Cyber Europe 2018 – Get prepared for the next cyber crisis

EU Cybersecurity Agency ENISA organised an international cybersecurity exercise

Imagine this: It is a normal day at the airport. All of a sudden, the automated check-in machines display a system failure. Travel apps on smartphones stop functioning. The agents at the check-in counters cannot operate their computers. Travellers can neither check in their luggage, nor pass through security checks. There are huge lines everywhere. All flights are shown as cancelled on the airport monitors. For unknown reasons, baggage claim has stopped working and more than half of the flights must remain on the ground.

A radical group have reportedly taken control of the airport's critical systems by means of digital and hybrid attacks. They have already claimed responsibility for the incident and are using their propaganda channels to spread a call to action and attract more people to adopt their radical ideology.

This was the intense scenario which over 900 European cybersecurity specialists from 30 countries had to face on 6 and 7 June 2018, during the 'Cyber Europe 2018' (CE2018) – the most mature EU cybersecurity exercise to date.

The two-day exercise was orchestrated by ENISA at its headquarters in Athens, Greece, while the participants either stayed at their usual workplace or gathered in crisis cells. ENISA controlled the exercise via its Cyber Exercise Platform (CEP), which provided a 'virtual universe' (integrated environment) for the simulated world, including incident material, virtual news websites, social media channels, company websites and security blogs.

Organised by the EU cybersecurity agency ENISA in collaboration with cybersecurity authorities and agencies from all over Europe, the CE2018 was intended to enable the European cybersecurity community to further strengthen their capabilities in identifying and tackling large-scale threats as well as to provide a better understanding of cross-border incident contagion.

Most importantly, CE2018 focused on helping organisations to test their internal business continuity and crisis management plans including media crisis communication, while also reinforcing cooperation between public and private entities.

The scenario contained real life-inspired technical and non-technical incidents that required network and malware analysis, forensics, and steganography. The incidents in the scenario were designed to escalate into a crisis at all possible levels: organisational, local, national and European.

Mariya Gabriel, Commissioner for the Digital Economy and Society, said: "Technology offers countless opportunities in all sectors of our economy. But there are also risks for our businesses and our citizens. The European Commission and the Member States must work together and equip themselves with the necessary tools to detect cyber-attacks and protect the networks and systems. This is how ENISA's 'Cyber Europe' exercise was born eight years ago. It has grown into a major cybersecurity exercise and has become an EU flagship event which brings together hundreds of cybersecurity specialists from all over Europe. We should build on this success and I am confident that we can develop further the EU cooperation mechanisms, in particular to respond to large scale cyber incidents."

Prof. Dr. Udo Helmbrecht, Executive Director of ENISA, explained: “Over the last decade, the aviation sector has made a tremendous leap into the evolving age of technology. We can now enjoy the benefits of navigational apps, online check-in, and automated baggage screening. Smart technology saves time, money, and makes travellers’ lives easier. However, just as technology evolves, so do cyber threats. Through events such as the Cyber Europe 2018, our agency strengthens the level of cybersecurity within the EU. European countries and organisations working together as one entity is the modern response to borderless cyber threats. On behalf of ENISA and its staff, I would like to congratulate everyone involved in the Cyber Europe 2018.”

In the end, the participants were able to mitigate the incidents timely and effectively. This shows that the European cybersecurity sector has matured over the last few years and the actors are much more prepared. ENISA and the participants will shortly follow up on the exercise and analyse the actions taken to identify areas that could be improved. ENISA will publish a final report in due course.

Facts at a glance

- **Participating countries**: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom
- **Participating organisations**: approximately 300
- **Number of participants**: over 900 cybersecurity professionals
- **Number of injects**: 23 222

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. ENISA has already organised four pan-European cyber exercises in 2010, 2012, 2014 and 2016.

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, opt-in and opt-out scenarios, the participants can customise the exercise to their needs.