EUROPEAN UNION AGENCY
FOR CYBERSECURITY

LEGAL AND ORGANISATIONAL ASPECTS OF COOPERATION BETWEEN CSIRTS AND LE

Toolset, Document for trainees

DECEMBER 2019

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found www.enisa.europa.eu.

CONTACT

For contacting the authors please use CSIRT-LE-cooperation@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

AUTHORS

Alexandra Michota (ENISA), Andreas Mitrakas (ENISA), Constantinos Patsakis, Václav Stupka

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-339-1, DOI: 10.2824/68202

TABLE OF CONTENTS

1. WHAT YOU WILL LEARN

1.1 THEMATIC AREA

In 2017, ENISA presented technical as well as legal and organisational aspects of the cooperation between Computer Security Incident Response Teams (CSIRTs) -in particular national and governmental CSIRTs, and Law Enforcement (LE) and provided some recommendations to help them cooperate closer to fight against cybercrime.

ENISA confirmed that CSIRTs and LE often exchange information during incident handling and criminal investigations, both formally and informally, and that trust is the key success factor to their cooperation. However, it is clear that there are challenges related to the diversity of legal systems and legal provisions of the Member States. Adding further complexity is the diversity of communication channels between the various Member States, which hinders the effectiveness of fighting cybercrime.

- **Learning outcomes**

As a result of attending this course, the trainee should be able to:

- Analyse sample legal and organisational aspects of cooperation between CSIRTs and LE
- Identify the key drivers of this cooperation
- Identify the key inhibiting factors of this cooperation

2. CASE STUDIES

2.1 CASE STUDY – LE APPROACH

The objective of this case study is to present the main limitations to the cooperation between CSIRTs and LE due to the diversity of current legislation in different Member States.

For this case study, it is recommended to divide the trainees in groups; thus, the results and approaches of each group can be compared. This should lead to discussion of the advantages and disadvantages of the individual solutions.

2.1.1 Summary

Figure 1: Main objective of the case study

Main Objective	
Targeted Audience	LE, investigators etc.
Total Duration	30 minutes
Scenario	Trainee is a police investigator who deals with cybercrimes.
Task 1	Identify expected activities of relevant stakeholders by filling in the 'Segregation of Duties' (SoD) matrix
Task 2	Identify data to be shared with the CSIRT
Task 3	Identify the procedures should be followed for appointing a CSIRT member as forensic expert
Task 4	Request and use information from the CSIRT cooperation network

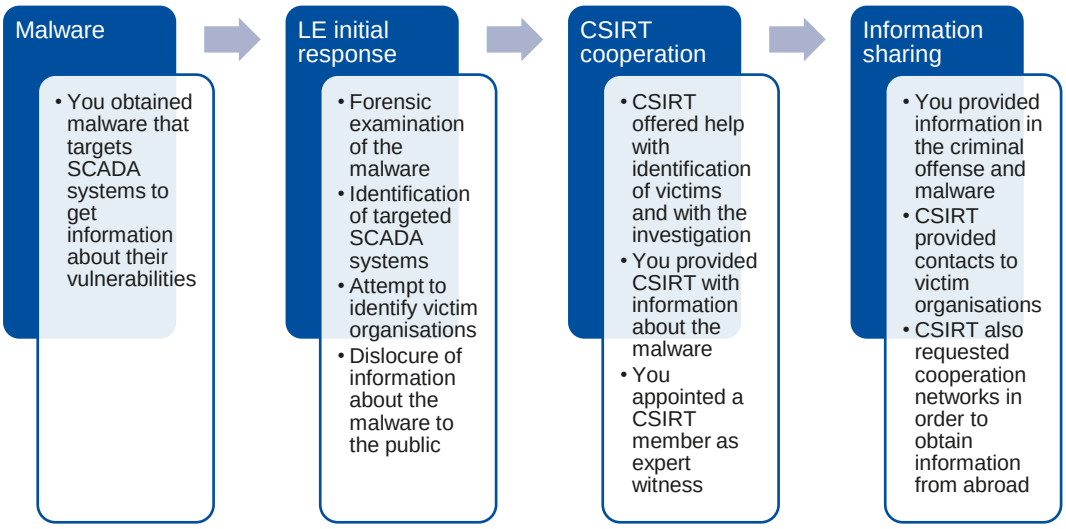
2.1.2 Objectives

- To learn what kind of cooperation and support you can expect from the CSIRT
- To learn how to properly request cooperation and information from the CSIRT
- To evaluate what data and information can be provided by the CSIRT
- To evaluate what data and information you can provide to the CSIRT
- To compare legal procedures for sharing of information and data in different legal cultures

2.1.3 Scenario

The scenario of the case study is presented in the following page.

