More than 90% of cyberattacks are made possible by human error

June 9 2022

Credit: Pixabay/CC0 Public Domain

In a ransomware attack, a company's computer systems are locked, and the attacker demands a ransom in cryptocurrency in return for unlocking the system. Malware infects a network of objects connected to the

Internet of Things to steal the personal data of its users. Talking about cybersecurity is talking about technology. However, it is increasingly common to study cyber risk as part of an interdisciplinary approach. After all, threats are technological, but they also have to do with behavioral, social and ethical factors.

Addressing cybersecurity from this point of view is precisely the objective of the European Interdisciplinary Cybersecurity Conference to be held on 15 and 16 June in Barcelona. The conference is being coordinated by two researchers from the Universitat Oberta de Catalunya (UOC): professor David Megías, director of the Internet Interdisciplinary Institute (IN3), and Helena Rifà, a researcher at the IN3 and director of the Master's Degree in Cybersecurity and Privacy, of the Faculty of Computer Science, Multimedia and Telecommunications.

The cybersecurity situation in 2022

The data are clear: cyberattacks have been on the rise in recent years and the cybersecurity situation is increasingly complex. According to the latest report from ENISA, the European Union Agency for Cybersecurity, attacks increased in 2020 and 2021, not only in terms of vectors and number but also in terms of their impact. And according to McAfee, ransomware-like attacks (attacks asking for a ransom in exchange for stopping or releasing the hijacked information) are the most common.

"Over the past two years, we haven't only had a health pandemic but there has been a genuine pandemic of cyberattacks and cybercrime," said David Megías, leader of the K-riptography and Information Security for Open Networks (KISON) research group. "Cybercriminals have taken advantage of the pandemic in many ways. In addition, with the increase in teleworking, cybercriminals have had easier access to computers that weren't as well protected as those of companies. And,

undoubtedly, the most common form of attack during these two years was ransomware, affecting institutions of all kinds: banks, energy suppliers, telecommunications companies, universities and public services."

The big cybersecurity challenges in 2022

"Cybersecurity is not just a technical discipline; it takes in many fields of knowledge and affects many different departments and practices in companies," said Helena Rifà, also a researcher in the KISON group. This being the case, the great challenges in the field of cybersecurity are not only technical but transcend the frontiers of technology. According to UOC experts, these are the main challenges.

1. Awareness-raising, the first line of defense

More than 90% of cyberattacks are made possible, to a greater or lesser extent, by human error, according to IBM data. Therefore, despite technological advances to minimize threats, the first major line of defense is the awareness and good practices of users. "Many of the cybersecurity issues companies face come about as a result of well-known vulnerabilities. If we all did our homework better, it'd be easier to reduce online threats. We all use electronic devices, and we all have to put in place a minimum of cybersecurity," explained Helena Rifà.

2. A new generation of hybrid threats

Cyber-physical systems are increasingly present in our daily lives, from industrial control systems and energy infrastructure to home automation. The technological revolution they are fostering, which has generated multiple business opportunities, carries its own threats, combining both complex technological and human aspects. The rise of hybrid cyber

threats will be the central theme of one of the two keynote presentations at the European Interdisciplinary Cybersecurity Conference, which will be given by Fulvio Valenza, an assistant professor at the Politecnico di Torino.

3. And more sophisticated defense tools

Faced with the increasing complexity of threats, artificial intelligence (AI) and machine learning are becoming increasingly important as protection tools. "The greatest scientific challenge today is trying to stay ahead of the increasingly sophisticated threats," added Rifà. "AI is increasingly being used both to quickly identify attacks and vulnerabilities and to resolve them."

4. Towards sustainable cybersecurity

We are all responsible for managing and protecting the resources in our environment for future generations. The basic definition of sustainability is also relevant in the field of cybersecurity. "In this sense, sustainability is understood as the mechanisms that allow the interactions of stakeholders (users, service providers and device manufacturers) with the technological ecosystem to be deliberate and with full knowledge of their consequences on the security and stability of the system," said David Megías.

The Internet of Things is generating an unprecedented increase in the number of devices sharing users' sensitive data and information. In addition, 5G and other telecommunications technologies allow broadband connectivity for an almost unlimited number of devices, multiplying the internet infrastructure. "As a result, technological infrastructure is becoming unsustainable due to various malicious threats and unintentional mistakes. It's imperative to achieve a more sustainable

ICT infrastructure by providing solutions that are secure and ensure privacy," Megías added.

5. The Great Privacy Battle

Cyberattacks are not the only way in which users' personal data can be compromised. On many occasions, data are exposed by the architecture of the platforms themselves or by the ignorance of netizens. For Helena Rifà, there are still many problems for technology to solve in order to better protect data, such as being able to send only the precise information for each purpose, better anonymization of databases and ensuring privacy for all the data stored on the web.

"At the social level, we also have to provide usability methodologies so that people know how to act on social media and the internet in general, what can be shared and what can't," she said. "In the end, the big challenge is to make data security and privacy compatible so that technology is usable, and we can work comfortably with it while protecting our systems and data."

Provided by Universitat Oberta de Catalunya

Citation: More than 90% of cyberattacks are made possible by human error (2022, June 9) retrieved 24 April 2024 from https://techxplore.com/news/2022-06-cyberattacks-human-error.html