http://eng.nask.pl/en/news/events/events-2017/745,NC-Cyber-14000-incidents-and-development-of-partnership-cooperation.html
2018-04-20, 01:04

NC Cyber – 14,000 incidents and development of partnership cooperation

More than 30 companies from key sectors, important for the Polish economy and efficient operation of the state, have signed the cooperation agreement with the National Cybersecurity Center (NC Cyber) that was set up a year ago. Within that period there were over 14,000 submissions reported to the NC Cyber, and more than 2,000 of them were classified as dangerous incidents on the network.

Thanks to information exchange and cooperation between the NC Cyber and key actors involved, we responded professionally to global threats, such as ransomware called WannaCry. Efficient operation and rapid reaction to threats also allow warning Polish and foreign institutions and users.

The National Cybersecurity Center was formally launched on July 4, 2016. It operates within the structure of the National Research Institute NASK that is supervised by the Ministry of Digital Affairs. It is a coordinating body that is responsible for analytical, prognostic and prevention activities in the area of civilian cybersecurity at the national level, especially in the key services (e.g. healthcare, transport, energy). Setting up such a unit is required by the EU Directive on the security of network and information systems (NIS Directive). The unit is also responsible for the international cooperation with its counterparts in other member states.

All provisions of the NIS Directive will come into force in one year, but we don’t want to delay the process. Building up a well-functioning network of cooperation in cybersecurity area, both for institutions and state and private enterprises, was really needed. The number of threats is growing and the attack on a key sector may have dramatic effects. The only way to avoid such a scenario is to cooperate, to use all available competence and sources of information. Polish companies understand it so they are willing to

cooperate with us - says Wojciech Kamieniecki Ph.D, NASK director.

Over 14,000 submissions and more than 2,000 incidents, illegal content

Since launching the NC Cyber until the end of June 2017, there were 14,297 submissions, including 2,178 dangerous incidents reported. The largest group – 892 cases concerned phishing, the attempt to obtain sensitive information. It also happens that cybercriminals try to find out logins passwords to social networking portals, paid services, such as games or video sites, as well as business accounts giving access to secured resources of an institution.

Malicious malware (446 incidents) is also the important issue. For example, it’s the ransomware described widely in media, but also spying programs. “This is the most advanced form of attack on a user. Cybercriminals are still developing malware, trying to exploit vulnerabilities and to overtake the actions of those developing protective mechanisms. This is why our work requires constant analysis of new types of malicious software. We are also the initiators or participants of many R&D projects aiming at developing the ways of detecting and reacting quickly to new attacks - explains Juliusz Brzostek, director of the NC Cyber and adds that exchanging information at national and international level is the efficient tool to fight against malware. It allows to collect information on new phenomenon.

CERT Polska team, operating at NASK since 1996, is a key part of the NC Cyber. It is the first Polish computer emergency response team. Since its launch, the core of the team's activity has been handling security incidents and cooperation with similar units worldwide. Facing global incidents, such as recent massive ransomware attacks, CERT Polska team has always undertaken professional actions analyzing threats and publishing complete and reliable warnings and guidance for those who have been

victims of cybercrime.

The Dyżurnet.pl team is a point of contact that has been functioning within the framework of NC Cyber. It was established in 2005. Sice then Dyżurnet.pl have analyzed 13,677 cases of harmful or illegal content published on the Internet. Internet users have reported to the team mainly sites, where, in their opinion, may include pornographic content involving a minor. There were 11,131 such submissions. The actual number of identified child abuse (CSAM) cases was 2,876. The majority of CSAM content was found on foreign servers and therefore Dyżurnet.pl forwarded reports do INHOPE network. Since the beginning of July 2016 till June 2017, 3,265 incidents were reported to INHOPE.

Cooperation with public institutions and partners from key sectors

In the first year of operation NC Cyber together with law enforcement agencies organized first two editions of exercises. The participants were the NC Cyber specialists and representatives of the Regional Prosecutor's Office in Warsaw and the Police Headquarters, specializing in combating computer crime. The exercises are the beginning of permanent cooperation between law enforcement agencies and the NC Cyber. NC Cyber experts will co-create (with police officers and prosecutors) a specialized team to provide ongoing advice and technical assistance in investigating the circumstances of cybercrimes. In order to conduct its mission successfully, NC Cyber is carrying out a special partnership program for key services operators. Currently, a dozen of entities is involved in the cooperation under 33 agreements and 19 bilateral agreements. It can be expected that by the end of the year there will be more than 70 such entities. The NC Cyber organizes regular meetings where experiences, analysis and best practices are exchanged. The NC Cyber Group for Development has also been formed to develop the principles and directions of the partnership.