21st SECURE conference - security of the Internet by world experts

Many prominent IT security specialists, intense hours of presentation on ransomware, botnets, encryption, attacks on IT networks and industrial objects, debates and workshops on protection, state and enterprise policies, strategies, techniques and technologies. And a pinch of magic. It's all during the 21st SECURE 2017 Conference, held on October 24-25 in Warsaw.

SECURE 2017 has been given honorary patronage of Ministry of Digital Affairs, ENISA, Office of Electronic Communication, Polish House od Informatics and Telecommunication and The Kosciuszko Institute.

"The SECURE conference is organized by NASK for the twenty-first time. Year after year, it enjoys increasing interest and constant high level of content. Speakers, who share their knowledge, are experts with unique experiences. Their presence at the conference allows us to review the landscape of ICT threats we are currently dealing with and which we are forecasting for the coming months or years" - says Wojciech Kamieniecki Ph.D., Director of NASK National Research Institute.

Need for cooperation

One of the topics to be addressed during the conference is the growing need for cooperation between different institutions (including cross-border cooperation) - a result of the scale and complexity of new challenges. "Few people are able to successfully tackle the threat on their own. When it comes to companies, for example, designing and implementing an effective cyber security strategy with their own means can go beyond the capabilities of such an entity. Companies are increasingly using specialized security services provided by external partners. The second very important aspect is the exchange of information about security incidents. The sooner a threat is discovered, investigated and understood by experts, the greater the chance of protecting further individuals, companies and institutions from it" - says Przemek Jaroszewski, CERT Polska director of operations at the National Security Center at NASK PIB.

There is the growing awareness of Polish users, who increasingly report disturbing

events to CERT Polska, which enables the team to quickly analyze incidents and develop ways to counter their effects - such as data decryption tools for users attacked by ransomware.

Exchange of information and experience is also crucial for experts. According to European Commission in 2015 there were 8.2 billion cyberattacks. Such a mass of events forces the researchers to specialize and divide the "market". As a result, individual experts are tracking the perils only of some type. For this reason, the regular exchange of knowledge and experience is essential in order for everyone to have up-to-date knowledge of the whole phenomenon. "In fact, our community, despite its rivalry, is able to cooperate effectively in combating particular threats" - adds Przemek Jaroszewski.

Responsibility for cyber security

The legal challenges typically associated with cyber security are also complicated year by year. "During the SECURE 2017 conference, there are several lectures and debates on legislation and law enforcement. We are talking about regulations aimed at more effective protection against cyber threats, the evidential value of the work of the Police among cybercriminals and the liability for failures in security procedures that cause vulnerability" - explains Wojciech Kamieniecki, Ph.D. The last issue is particularly up-to-date because often another company produces a device, another software for it, another one is an operator and data administrator, and another one is a user. Accurate determination of responsibility for causing the threat is very difficult. Often the blame is partially shared by all, and the responsibilities of the parties are not yet clearly defined in the rules and practice of operation. Some experts postulate introducing regulations that impose greater security obligations on smart home appliances (IoT) manufacturers because they are, as they say, often too vulnerable. On the one hand, the threat is probably enhanced by the users, who are just starting to get more into the specifics of IoT devices. This makes many of them careless about security, for example, they do not change the factory defaults or allow the devices too broad data access. On the other hand, manufacturers also do not always prioritize security, trying to introduce novelty to the market as quickly as possible, or optimizing its performance (eg lowering energy consumption). Producer representatives declare their readiness to dialogue on multilateral responsibility in the IoT area. This issue will be addressed during SECURE 2017.

Real cyber weapon

Although the Internet is called a virtual reality, the effects of malicious software can be quite real, including material damage. "When we saw in 2010 the case of the Stuxnet

virus, which damaged the nuclear facility in Iran, we entered a new era. In a sense, science fiction has become a reality. Today such events are considered real risks, which must be taken into account when developing and operating industrial automation" - says Wojciech Kamieniecki Ph.D.

Therefore, when addressing cyber threats we must, according to experts of NC Cyber at NASK, pay attention to IIoT devices (Industrial Internet of Things), which allow remote monitoring or control of industrial automation components via the Internet. The situation is so important because of the fact that many industrial automation installations and devices were not designed to take into account today's threats or even need to be connected to the public Internet. This also applies to key industries such as energy, healthcare, utilities. Today, it became common practice to collect and control information remotely from computers connected to the public network. Such a combination of "two worlds", however, introduces completely new threats in industrial systems. For this reason, analysts point out that strategic sectors will be particularly vulnerable in the coming years.

Presentations, debates and workshops on these and many other cyber security topics with hundreds of experts from Poland and other countries are scheduled on the 24th and 25th of October in Warsaw (Hotel Airport Hotel Okęcie, 17 Stycznia Street).