Biggest ever cyber security exercise in Europe today

@Enisa_EU #CyberSecurity #CyberEurope2014

More than 200 organisations and 400 cyber-security professionals from 29 European countries are testing their readiness to counter cyber-attacks in a day-long simulation, organised by the European Network and Information Security Agency (ENISA). In Cyber Europe 2014 experts from the public and private sectors including cyber security agencies, national Computer Emergency Response Teams, ministries, telecoms companies, energy companies, financial institutions and internet service providers are testing their procedures and capabilities against in a life-like, large-scale cyber-security scenario.

#CyberEurope2014 is the largest and most complex such exercise organised in Europe. More than 2000 separate cyber-incidents will be dealt with, including denial of service attacks to online services, intelligence and media reports on cyber-attack operations, website defacements (attacks that change a website's appearance), ex-filtration of sensitive information, attacks on critical infrastructure such as energy or telecoms networks and the testing of EU cooperation and escalation procedures. This is a distributed exercise, involving several exercise centres across Europe, which is coordinated by a central exercise control centre.

European Commission Vice-President @NeelieKroesEU said: "The sophistication and volume of cyber-attacks are increasing every day. They cannot be countered if individual states work alone or just a handful of them act together. I'm pleased that EU and EFTA Member States are working with the EU institutions with ENISA bringing them together. Only this kind of common effort will help keep today's economy and society protected."

The Executive Director of ENISA, Professor Udo Helmbrecht, commented: "Five years ago there were no procedures to drive cooperation during a cyber-crisis between EU Member States. Today we have the procedures in place collectively to mitigate a cyber-crisis on European level. The outcome of today's exercise will tell us where we stand and identify the next steps to take in order to keep improving."

The #CyberEurope2014 exercise will, among others, test procedures to share operational information on cyber-crisis in Europe; enhance national capabilities to tackle cyber crises; explore the effect of multiple and parallel information exchanges between private-public, private-private at national and international level. The exercise also tests out the EU-Standard Operational Procedures (EU-SOPs), a set of guidelines to share operational information on cyber crisis.

Background

According to ENISA's Threat Landscape report (2013), threat agents have increased the sophistication of their attacks and their tools. It has become clear that maturity in cyber activities is not a matter of a handful of countries. Rather, multiple countries have developed capabilities that can be used to infiltrate all kinds of targets, governmental and private in order to achieve their objectives.

In 2013, global web web-based attacks increased by almost a quarter and the total number of data breaches was 61% higher than 2012. Each of the eight top data breaches resulted in the loss of tens of millions of data records while 552 million identities were exposed. According to industry estimates cyber-crime and espionage accounted for between $300bn and $1tn in annual global losses in 2013.

The exercise

This exercise simulates large-scale crises related to critical information infrastructures. Experts from ENISA will issue a report with key findings after the exercise ends.

#CyberEurope2014 is a bi-annual, large scale cyber security exercise. It is organised every two years by ENISA, and this year counts 29 European countries (26 EU and 3 from EFTA) plus EU Institutions. It takes place in 3 phases throughout the year: technical, which involves the incident detection, investigation, mitigation and information exchanges (completed in April); operational/tactical, dealing with alerting, crisis assessment, cooperation, coordination, tactical analysis, advice and information exchanges at operational level (today) and early 2015; strategic, which examines decision making, political impact and public affairs. This exercise will not affect critical information infrastructures, systems, or services.

In the Cyber security Strategy for the EU and proposed Directive for a high common level of network and information security (NIS), the European Commission calls for the development of national contingency plans and regular exercises, testing large-scale networks' security incident response and disaster recovery. ENISA's new mandate also highlights the importance of cyber-security

preparedness exercises in enhancing trust and confidence in online services across Europe. The draft EU-SOPs have been tested over the last three years, including during CE2012.

Useful links

Cyber security in the Digital Agenda

ENISA's Cyber Crisis Exercises

ENISA's briefing pack on CE2014

Press Release CE2014 Technical Level Exercise: TLEx

Neelie Kroes - Follow Neelie on Twitter

Contacts

Email: comm-kroes@ec.europa.eu, c3e@enisa.europa.eu

Tel: +32.229.57361 Twitter: @RyanHeathEU, @enisa_eu