THE EU CYBERSECURITY AGENCY

CSIRTS IN EUROPE AND CURRENT TRENDS

Andrea DUFKOVA
CSIRT Relations Team Leader
Core Operations Department
ENISA

THE EU CYBERSECURITY AGENCY

Securing Europe’s Information society

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

STUDY ON CSIRT LANDSCAPE AND IR CAPABILITIES IN EUROPE 2025

KEY FINDINGS

https://www.enisa.europa.eu/publications/study-on-csirt-landscape-and-ir-capabilities-in-europe-2025

FINDING A FO NOITPODA EHT SRETSOF EVITCERID SIN EHT FO NOITATNEMELPMI EHT -1 LANOITAN FO TNEMNGILA DRAWPU NA DNA RI SDRAWOT HCAORPPA CITSILOH SEITILIBAPAC

Identified trends

- All European countries have cybersecurity legislation and regulations in place
- There is an harmonisation of strategic and policy objectives, structures and practices in the fields of IR and CSIRT, reflected in the new cybersecurity strategies and the national transposition measures of the NIS Directive
- National cybersecurity agencies increasingly integrate the national/governmental CSIRT and act as focal points for international cooperation in IR

Analysis

- These recent policy and regulatory orientations do not however indicate if this harmonisation of legislations will lead to an actual harmonisation and upgrade of the national IR capacities .
- With much of the detailed application of the NIS Directive left to the national implementing laws of Member States, there remains a risk of fragmentation in terms of capabilities

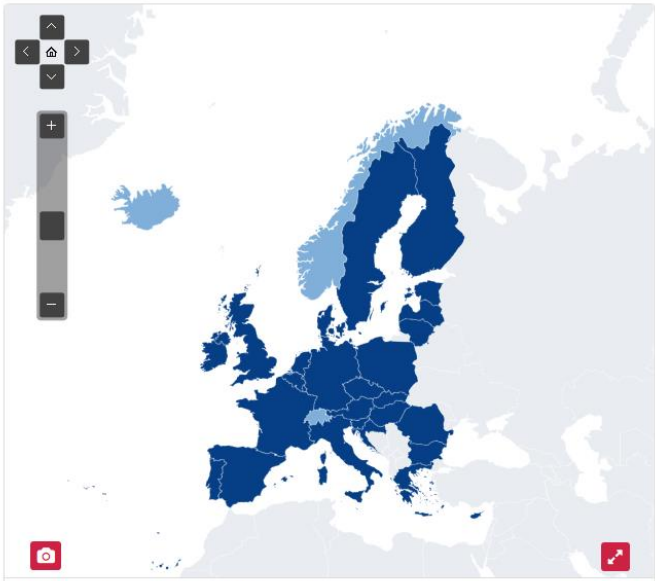
CSIRTS SITUATION IN EUROPE TODAY

- **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 25*
    - 7 out of 25 are CSIRTs Network members
  - FIRST members: 175 out of 450

http://enisa.europa.eu/csirts-map

* 16 certified and 9 Re-Certification Candidate

National Cyber Security Strategies



Select a country on the map to view details.

Country
Czech Republic

Strategy status
Complete

Implementation date
16/02/2015

Download in English
PDF document, 1.72 MB

Download in Czech
PDF document, 609 KB

Objectives

- Balance security with privacy
- Citizen's awareness
- Critical Information Infrastructure Protection
- Engage in international cooperation
- Establish a public-private partnership
- Establish an incident response capability

  Government CERT (GovCERT.CZ) continues to expand its capacity, reflecting the ever increasing demands on its analytical capabilities in investigating cyber security incidents. NCISA and its national partners also supports a creation of new CERT / CSIRT teams in the Czech Republic via informing public and private entities (especially those that are obliged by the Act on Cyber security) about CERT and CSIRT teams' advantages.
- Establish an institutionalised form of cooperation between public agencies
- Foster R&D
- Organise cyber security exercises

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

FINDING 2- IN THE CYBERSECURITY FIELD, THE EU LEVEL INTERACTS WITH THE REGIONS AND THE WORLD AS A 'STANDARD SETTER'