Figure 2: Case study scenario



2.1.3.1 Organisational profile

You are a police investigator dealing with cybercrime, specifically focused on investigation of organised crime. Your department's jurisdiction is nationwide and deals with cross-border incident cases. LE in your country cooperates with the national and governmental CSIRT via a liaison who is a police officer.

2.1.3.2 Before the breach

You are investigating a crime committed by a foreign perpetrator, which consists of making customized computer viruses. As part of the investigation, you have obtained several malicious programs created by the attacker, including their source code. During the forensic analysis, you have determined that they are designed to attack critical infrastructure in your country, and they collect information about systems' vulnerabilities; this information is uploaded to a server with IP within your national range.

2.1.3.3 Initial response

- Malware collects information about the vulnerabilities of specific SCADA systems.
- You have contacted several critical infrastructure operators, but none of them is using such systems.
- Therefore, you have published in the media information about the vulnerable systems.
- After releasing the information, you are contacting the national CSIRT, which offered you cooperation and help.

2.1.4 Tasks

You, as the lead investigator of the case decided to initiate and lead the cooperation with the CSIRT. Your goal is to both collect as much evidence as possible and help the CSIRT to identify possible attacked operators and help them with the mitigation of any incidents caused by the malware.

2.1.4.1 Segregation of Duties

Please use the SoD matrix (Figure 3) to identify, what activities can be performed or facilitated by your Law Enforcement Agency (LEA), and what you expect from the CSIRT and the judiciary. The SoD matrix should help you to identify expected activities of relevant stakeholders throughout the cybercrime investigation lifecycle. The aim of this matrix is to highlight conflicting or overlapping duties performed by one community or more.

Figure 3: 'Segregation of Duties' matrix

Cybercrime fighting activities	CSIRTs	LE	Judges	Prosecutors	Training topics (e.g. technical skills etc.)
Prior to incident/crime					
Delivering/participating in training					Problem-solving and critical thinking skills
Collecting cyber threat intelligence					Knowledge of cyber threat intelligence landscape
Analysis of vulnerabilities and threats					Development and distribution of tools for preventive and reactive mitigation
Issuing recommendations for new vulnerabilities and threats					Dealing with specific types of threats and vulnerabilities
Advising potential victims on preventive measures against cybercrime					Raising awareness on preventive measures against cybercrime
During the incident/crime					
Discovery of the cybersecurity incident/crime					Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis
Identification and classification of the cybersecurity incident/crime					Incident and crime classification and identification
Identify the type and severity of the compromise					Knowledge of cyber threats and incident response procedures
Evidence collection					Knowledge of what kind of data to collect; organisation skills
Providing technical expertise					Technical skills
Preserving the evidence that may be crucial for the detection of a crime in a criminal trial					Digital investigations; forensics tools;
Advising the victim to report / obligation to report a cybercrime to law enforcement (LE)					Obligations and restriction on information sharing; communication channels
Duty to inform the victim of a cybercrime					Obligations and restrictions to the information sharing
Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.)					Obligations and rules for information sharing among communities.
Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling					Communication skills; communication channels
Mitigation of an incident					Well-prepared & well-organised to react promptly in an incident
Conducting the criminal investigation					Knowledge of the legal framework; decision-making skills
Leading the criminal investigation					Knowledge of the incident response plan; leadership skills
In the case of disagreement, the final say for an investigation					Knowledge of the legal framework; decision-making skills
Authorizing the investigation carried out by the LE					Decision-making in the criminal procedure
Ensuring that fundamental rights are respected during the investigation and prosecution					Fundamental rights in criminal investigations and prosecutions
Post incident/crime					
Systems recovery					Technical skills
Protecting the constituency					Drafting and establishing procedures; technical knowledge
Preventing and containing IT incidents from a technical point of view					Technical skills pertaining to system administration, network administration, technical support or intrusion detection
Analysis and interpretation of collected evidence					Criminalistics, digital forensics, admissible evidence
Requesting testimonies from CSIRTs and LE					Testimonies in a criminal trial
Admitting and assessing the evidence					Evidence in a criminal trial
Judging who committed a crime					Technical knowledge and knowledge of the legal framework
Assessing incident damage and cost					Evaluation skills
Reviewing the response and update policies and procedures					Knowledge how to draft an incident response and procedures

