By 2025, the worldwide cost of cyberattacks may triple compared to 2015

February 9 2023

Credit: Pixabay/CC0 Public Domain

In an increasingly digital world, secure internet infrastructures are both a challenge and an obligation. As the number of devices sharing data grows thanks to the rise and democratization of the Internet of Things

(IoT), the number of threats that users face is also on the increase. Estimates suggest that if the current rate of growth continues, the value of the damage caused by cyberattacks will amount to around $10.5 trillion a year by 2025, compared with $3 trillion in 2015, an increase of more than 200%.

The development of cybersecurity measures to mitigate and reduce these risks must be sustainable. Any commitment to sustainability must be aimed at making the internet environmentally responsible, ensuring equitable access, fostering digital inclusion and promoting social responsibility.

Those are the assumptions that led researchers at the Universitat Oberta de Catalunya (UOC) to coordinate the Bringing Sustainable Cybersecurity to the Internet of Things (SECURING) project, which also involves the Universitat Autònoma de Barcelona and the Universitat Rovira i Virgili.

The project seeks to contribute to sustainable development of the internet by providing cybersecurity and privacy technologies that efficiently protect the infrastructures of the Internet of Things. This will provide protection for a significant part of economies, while at the same time fostering sustainability from the social and environmental point of view.

The importance of a sustainable internet

It is becoming increasingly apparent that the concept of sustainability must not be limited to the economy and the environment, but instead needs to be included in all areas and sectors. These areas include the digital realm: the internet is an engine for the world, so if it turns out to be unsustainable, the same will also apply to the world.

There were more than 9.7 billion IoT-based devices on the planet in 2020, and estimates suggest that the number may triple by 2030. Sustainable methods are required to produce, maintain and protect these devices and the activities they carry out (thanks to cybersecurity).

"In the context of the IoT, sustainable cybersecurity means making sure that devices and systems are secure and private, while minimizing environmental impacts and making the most of opportunities for energy efficiency," explained Professor David Megías, director of the Internet Interdisciplinary Institute (IN3) at the UOC and coordinator of the SECURING project, together with Helena Rifà, researcher and member of the Faculty of Computer Science, Multimedia and Telecommunications.

A failure to promote sustainability would have consequences in various areas. "We can speculate on some of the potential consequences of failing to promote sustainable cybersecurity, such as service outages due to cyberattacks; the loss of privacy, information and trust by users, and an increase in congestion issues that could reduce the network's speed and efficiency," explained Megías, who heads the K-riptography and Information Security for Open Networks (KISON) research group.

Furthermore, if IoT devices are not designed to be energy-efficient and are not recycled properly, they can contribute to the internet's environmental impact and lead to both the emission of greenhouse gases that cause climate change, and an increase in waste.

SECURING: Combining sustainability and cybersecurity

According to the project's coordinators, preventing these problems requires a proactive approach to security, adequate regulations, and the

promotion of a culture of sustainable cybersecurity. This culture must be fostered among all stakeholders: from software developers to users.

The first step towards ensuring sustainability must be taken in the creation of IoT devices, which is the focus of the SECURING project. "Incorporating sustainable cybersecurity into ICT and IoT design is essential, because it ensures that devices are secure and private from the outset, and it protects users from potential cyberattacks and breaches of privacy," said the IN3 director.

"The environmental impact of technologies can also be reduced by using more efficient materials and production processes and creating devices that last longer and are easier to repair. In short, by considering sustainable cybersecurity as a factor in ICT and IoT design, safer, more sustainable and efficient solutions can be created, and these benefit both users and the environment," said the UOC professor.

The SECURING methodology and objectives

The objective of SECURING is to offer new technological solutions to security and privacy issues. The researchers are aiming to make a contribution with infrastructures focused on techniques for intrusion detection and prevention (IDP), designing new sustainable privacy protocols, and proposing a new communication paradigm for community-based crowdsensing.

Their methodology is based on the design and creation of software and hardware solutions and on subsequently carrying out formal tests. The project will be developed using technologies including machine learning, blockchain and digital watermarks, and privacy guarantee mechanisms will be implemented to ensure that end users' personal data are protected at all times.

The project is a multidisciplinary initiative which combines ICT with law. "One of the members of the research team is specialized in law, and specific research methods from that field will be used to apply regulations such as the General Data Protection Regulation (GDPR) to the technological solutions that are developed," explained Megías.

"Cyber risk is a complex issue involving many technical, legal, economic and social aspects. An interdisciplinary approach means we can address these aspects from an overall perspective, which makes it easier to obtain a more in-depth understanding of the problem and to develop more effective solutions that cannot be only technological, but must also have an important social aspect," concluded the project coordinator.

Provided by Universitat Oberta de Catalunya

Citation: By 2025, the worldwide cost of cyberattacks may triple compared to 2015 (2023, February 9) retrieved 6 May 2024 from https://techxplore.com/news/2023-02-worldwide-cyberattacks-triple.html