Identified trends

- Emerging harmonization of domestic legal frameworks with the EU legal framework in the field of cybersecurity in Europe's neighbouring regions (e.g. Balkans) and to a lesser extent internationally
- Some candidate countries for EU membership have increased their cybersecurity legislation in recent years with specific references to the NIS Directive and relevant EU regulations.
- NIS Directive and other regulations in this field impact global companies having activities within the EU

Analysis

- The NIS Directive demonstrates the ability of the EU to create political and normative consensus between nations on (cyber)security-related issues
- With the NIS but also the GDPR, the EU acts as a legal standard setter on issues pertaining to cybersecurity, with third countries showing a growing interest in EU-lead initiatives (e.g. the USA)

DIRECTIVE (EU) 2016/1148 (NISD)

Scope: to achieve a high common level of security of NIS within the Union (first EU regulatory act at this level).

Provisions:

- Obligations for all MS to adopt a national NIS strategies and designate national authorities.
- Creates first EU cooperation group on NIS, from all MS.
- Creates a EU CSIRTs Network.

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

- Establishes security and notification requirements for operators of essential services (OES) and digital service providers (DSP).

enisa

RITY AGENCY

Strategic
NIS Cooperation Group

NCSS

cloud computing services

Online market places

Search engines

DSPs

OES

s

transport

energy

banking

Incident Reporting

Security requirements

CSIRTs NETWORK

Tactical /Operational
CSIRTs Network

https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

List of SPOCS – NIS Directive

Austria
Details tbd.

Belgium
Centre for Cybersecurity Belgium
Addresss: Rue de la Loi, 18 - 1000 Brussels
Email: info@ccb.belgium.be
Phone: +32 479 365 694

Bulgaria
State "E-gov" Agency
Address: "Gen. Yosif V. Gurko" Street 6, 1000 Sofia, Bulgaria
Email: mail@e-gov.bg
Phone: +359 (2) 949 20 40
Contact Hours: Monday-Friday 09:00-17:30 UTC+2

Croatia
The Office of the National Security Council
Address: Jurjevska 34, Zagreb
Phone: +385 14681 206, +385 1 4681 206, +385 1 4681 254, +385 4681 269
Contact Hours: Monday-Friday 08:30-16:30

Cyprus

CSIRTS NETWORK

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

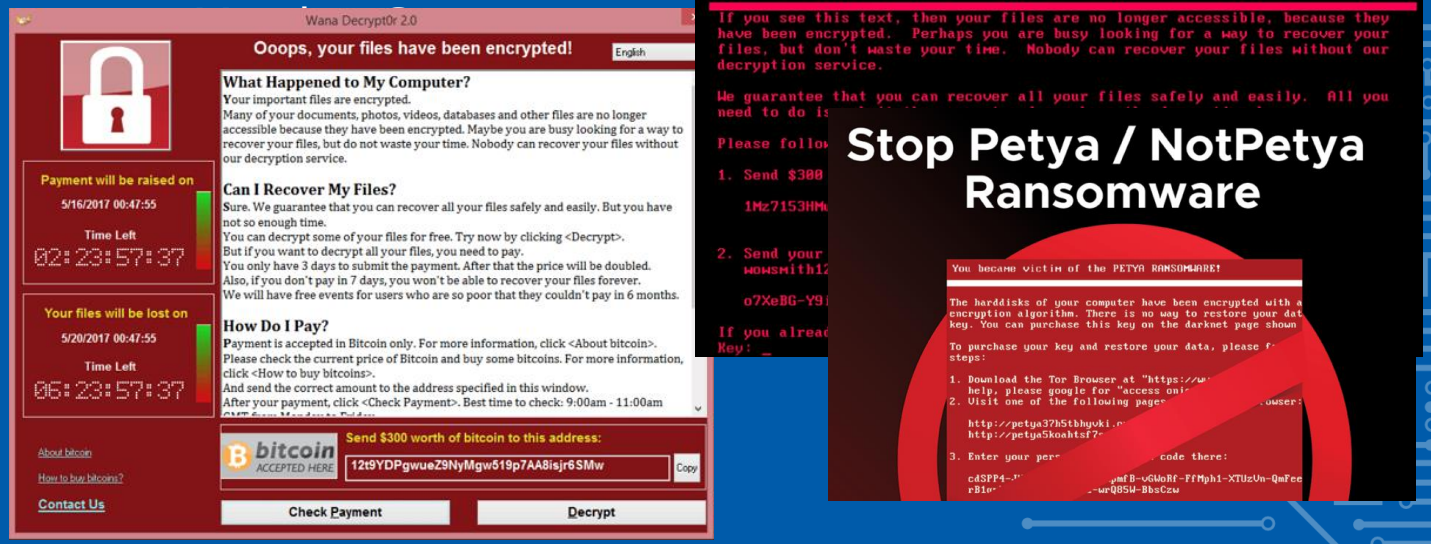
- cooperate
- exchange information
- build trust
- improve the handling of cross-border incidents
- discuss how to respond in a coordinated manner to specific incidents.

