Cyber Europe 2016: the pan-European exercise to protect EU Infrastructures against coordinated cyber-attack

Safeguarding Europe's Digital Market through cyber security

The European ICT Industry is one of the most advanced in the world. Making the EU's single market fit for the digital age could contribute €415 billion per year to our economy and create hundreds of thousands of new jobs[1]*. The pervasiveness of high-speed connectivity and the richness and quality of online services in the European Union are among the best globally. Such advantages have considerably increased the dependability of European citizens on ICT services. These two elements, quality of services and customer base, make this industry particularly appealing to global business. What if this important piece of the global economy becomes a target? Computer security attacks are increasingly used to perform industrial reconnaissance, lead disinformation campaigns, manipulate stock markets, leak sensitive information, tamper with customer data, sabotage critical infrastructures. In Cyber Europe 2016, Member State cybersecurity authorities and cybersecurity experts from the public and private sectors, are called to react to a series of unprecedented, coordinated cyber-attacks.* This is a summary of the Cyber Europe 2016 scenario.

Today marks the climax of this realistic scenario which thousands of experts from all 28 EU Member States, Switzerland and Norway are facing in Cyber Europe 2016 – a flagship activity organised every two years by ENISA, the EU Agency for Network and Information Security.

Cyber Europe 2016 (CE2016) is the largest and most comprehensive EU cyber-security exercise to date. This large-scale distributed technical and operational exercise started in April 2016, offering the opportunity for cybersecurity professionals across Europe to analyse complex, innovative and realistic cybersecurity incidents. On 13th and 14th of October ICT and IT security industry experts from more than 300 organisations, including but not limited to: national and governmental cybersecurity agencies, ministries, EU institutions as well as internet and cloud service providers and cybersecurity software and service providers will be called upon to mitigate the apex of this six-month long cyber crisis, to ensure business continuity and, ultimately, to safeguard the European Digital Single Market[2].Cyber Europe 2016 paints a very dark scenario, inspired by events such as the blackout in an European Country over Christmas period and the dependence on technologies manufactured outside the jurisdiction of the European Union. It also features the Internet of Things, drones, cloud computing, innovative exfiltration vectors, mobile malware, ransomware, etc. The exercise will focus on political and economic policies closely related to cybersecurity. This also takes into account new processes and cooperation mechanisms contained in the Network and Information Security (NIS) Directive. For the first time, a full scenario was developed with actors, media coverage, simulated companies and social media, bringing in the public affairs dimension associated with cyber crises, so as to increase realism to a level never seen before in cybersecurity exercises.

The Cyber Europe motto is **'stronger together'**. Cooperation at all levels is key to the successful mitigation of major, borderless cyber incidents.

[1] https://ec.europa.eu/priorities/digital-single-market_en

[2] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa2019s-role-in-the-european-digital-single-market-dsm

ENISA plays a key role in EU cyber preparedness

The NIS Directive[3] is a major step forward in the EU's abilities to deal with large cross border incidents that can lead to such crises. The CSIRT Network established by the Directive, along with work done so far for the EU Cyber Europe cycle, are key in providing decision makers with an overview of the situation and ultimately to respond to such complex threats.

"Günther H: Oettinger; European Commissioner for the Digital Economy and Society said: "In our connected societies, cyber-security concerns us all: we are only as strong as our weakest link. This is why our Directive on Network and Information Security promotes cooperation between EU Member States. With the help of our security agency ENISA, we are running "Cyber Europe" exercises. "Cyber Europe 2016" provides a unique opportunity for Member States, public and private partners to enhance cyber contingency plans and pan-European cooperation. ""

Udo Helmbrecht, Executive Director of ENISA, said: *"The role of ENISA in assisting the EU Member States for cyber crises is essential, both by organising exercises and by bringing together key stakeholders. Six years have passed since our first cyber crisis simulation and in that time the maturity level and response capability on complex cyber issues has increased. We are better prepared than we were, but that does not mean we have done enough and the work must continue. Cyber-attacks are more sophisticated than before. Cybersecurity is not a state, it is a process."*

ENISA, the European Commission and the Member States are investing in strengthening of an EU-wide cybersecurity crisis cooperation. The future of cyber crisis management in Europe - currently planned by the European Commission, concerns the drafting of a cyber crisis cooperation plan and the development of a cyber crisis management platform. ENISA's exercises provide a unique opportunity to test new developments, prepare for the future and develop further the sense of cooperation in the EU.

Next steps

The outcomes of Cyber Europe 2016 will be analysed by ENISA and the Member States. Detailed lessons learned will be shared with the participants to the exercise in order to establish a list of actions to improve cybersecurity in Europe. It is expected that many of the findings of the exercise are useful for the implementation of the NIS Directive and the work of the CSIRT Network, and the European cyber cooperation platform.

An after action report will be published with the main findings which will be made publically available early in 2017. Cyber Europe will follow up in 2018, while a number smaller scale exercises are planned in between.

Notes to editors:

Cyber Europe 2016 Exercise Q&A

Audio-visual material for Cyber Europe 2016:
Logo (ENISA Cyber Europe and Cyber Europe 2016)

[3] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

Cyber Europe 2016 video trailer and promo video
Cyber Europe 2016 poster 1 (A4, web)
Cyber Europe 2016 Exercise images

Cyber Europe website

Cyber Exercise Series
After Action report Cyber Europe 2014
Cyber crisis cooperation

For more information: Cyber Crisis Cooperation and Exercises Team, email: c3@enisa.europa.eu
For press and media interviews: please email press@enisa.europa.eu **Tel.** +30 2814 409 576