through the common interests of both sectors, the greatest of which are securing the safety of the public, the continuous operation of critical systems, and preserving the privacy of civilians and users.
The third side of the triangle is in cultivating the relationship between businesses and with suppliers of cyber products and services. Cyber companies provide the defensive tools as CDR & File sanitization, Attack Simulations platforms, 360 endpoints solutions, Cyber Intelligence etc attaining stronger and reinforced defenses requires a deeper and more expansive cooperation between all sides of the triangle – government, business sector, and suppliers. The results will be felt almost immediately in increasing Cyber awareness programs that effectively meet their goals.
In the DES conference that will take from May 23-25 in Spain, we will be exhibiting unique solutions to protect against attacks like this, all from Israeli cyber companies that is regarded world-wide as the leading cyber hub."

DES|Digital Business World Congress (taking place in Madrid, IFEMA, over the **23, 24 and 25 May**) is the world's largest international forum on digital transformation, which will bring together more than 18,000 professionals looking for technology partners. In addition, DES2017 will assemble public institutions and all the leaders of the international technology industry, more than 300 companies in total, which include Amazon, IBM, Intel, Deloitte and Accenture to guide companies towards digitalization.

Video DES2016: https://www.youtube.com/watch?v=95osOghtEWs

Press contact
Juliana Lorenzo
jlorenzo@tinkle.es / press@des-madrid.com
673 270 351