http://www.csirtsnetwork.eu/

THE EU CYBERSECURITY AGENCY

CSIRTs Network

- **Why?** to enable cooperation (IEx) on incidents, vulnerabilities, threats and risks among **all EU MS**
  - in order to developing c



CSIRTs NETWORK members

Powered by ENISA

CERT.at	CERT-EU	CSIRT Malta
GovCERT Austria	NCSC-FI	NCSC-NL
AEC	CERT-FR	CERT POLSKA
CERT.be	NCSC (UK)	CERT.PT
CERT Bulgaria	Hellenic MCIRC	CERT-RO
CSIRT-CY	CERT ZSIS	CERT-SE
CSIRT.CZ	CERT.hr	SI-CERT
GOVCERT.CZ	GovCERT-Hungary	CSIRT.SK
CERT-Bund	CSIRT-IE	SK-CERT
CFCS	IT-CERT	NCERT.LU
CERT-EE	CERT-LT	GOVCERT.LU
CCN-CERT	CIRCL	
CERTSI	CERT.LV	

https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#network-status=Member

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/

FINDING 3- RECENTLY CREATED CSIRTS AND ENHANCEMENTS OF CAPABILITIES AND COLLABORATION AT NATIONAL AND EUROPEAN LEVEL

Identified trends and facts

- Europe is the region in the world with the highest presence of national, government and sectoral CSIRTs
- The study identified 27 CSIRTs recently created by operators of essential services in the seven sectors identified in the NIS Directive; and 11 CSIRTs recently created by national and local administrations
- This effort includes the development of sector-specific and sector-wide CSIRTs and IR collaboration mechanisms, both at EU and national levels, going beyond simple information exchange

Analysis

- These figures demonstrate the increased effort of operators of essential services and administrations to build or upgrade their IR capabilities
- They also further highlight the ‘capability-building impact’ of the NIS Directive

COOPERATION

National Network of CSIRTs
European Commission
ENISA
ISAC
NATO
OSCE
Project "No More Ransom"

Home • Cooperation • National Network of CSIRTs

National Network of CSIRTs

The National Network of CSIRTs is a forum of excellence that enables the sharing of operational information. The main objectives of the National Network of CSIRTs are:

- Trust building between computer security professionals in order to create a cooperative and mutual assistance environment for incident treatment and best practices sharing;
- Develop indicators and national information statistics c proactive and reactive counter measures;
- Create the necessary instruments for the prevention an
- Promote a security culture in Portugal.

Computer Emergency Response Team Austria

WARNUNGEN SERVICES DOWNLOADS **ÜBER UNS** BERICHT

Austrian Trust Circle

Der Austrian Trust Circle ist eine Initiative von CERT.at und dem österreichischen Bundeskanzleramt und besteht aus Security Information Exchanges in den einzelnen Bereichen der strategischen Informationsinfrastruktur (CIIP).

CERT.at bietet hier in Kooperation mit GovCERT Austria und dem österreichischen Bundeskanzleramt einen formellen Rahmen für praxisnahen Informationsaustausch und gemeinsame Projekte im Sicherheitsbereich.

