SUPPORTING EU INCIDENT RESPONSE CAPABILITIES

Rossella Mattioli
CSIRT Relations Team
Expert in Network and Information Security
& proud TALTECH alumni

21 | 01 | 2019
ENISA MISSION:
SECURING EUROPE’S INFORMATION SOCIETY

https://www.enisa.europa.eu/
EU CYBERSECURITY ACT

TODAY POLICY FRAMEWORK

- EU Cybersecurity Strategy
- Digital Single Market Strategy
- Strengthening Europe’s Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry

Network and Information Security Directive
eIDAS Regulation
Payment Services Directive 2
General Data Protection Regulation
Proposal for a Regulation on Privacy and Electronic Communications
POSITIONING ENISA’S ACTIVITIES

1. RECOMMENDATIONS ON CYBER SECURITY AND INDEPENDENT ADVICE

2. SUPPORT MS & EC IN POLICY IMPLEMENTATION AND HARMONISATION ACROSS EU

3. ‘HANDS-ON’ WORK, COLLABORATING WITH OPERATIONAL TEAMS THROUGHOUT EUROPE
# EXPERTISE

<table>
<thead>
<tr>
<th>Cloud and Big Data</th>
<th>Critical Infrastructures and Services</th>
<th>CSIRT Services</th>
<th>CSIRTs and communities</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSIRTs in Europe</td>
<td>Cyber Crisis Management</td>
<td>Cyber Exercises</td>
<td>Cyber Security Education</td>
</tr>
<tr>
<td>Data Protection</td>
<td>Incident Reporting</td>
<td>IoT and Smart Infrastructures</td>
<td>National Cyber Security Strategies</td>
</tr>
<tr>
<td>Standards and certification</td>
<td>Threat and Risk Management</td>
<td>Trainings for Cyber Security Specialists</td>
<td>Trust Services</td>
</tr>
</tbody>
</table>

[https://www.enisa.europa.eu/topics](https://www.enisa.europa.eu/topics)
COMMUNITY

http://www.csirtsnetwork.eu/

https://www.enisa.europa.eu/trainings

https://cybersecuritymonth.eu/

https://www.enisa.europa.eu/topics/cyber-exercises/

https://www.europeancybersecuritychallenge.eu/
CSIRTS SITUATION IN EUROPE TODAY

- 383 ENISA Inventory listed teams:
  - teams in CSIRTs Network: 37
  - Trusted Introducer listed: 173 out of 174
  - Trusted Introducer accredited: 152 out of 158
  - Trusted Introducer certified: 25 out of 25
    - 7 out of 25 are CSIRTs Network members
  - FIRST members: 175 out of 450

http://enisa.europa.eu/csirts-map
73 studies so far:

- CSIRT Setting up Guide in 21 languages
- Incident Management
- Baseline Capabilities of National/Governmental teams
- Maturity assessment framework
- Information sharing - Threat Data - Actionable information
- Proactive detection of network security incidents – monitoring - honeypots
- Computer Emergency Response Capabilities for ICS/SCADA
- Cooperation between CERTs and Law Enforcement Agencies - Electronic evidence - interaction with the Judiciary
- Vulnerability Disclosure

https://www.enisa.europa.eu/publications#c8=CSIRTs
2019 ECONOMICS OF VULNERABILITY DISCLOSURE

Economic incentives, motivations and barriers in a coordinated vulnerability disclosure process

Source: ENISA study on the economics of vulnerability disclosure

Conclusions

• The speed at which major vendors develop and roll out appropriate remediation measures can have direct effects on limiting the impact and costs of attacks.

• The inability or lack of incentives for users to monitor security developments and apply appropriate security updates or patches – even when faced with significant threats

• Stockpiling vulnerabilities can backfire (equities problem).

• More coordinated vulnerability disclosures is needed.

Conclusions:
• CSIRTs interact much more with LE than with the prosecutors and they interact very rarely with the judiciary
• There are legal provisions on CSIRTs and LE cooperation and their interaction with the judiciary
• The understanding of whether CSIRTs have to report to/inform LE and/or prosecutor of suspicious criminal activities could be improved. Depending on the Member State, the CSIRTs may be obliged or not
• There is need for a more extensive usage of information from CSIRTs in criminal investigations

https://www.enisa.europa.eu/publications/csirts-le-cooperation
2019 “COOPERATION BETWEEN CSIRT AND LAW ENFORCEMENT: INTERACTION WITH THE JUDICIARY”:

Recommendations:

• ENISA, Europol EC3, Eurojust and CEPOL: to facilitate joint training across the three communities on aspects of their cooperation among the EU and EFTA
• National/governmental CSIRTs, LE and possibly prosecutor services: to work together towards a better mutual understanding of the strengths, needs and limitations of the 3 communities
• National/governmental CSIRTs, LE and possibly prosecutor services: to appoint liaison officers to facilitate the cooperation and the interaction.
• National/governmental CSIRTs, LE and possibly prosecutor services: to investigate how the tools they use can be further improved to better receive the information provided by other communities and to better formulate their request for information addressed to the other communities.

https://www.enisa.europa.eu/publications/csirts-le-cooperation
Established by the NIS Directive "in order to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation".

