http://eng.nask.pl/en/news/events/events-2017/905,NC-Cyber-we-are-recording-a-steady-increase-in-the-number-of-incidents-in-the-ne.html
2018-04-20, 00:55

NC Cyber: we are recording a steady increase in the number of incidents in the network

From January to October 2017, CERT Polska team, operating within the framework of NC Cyber NASK, handled 647 malware incidents.

There were 211 such incidents in 2016, and now alert messages prepared by NC Cyber are available in the Regional Early Warning System.

The total number of submissions to NC Cyber was below 9,000 this year. From January to the end of October 2017 CERT Polska team registered 221 break-in attempts to IT resources. This is twice as much as in 2016, when 109 incidents were handled. The increase in the number of incidents handled by CERT Polska does not directly mean an increase in the number of computer crimes. In our opinion the increase mainly results from the growing awareness of Internet users. More and more people are aware of the importance of reporting all alarming incidents to CERT Polska. This gives experts the opportunity to analyze new threats, and quickly assess how serious they are and thus warn other people and institutions before they fall victim to cybercriminals – comments Juliusz Brzostek, Head of NC Cyber at NASK.

As he adds, the more data about a particular threat will be obtained by the NC Cyber specialists, the greater chance that they will develops methods of counteracting cybercrime. This is how tools to unblock data on computers infected by ransomware

are developed. Ransomware is one of the most common malicious phenomenon in the network. To support victims of this type of crime, a global No More Ransom initiative has been launched, bringing together top-class cyber-security specialists from commercial companies, public institutions (governmental and non-governmental) and research centers. “CERT Polska is a member of No More Ransom project that provides decryption tools free of charge.” – reminds the head of NC Cyber.

However, the bottom-up initiatives, involving the cooperation in the narrow field, are not sufficient to have a fundamental impact on the cyber security landscape, globally as well as in individual countries. Therefore, countries and international organizations, including the European Union, are involved in supporting cooperation between different actors.

The Ministry of Digital Affairs is carrying out consultations on draft law concerning the national cyber-security system that is to align Polish law with the requirements of the European Parliament and Council Directive on the measures to ensure high level of network and information security within the Union. The Directive aims to develop cooperation in the field of cybersecurity at the Member State and Community level. The draft law on the national cybersecurity level stipulates that designated key companies and institutions will report cyber security incidents to a designated coordination center, which will be responsible for risk assessment and implementation of further actions and international cooperation.

According to draft law, the national cybersecurity system includes: key service providers and digital service providers, CSIRT (Computer Security Incident Response Team) at the Ministry of National Defence, CSIRT at NASK, CSIRT GOV, telecommunications entrepreneurs, public authorities and their support units, courts and tribunals, the National Bank of Poland, Bank Gospodarstwa Krajowego (Polish national development bank), the Government Security Centre, units subordinate to and supervised by government administration bodies, local government units, local government units, and local authorities, and their associations and associations, public universities, the Polish Academy of Sciences, entities providing cyber-security services and bodies competent for cyber-security matters.

The Ministry of Digital Affairs informs that ensuring a high level of cybersecurity is one of its priorities. New regulations are to guarantee among others undisturbed provision of key services (hospitals, drinking water supply, power engineering, banking) and

digital services by achieving a high level of security of the information systems used to provide them.