Ziele des Austrian Trust Circles sind

- Unterstützung der Selbsthilfe in den Sektoren im Bereich Sicherheit
- Operative Kontakte für CERT.at bei der Information über und Behandlung von Sicherheitsvorfällen in den Organisationen
- Operative Experten für das Bundeskanzleramt im Krisenfall
- Das Schaffen einer Vertrauensbasis um im Ernstfall gemeinsam agieren zu können
- Vernetzung und Informationsaustausch in und zwischen den Sektoren der strategischen Infrastruktur

Link zur Webseite: www.austriantrustcircle.at

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Home | Current topics | Incident Response | Expertise & Advice | **Cooperation** | Organisation | Conference

Home › Cooperation › National Response Network

Cooperation

I would like to start collaboration | I would like to strengthen my collaboration | International collaboration

National Response Network | ISAC's | Liaisons | ICT Response Board | Cyber Security Council

National Response Network

The National Response Network (NRN) is a collaboration aimed to strengthen the joint response to cyber security incidents. This happens by way of clustering the strengths of various response capabilities. This structures cohesiveness and existing capacities are strengthened.

Study on CSI

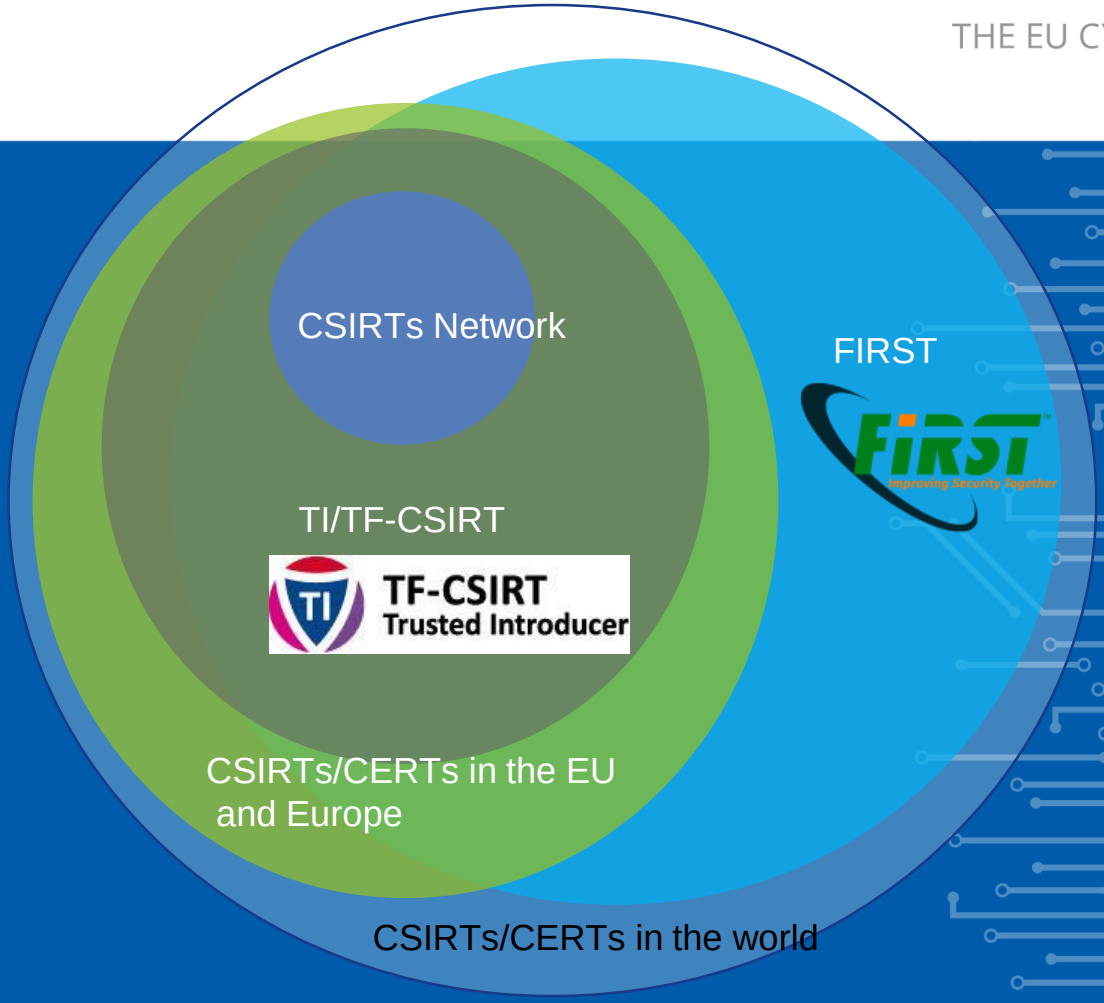
FINDING EHT NI SEVITAITINI NOITAREPOOC LUFSSECCUS -4 NA TA SEITILIBAPAC ESNOPSER TNEDICNI FO DLEIF ETAVIRP-CILBUP YB NEVIRD ERA LEVEL LANOITANRETNI SPIHSRENTRAP

