DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Press release: The Directorate took part in the cyber exercise Cyber Europe 2022, testing the resilience of the European healthcare sector

Bucharest, 9th of June 2022

The National Cyber Security Directorate (NCSD) took part in the cyber security exercise Cyber Europe 2022 between the 8th and 9th of June 2022, organised by the European Union Agency for Cyber Security (ENISA). The main objective of the 2022 edition was testing the responses to cyber attacks on the infrastructure and healthcare services in the EU.

To ensure citizens' trust in the medical services and infrastructure available to them, health services should function at all times. If health services and infrastructures in Europe were the object of a major cyber attack, how would we respond and coordinate at both national and EU level to mitigate the incidents and prevent an escalation? This is the question Cyber Europe 2022 sought to answer using a fictitious scenario.

The first day featured a disinformation campaign of manipulated laboratory results and a cyber attack targeting European hospital networks. On day two, the scenario escalated into an EU-wide cyber crisis with the imminent threat of personal medical data being released and another campaign designed to discredit an implantable medical device with a claim on vulnerability.

"Cyber Europe 2022 is a great opportunity to strengthen the cyber resilience of the healthcare sector at national and EU level, in exercise mode, by addressing the challenges of advanced cyber attack scenarios. For the Romanian National Cyber Security Directorate, working towards ensuring a high level of maturity and cyber resilience of the sector is one of our top priorities for this year", stated **Dan Cîmpean**, Director of NCSD.

The Executive Director of the EU Agency for Cybersecurity, **Juhan Lepassaar**, said: "The complexity of our challenges is now proportionate to the complexity of our connected world. This is why I strongly believe we need to gather all the intelligence we have in the EU to share our expertise and knowledge. Strengthening our cybersecurity resilience is the only way forward if we want to protect our health services and infrastructures and ultimately the health of all EU citizens."

The pan-European exercise organised by ENISA rallied a total of 29 countries from both the European Union and the European Free Trade Association (EFTA), as well as the EU agencies and institutions, ENISA, the European Commission CERT-EU, Europol and the European Medicine Agency (EMA). More than 800 cybersecurity experts were in action to monitor the availability and integrity of the systems over the two days of this latest edition of Cyber Europe.

Can we strengthen the cyber resilience of the EU healthcare?

The participants who engaged in the complex exercise were satisfied with the way the incidents were dealt with and the response to fictitious attacks.

Now, the analysis of the process and of the outcomes of the different aspects of the exercises need to be performed in order to get a realistic understanding of potential gaps or weaknesses which may require mitigation measures. Dealing with such attacks requires different levels of competences and processes which include efficient and coordinated information exchange, the sharing of knowledge around specific incidents and how to monitor a situation which is about to escalate in case of a generalised attack. The role of the EU level CSIRTs Network (the network of

CSIRT/ CERT structures) and the standard operation processes (SOPs) of the CyCLONe group also need to be looked into.

This thorough analysis will be published in the after-action report. The findings will serve as a basis for future guidance and further enhancements to reinforce the resilience of the healthcare sector against cyber attacks in the EU.

About Cyber Europe exercises

'Cyber Europe' exercises are simulations of large-scale cybersecurity incidents that escalate to EU-wide cyber crises. The exercises offer opportunities to analyse advanced cybersecurity incidents, and to deal with complex business continuity and crisis management situations.

Since its founding, NCSD (CERT-RO before September 2021) participated as national coordinator in all the editions of the pan-European exercise organised by ENISA (2012, 2014, 2016 and 2018). The event usually takes place every two years but the 2020 edition was cancelled due to the COVID-19 pandemic.

International cooperation between all participating organisations is inherent to the gameplay, with most European countries participating. It is a flexible learning experience: from a single analyst to an entire organisation, with opt-in and opt-out scenarios, and where the participants can customise the exercise to their needs.

Further information

Cyber Europe 2022

Cyber Exercises – ENISA topic

Cyber Europe 2018 – After Action Report

Contacts:

For questions related to the press and interviews, please contact:

NCSD media@dnsc.ro

ENISA press(at)enisa.europa.eu