Representatives of the Member States’ CSIRTs and CERT-EU can

• cooperate
• exchange information
• build trust
• improve the handling of cross-border incidents
• discuss how to respond in a coordinated manner to specific incidents.

http://www.csirtsnetwork.eu/
### members

| Austria | Belgium | Bulgaria | CY | Czech Republic | Germany | France | Finland | Italy | Lithuania | Luxembourg | Malta | Netherlands | Poland | Portugal | Romania | Sweden | Switzerland | Turkey | UK |
|---------|---------|----------|----|----------------|---------|--------|---------|-------|-----------|------------|-------|-------------|--------|----------|----------|--------|-------------|--------|----|-------|
| CERT.at | GovCERT Austria | AEC | CERT.be | CERT Bulgaria | CSIRT-CY | CSIRT.CZ | GOVCERT.CZ | CERT-Bund | CFCS | CERT-EE | CCN-CERT | CERTSI | CERT-EU | NCSC-FI | CERT-FR | NCSC (UK) | NCERT-GR | CERT ZSIS | CERT.hr | GovCERT-Hungary | CSIRT-IE | IT-CERT | CERT-LT | CIRCL | CERT.LV | CSIRT Malta | NCSC-NL | CERT.POLSKA | CERT PT | CERT-RO | CERT-SE | SI-CERT | CSIRT.SK | SK-CERT | NCERT.LU | GOVCERT.LU |
ENISA provides the secretariat and actively supports the cooperation among members:

- organizes meetings of the CSIRTs Network
- provides infrastructure
- provides its expertise and advice both to the EC and MS

http://www.csirtsnetwork.eu/
ENISA TRAININGS SINCE 2008

- Online training material – with over 40 trainings made available online, free to use by the community
- Training Courses on site
- Train the trainer programme – to scale trainings in the different MS

https://www.enisa.europa.eu/trainings
ENISA TRAININGS PORTFOLIO

Mobile threats incident handling
Digital forensics
Large scale incident handling
Network forensics

Triage & basic incident handling
Vulnerability handling
Artifact analysis fundamentals
Advanced artifact handling

Writing security advisories
Developing countermeasures
Identification and handling of electronic evidence
Automation in incident handling

https://www.enisa.europa.eu/trainings
### Technical
- Building artefact handling and analysis environment
- Processing and storing artifacts
- Artefact analysis fundamentals
- Advanced artefact handling
- Introduction to advanced artefact analysis
- Dynamic analysis of artefacts
- Static analysis of artefacts
- Forensic analysis: Local Incident Response New
- Forensic analysis: Network Incident Response New
- Forensic analysis: Webserver Analysis New
- Developing Countermeasures
- Common framework for artefact analysis activities
- Using indicators to enhance defence capabilities
- Identification and handling of electronic evidence
- Digital forensics
- Mobile threats incident handling
- Mobile threats incident handling (Part II)
- Proactive incident detection
- Automation in incident handling
- Network forensics
- Honeypots
- Vulnerability handling
- Presenting, correlating and filtering various feeds

### Operational
- Incident handling during an attack on Critical Information Infrastructure
- Advanced Persistent Threat incident handling
- Social networks used as an attack vector for targeted attacks
- Writing Security Advisories
- Cost of ICT incident
- Incident handling in live role playing
- Incident handling in the cloud
- Large scale incident handling

### Legal and Cooperation
- Establishing external contacts
- Cooperation with law enforcement
- Assessing and Testing Communication Channels with CERTs and all their stakeholders
- Identifying and handling cyber-crime traces
- Incident handling and cooperation during phishing campaign
- Cooperation in the Area of Cybercrime
- CERT participation in incident handling related to the Article 13a obligations
- CERT participation in incident handling related to the Article 4 obligations

ENISA training on aviation cybersecurity co-organized with EASA

ATTACK SCENARIO: SCADA SYSTEM COMPROMISE

Information gathering → Target → Social engineering → Logon abuse → Exploit vulnerabilities