Identified trends

- 2 main kinds of international cooperation initiatives identified in the field of IR and cybersecurity at large:
  - Cooperation between global economic actors of the same sector, as illustrated by the March 2018 initiative led by the World Economic Forum (WEF) in the field of financial services cybersecurity;
  - ‘Cyber Diplomacy’, in particular in the framework of the UN working group on information security which has limited effects due to states’ reluctance to agree on binding measures.

Analysis

- Sovereign states show an unwillingness to agree on binding measures to regulate their behaviours and instead favour a voluntary approach.
- Addressing cybersecurity indeed requires involving technology giants owning the digital infrastructures and data;
- Public-private partnerships are necessary to reach effectiveness at the international level in the field of cybersecurity, even though security is a sovereign domain;


CSIRTs Network
FIRST
TI/TF-CSIRT
TF-CSIRT
Trusted Introducer
CSIRTs/CERTs in the EU
and Europe
CSIRTs/CERTs in the world

THE EU CYBERSECURITY AGENCY

Information Sharing and Analysis Center (ISAC)


```
{
  "values": [
    {
      "entry": [
        {
          "description": "Or 'Unsolicited Bulk Email', this means that the recipient has not granted verifiable permission for the
          "expanded": "Spam",
          "value": "spam"
        },
        {
          "description": "Discreditation or discrimination of somebody, e.g. cyber stalking, racism or threats against one or more
          "expanded": "Harmful Speech",
          "value": "harmful-speech"
        },
        {
          "description": "Child pornography, glorification of violence, etc.",
          "expanded": "Child Porn/Sexual/Violent Content",
          "value": "violence"
        }
      ],
      "predicate": "abusive-content"
    },
    {
      "entry": [
        {
          "description": "System infected with malware, e.g. PC, smartphone or server infected with a rootkit.",
          "expanded": "Infected System",
          "value": "infected-system"
        },
        {
          "description": "Command-and-control server contacted by malware on infected systems.",
          "expanded": "C2 Server",
          "value": "c2-server"
        },
        {
          "description": "URI used for malware distribution, e.g. a download URL included in fake invoice malware spam.",
          "expanded": "Malware Distribution",
          "value": "malware-distribution"
        },
        {
          "description": "URI hosting a malware configuration file, e.g. webinjects for a banking trojan.",
          "expanded": "Malware Configuration",
          "value": "malware-configuration"
```