2.1.4.2 Provide information to CSIRT

Your goal is to identify possible harmed infrastructure operators, to prevent possible damage and to prevent losing valuable evidence. In order to identify the victims, you need to provide the CSIRT team with detailed information about the malware, the type of systems it is targeting, and the type of incidents that may arise from its use. For this purpose, you can use the common taxonomy developed by ENISA in cooperation with Europol, which links criminal offenses to specific types of incidents. Please identify data you can share with the CSIRT. If there are any legal restrictions preventing you from sharing specific data, please explain them.

Figure 4: List of information provided to the CSIRT

Information provided to the CSIRT

2.1.4.3 Appoint a CSIRT member as forensic expert

Since none of forensic experts who are available has experience with targeted SCADA systems, you would like to appoint a CSIRT member who is able to provide valuable input about specifics and target vectors implemented by the malware. The CSIRT member is however not listed in any national forensic experts' list nor does he have any experience with criminal procedure. Please explain if it is possible to appoint the CSIRT member as expert witness and what procedure you need to follow. If there are legal restrictions preventing you from appointing him, please propose other ways on how to make use of his knowledge and experience in the criminal investigation.

Figure 5: List of procedures for CSIRT members as expert witnesses

CSIRT member as expert witness

2.1.4.4 Request and use information from CSIRTs cooperation network

You have found out that the creator of the malware is operating abroad in a country where there is no informal police and judicial cooperation and formal mutual legal assistance is ineffective. Therefore, you would like to take advantage of the CSIRT cooperative networks through which unofficial information can be obtained and help you to identify the attacker. Please describe in what legal ways such information could be obtained and for what purposes it could be used in criminal proceedings.

Figure 6: Use of information obtained from the CSIRT network.

Use of informal information from CSIRT cooperation networks

2.1.4.5 Outcomes

After completing the tasks, you should be able to make use of SoD and common taxonomy for cooperation with the CSIRT. You should also know more ways how CSIRTs can help LE and vice versa. Main advantages of cooperation and information sharing is the possibility of use of specific knowledge and information sources of both communities. It is also clear, that there are often legal limitations to the cooperation, which however vary from country to country.

2.1.5 Lessons learned

- Cooperation between CSIRT and LE communities is sometimes necessary to both successfully prosecute cybercriminal and ensure security of attacked infrastructures and systems.
- Table of 'Segregation of Duties' may help you to identify which community should be responsible for what as well as to learn how to avoid duplication of tasks and interference between activities of individual communities.
- Cooperation and information sharing between LE and CSIRTs is sometimes complicated due to lack of specific legislation that would allow closer cooperation.
- There are legal limitations to what kind of information can be shared between CSIRTs and LE; these limitations vary from country to country.
- It could be useful to appoint CSIRT members as expert witnesses; however, there might be legal or procedural limitations.
- CSIRTs are members of cooperative international networks, which may be used in some cases for obtaining valuable information or even evidence.

3. REFERENCES

ENISA. (2017). *Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects.* Retrieved from https://www.enisa.europa.eu/publications/improving-cooperation-between-csirts-and-law-enforcement

A ANNEX: ABBREVIATIONS

Abbreviation	Description
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial-of-Service (attack)
GDPR	General Data Protection Regulation
IOC	Indicators Of Compromise
IP	Internet Protocol
LE	Law Enforcement
LEA	Law Enforcement Agency
SoD	Segregation (or separation) of Duties

TP-01-20-177-EN-N

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-339-1
DOI: 10.2824/68202