EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CYBER EUROPE 2020

The European Union Agency for Cybersecurity ENISA

23 | 12 | 2019

CYBER EUROPE 2020

CYBER EUROPE

- Simulation of cybersecurity incidents and cyber crises
- **Business continuity** and **crisis management** situations and scenarios
- Advanced **technical** real-life and advance incidents
- Scenarios inspired by real-life incidents
- Goals/objectives:
  - Procedure **testing**
  - Cooperation **enhancement**
  - Technical skills **training**
  - Gap **detection/analysis**

CYBER EUROPE enisa 2018
CYBER EUROPE 2016 CYBER EUROPE
CYBER EUROPE 2014 CYBER EUROPE
CYBER EUROPE 2012 CYBER EUROPE
CYBER EUROPE 2010 CYBER EUROPE
CYBER EUROPE enisa 2020

CYBER EUROPE 2020

Goals:

- G1. Test EU-level technical and operational cooperation during cyber-crises
- G2. Provide opportunities to test local-level incident response and procedures
- G3. Train EU- and local-level technical capabilities

Implicit goals:

- Help to build trust
- Engage the private sector
- Improve situational awareness
- Test public affairs response
- Improve exercise process and capabilities

CYBER EUROPE 2020

Setup:

- It is a **two-day** distributed exercise in June 2020
- Exercise is planned with the direct **contributions of National Planners**
- Also provide national monitoring and support players at local level
- Technical, procedural and media response to a variety of incidents
- The **players** are remote, usually at normal place of employment or in incident cells
- There will be a **central Exercise Control at ENISA HQ** in Athens

CYBER EUROPE 2020

Target audience:

- **Cyber security authorities**
  - National/Governmental CSIRTs / Cyber Security Authorities
- **Providers of essential services (health)**
  - Ministries of Health
  - Healthcare Organisations (e.g. hospitals/clinics/labs)
  - eHealth Service Providers
  - Health industry/insurance (medical device manufacturers, pharmaceutical companies, etc.)
- **EU institutions/bodies**
  - ENISA, Europol, CERT-EU, E.P., Council,..

CYBER EUROPE 2020

Example incidents:

- Spearphishing attacks,
- Wide-spread of malware,
- Mobile malware as information stealers,
- Rogue WIFI in hospitals,
- Insider attacks,
- Data breaches,
- Vulnerable medical devices,
- PACS/CIS attacks
- DICOM vulnerabilities exploitation
- and many others…

CYBER EUROPE 2020

How do I get involved?

Contact ENISA or the local planners within your country

How do I get more info? exercises@enisa.europa.eu

THANK YOU FOR YOUR ATTENTION

Exercises Team

The European Agency for Cybersecurity (ENISA)

☎ +30 6948 460 148 ✉ exercises@enisa.europa.eu