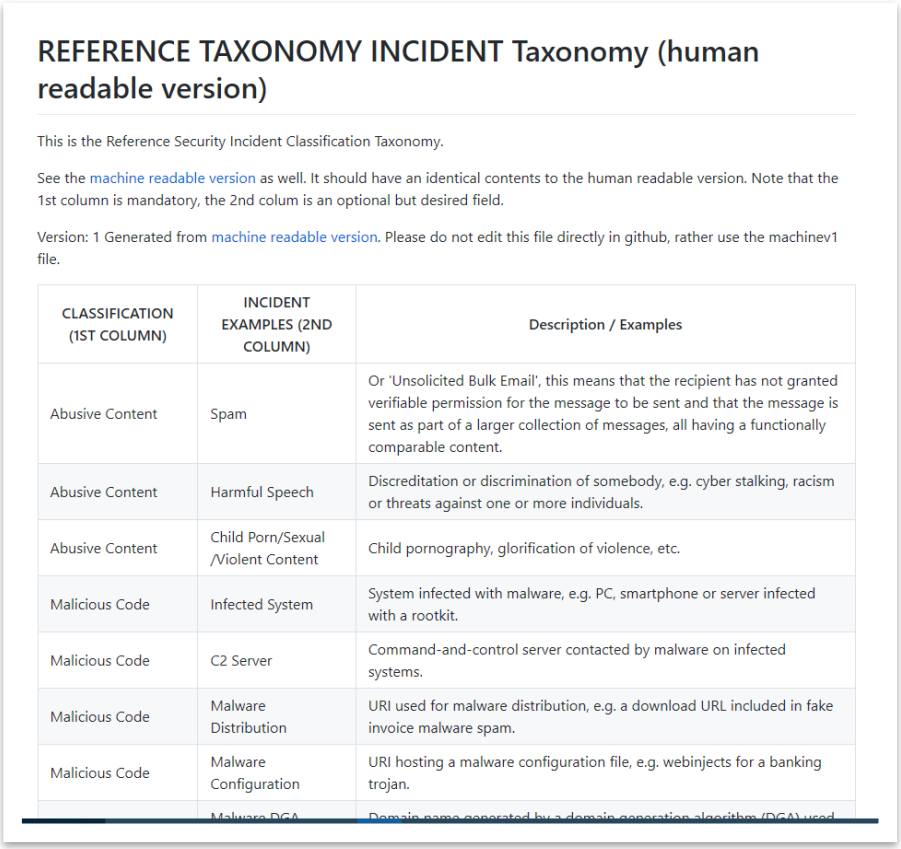

REFERENCE SECURITY INCIDENT TAXONOMY WORKING GROUP (RSIT WG)

REFERENCE INCIDENT TAXONOMY WORKING GROUP – RSIT WG

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

https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force

VERSION 1



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 colum 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.

CLASSIFICATION (1ST COLUMN)	INCIDENT EXAMPLES (2ND COLUMN)	Description / Examples
Abusive Content	Spam	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.
Abusive Content	Harmful Speech	Discreditation or discrimination of somebody, e.g. cyber stalking, racism or threats against one or more individuals.
Abusive Content	Child Porn/Sexual /Violent Content	Child pornography, glorification of violence, etc.
Malicious Code	Infected System	System infected with malware, e.g. PC, smartphone or server infected with a rootkit.
Malicious Code	C2 Server	Command-and-control server contacted by malware on infected systems.
Malicious Code	Malware Distribution	URI used for malware distribution, e.g. a download URL included in fake invoice malware spam.
Malicious Code	Malware Configuration	URI hosting a malware configuration file, e.g. webinjects for a banking trojan.
	Malware DGA	Domain name generated by a domain generation algorithm (DGA) used

https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force

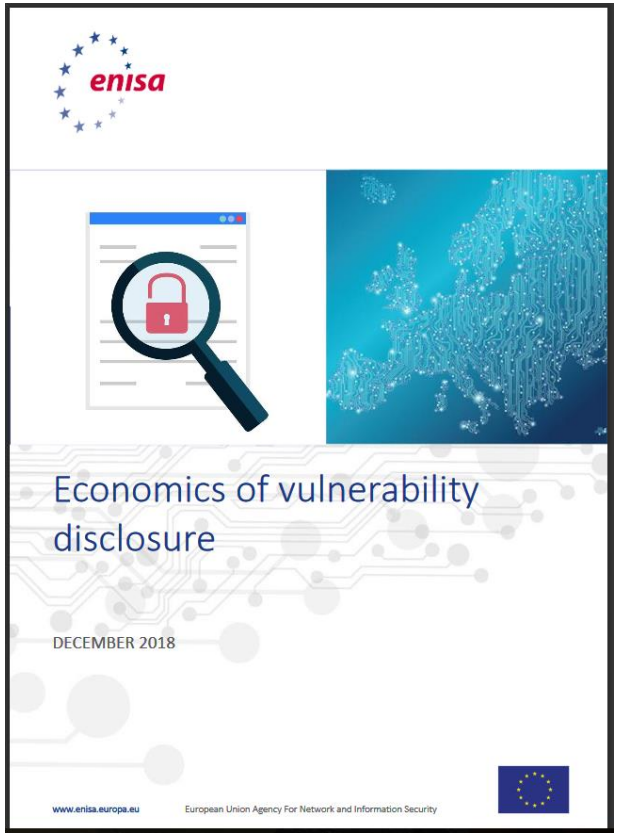
FINDING 5- THERE IS A NEED TO PROMOTE PARTNERSHIPS BETWEEN CSIRTS AND SECURITY VENDORS TO BENEFIT FROM THEIR EXPERTISE AND DEVELOP TOOLS FOR PROACTIVE DETECTION AND RESPONSE