Block the process → Power supply disruption → SCADA compromise and tampering → Compromising network → Backdoor
ENISA training on finance cybersecurity co-located with the EU Financial Information Sharing and Analysis Centre FI-ISAC in Athens, Greece in November 2018.
Introduction to Network Forensics:

- Exercise # 1: ICS/SCADA environment
- Exercise # 2: Detecting exfiltration on a large finance corporation environment
- Exercise #3: Analysis of an airport third-party VPN connection compromise

https://www.enisa.europa.eu/trainings
CSIRT CAPABILITIES DEVELOPMENT AND MATURITY ASSESSMENT METHODOLOGY
CSIRT CAPABILITIES DEVELOPMENT
BASELINING, EVALUATION, IMPROVEMENT

ENISA drives this effort continuously since 2009

In 2016 ‘How to assess maturity’
3 tier model introduced (basic, intermediate, ‘certifiable’)

In 2017 ENISA released Maturity Self-assessment Survey
Teams can assess their team’s maturity instantly

44 questions based on SIM3 model define results

ENISA suggests an additional peer review methodology for
CSIRTs Network practice

https://www.enisa.europa.eu/topics/csirts-in-europe
CSIRTS MATURITY ASSESSMENT METHODOLOGY

ENISA online assessment tool:
1. Basic (red)
2. Intermediate (yellow)
3. ‘Certifiable’ (green)

Online self assessment tool for incident response teams with 44 parameters covering:

- **O** - Organization
- **H** - Human
- **T** - Tools
- **P** - Processes

REFERENCE INCIDENT TAXONOMY WORKING GROUP – RSIT WG

- ENISA introduced this idea in 2017 to the TF-CSIRT
- 52 participants from 17 MS
- Approved as official TF-CSIRT working group by the TF-CSIRT Steering Committee on 26 September 2018.

Next meeting in
Wednesday
23rd January
2018 from 15:00
to 17:00 in the
Conference
Hall.
Join us!

---

**REFERENCE TAXONOMY INCIDENT Taxonomy (human readable version)**

This is the Reference Security Incident Classification Taxonomy. See the machine readable version as well. It should have an identical contents to the human readable version. Note that the 1st column is mandatory, the 2nd column is an optional but desired field.

Version: 1 Generated from machine readable version. Please do not edit this file directly in github, rather use the machinev1 file.

<table>
<thead>
<tr>
<th>CLASSIFICATION (1ST COLUMN)</th>
<th>INCIDENT EXAMPLES (2ND COLUMN)</th>
<th>Description / Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abusive Content</td>
<td>Spam</td>
<td>Or 'Unsolicited Bulk Email', this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content.</td>
</tr>
<tr>
<td>Abusive Content</td>
<td>Harmful Speech</td>
<td>Discreditation or discrimination of somebody, e.g. cyber stalking, racism or threats against one or more individuals.</td>
</tr>
<tr>
<td>Abusive Content</td>
<td>Child Porn/Sexual/Violent Content</td>
<td>Child pornography, glorification of violence, etc.</td>
</tr>
<tr>
<td>Malicious Code</td>
<td>Infected System</td>
<td>System infected with malware, e.g. PC, smartphone or server infected with a rootkit.</td>
</tr>
<tr>
<td>Malicious Code</td>
<td>C2 Server</td>
<td>Command-and-control server contacted by malware on infected systems.</td>
</tr>
<tr>
<td>Malicious Code</td>
<td>Malware Distribution</td>
<td>URI used for malware distribution, e.g. a download URL included in fake invoice malware spam.</td>
</tr>
<tr>
<td>Malicious Code</td>
<td>Malware Configuration</td>
<td>URI hosting a malware configuration file, e.g. webinjects for a banking trojan.</td>
</tr>
</tbody>
</table>

---

ENISA CSIRT Relations Team

- CSIRTs Community projects and services
- Onsite
- Sectorial
- Train the trainers
- VMs, tutorials
- CSIRTs in Europe
- CSIRTs map
- Reference Security Incident Taxonomy WG
- Active support and Secretariat
- CSIRTs self Assessment tool
- Leading tool development and maturity assessment

CSIRTs Network
Powered by ENISA
WHAT WE DO

Foster expertise with reports, trainings and community projects

Provide the secretariat of the CSIRTs Network

Actively support the cooperation among CSIRTs Network members

Facilitate incident exchange and collaboration

Help incident response teams to grow and advance

Support incident response capabilities to protect European citizens
THANK YOU FOR YOUR ATTENTION

AITAH TALTECH & CERT-EE

+30 28 14 40 9711
CSIRT-Relations@enisa.europa.eu
www.enisa.europa.eu