Identified trends

- The development of IRC –in particular for operators of essential sectors - also relies on managed detection and response (MDR) services provided by commercial organisations (these organisations are the most represented constituency in the ENISA inventory)
- The implementation of the 'Cybersecurity-by-design' concept is still below the expected considering the growing number of vulnerabilities found a patched by digital devices providers and hardware manufacturers every year
- Device manufacturers increasingly develop their own CSIRTs, sometimes called PSIRT (Product Security Incident Response Team): IBM, Cisco, Huawei etc.

- Analysis
- It raises a question pertaining to the benefit of both national/governmental CSIRTs and European cybersecurity services providers in the IR value chain
- It also questions the ability of these actors to play a central role should vulnerabilities and cyber-attacks directly affect devices

https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018



https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➲	1. Malware	➲	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	➲	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	➲	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	➲	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	➲	10. Physical manipulation/ damage/ theft/loss	➲	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

file:///C:/Users/dufkoan/AppData/Local/Temp/WP2018%20O.1.2.1%20-%20ENISA%20Threat%20Landscape%202018.pdf

FINDING 6- TRENDS IN THE ORGANISATION OF CYBER DEFENCE IN EUROPEAN ARMIES

Identified trends

- There is a growing number of cyber defence commands and cyber military agencies in European armies (e.g. Germany in 2018, France in 2017)
- Armed forces struggle to ensure the cybersecurity of their digitalized systems, given the complexity of these systems and their lifecycle in a context of a fast-moving ICT landscape
- Military cooperation in the field of cybersecurity takes place in the framework of both NATO and the European Union.

- Analysis
- Cyberspace is now considered as an integral component of modern defence and even warfare
- European armed forces are therefore increasing and rationalize the organisation of their IR and offensive capabilities at a rather rapid pace
- Going through a similar digitalization move and using similar tools than in the civilian sector, Armed Forces are facing similar IT security issues

PESCO – CYBER RAPID RESPONSE TEAMS AND MUTUAL ASSISTANCE

Coordinator

Project Members

Cyber Rapid Response Teams (CRRTs) will allow Member States to help each other to ensure higher level of cyber resilience and to collectively respond to cyber incidents.

Cyber RRTs could be used to assist other Member States and EU Institutions, CSDP operations as well as partner countries.

CRRTs will be equipped with unified Deployable Cyber Toolkits designed to detect, recognise and mitigate cyber threats.

The response teams would be able to assist with training, diagnostics and attribution forensics, and assistance in operations. The aim of this project is to integrate Member State expertise in the field of cyber defence.

https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/

SUMMARY OF THE FINDINGS

1. The implementation of the NIS Directive fosters the adoption of a holistic approach towards IR and an upward alignment of national capabilities
2. The NIS Directive may have a positive effect at the international level and provides the EU with a status of ‘norm setter ’
3. IR capability development of national administration and operators of essential services emphasizes the relevance of collaboration at national and European level
4. Successful cooperation initiatives in the field of Incident Response Capabilities at an international level are driven by public-private partnerships
5. There is an important development of IR services in the European private sector; however, new vulnerabilities tend to target the hardware layer of devices manufactured outside Europe
6. Acknowledging their exposure to cyber risks, military players tend to follow the same dynamics as the civilian sector when developing their IR capabilities

BUILD AND ADVANCE INCIDENT RESPONSE

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

THANK YOU FOR YOUR ATTENTION

+30 28 14 40 9711

CSIRT-Relations@enisa.europa.eu

www.enisa.europe.eu