EUROPEAN UNION AGENCY
FOR CYBERSECURITY

COOPERATION ACROSS CSIRTS, LE AND THE JUDICIARY

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: 978-92-9204-333-9, DOI: 10.2824/04836

TABLE OF CONTENTS

1. WHAT YOU WILL LEARN

1.1 THEMATIC AREA

In 2018, ENISA confirmed that Computer Security Incident Response Teams (CSIRTs), Law Enforcement (LE) and the judiciary have complementary roles and structures and that incident handling varies across Member States. The data CSIRTs and Law Enforcement Agencies (LEAs) have access to vary, and affect information sharing between them when they seek to respond to cybercrime. CSIRTs interact frequently with LEAs rather than with the prosecutor. CSIRTs offer support to LEAs to collect and analyse different types of evidence. CSIRTs are called rarely as witnesses in courts but the material they collect during the incident handling might be used to decide on cybercrime cases.

Cooperation challenges are identified in the areas of data retention, sharing of personal data (including IP addresses) and confidentiality of criminal investigations as well as admissibility of digital evidence. Legal challenges are followed by cultural, technical and organisational ones.

- **Learning outcomes**

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

  - Demonstrate knowledge of interactions across the three communities; strengths, needs and limitations
  - Analyse the legal and policy framework shaping this cooperation
  - Better understand tools and methods used for the cooperation between CSIRTs and LE and their interaction with the judiciary

2. CASE STUDIES

2.1 CASE STUDY 1

This case study examines the collaboration between CSIRTs and LE when addressing a security incident or a cybercrime as described in a ransomware related scenario. This scenario aims at identifying the roles of each party and thus setting out the means of effective cooperation between them.

Figure 1.1: Main objective of the case study

Main Objective	
Targeted Audience	CSIRTs and LE
Total Duration	30 minutes
Scenario	Trainee is a CSIRT member responsible for detection and mitigation of security incidents or cybercrimes. His/her goal is to address key ramifications of ransomware attack.
Task 1	List the internal guidelines of identifying security incidents or cybercrimes.
Task 2	List the investigation steps that you could undertake.
Task 3	Identify the type and categories of information that you could collect and share with LE in search of evidence.
Task 4	Identify expected activities of relevant stakeholders by filling in the 'Segregation of Duties' (SoD) matrix.
Task 5	List the conclusions that could be derived and the evidence that could be produced.

2.1.1 Objectives

In this exercise you will learn when and how CSIRT members cooperate with LE. In particular, the objectives of this exercise are to:

- Practice in identifying cybercrime cases;
- Raise the trainees' awareness regarding the differences between the legal systems of various countries and the consequences of these differences;
- Explain the legal aspects of CSIRT activity;
- Practice in writing instructions regarding the reporting of a cybercrime to LE;
- Provide information on how to advise LE in the event of a security incidents or cybercrimes.

2.1.2 Scenario

A ransomware attack has been launched through the following steps:

- **The attacker gathered information online and collected email addresses of several organisations.**
- **The attacker sent a malicious word file through an email to all these addresses.**
- **Some users opened the word file.**
- **The malicious payload of the word file downloaded a binary that was executed.**
- **The payload encrypted the files of the current user.**
- **The attacker requests ransom to be paid to a crypto wallet**

2.1.2.1 Organisational profile

Your organisation is a national CSIRT team responsible for detection and mitigation of cybersecurity incidents/cybercrimes.

2.1.2.2 Before the breach

The CSIRT provided its constituency with guidelines on how to identify and report incidents.

A LEA submits an official letter to a CSIRT in order to obtain the required information and investigate an individual incident:

- List the type and categories of data that should be included in that official letter.
- Provide advice on the data requested for each individual incident and list the obligatory and the optional information that should be requested.

Please note that specific rules, policies and guidelines apply in each national LE or CSIRT constituency. For example, identify the following:

- How long is data concerning IP addresses assignments stored?
- What data should the CSIRTs provide to the LE?

2.1.2.3 Initial response

Examples of questions that could be addressed by LE during the investigation process:

- LE asks for the list of log entries that could help to identify users connecting to the internet using computer with IP address 'xxxx'.
- LE asks to identify the user to whom the IP address 'xxxxx' was assigned in a specific period of time, e.g. a few years ago (WHOIS issues)

2.1.3 Tasks

2.1.3.1 Investigation analysis

List the type and categories of information that could be potentially shared with LE during the investigation process of the above described scenario:

Figure 1.2: List of information to be shared with LE

Information to be shared with LE

2.1.3.2 Segregation of Duties

Use the SoD matrix (Figure 1.4) to identify, what activities can be performed or facilitated by your CSIRT, and what you expect from the LE. The SoD matrix should help you also to identify, what kinds of information and data could be useful for the LE and what kinds of data you can request from them and use for mitigating the attack.

2.1.3.3 Outcomes

Through the investigation analysis and the correlation of data shared with LE, list the conclusions that you could derive and the evidence that could be collected:

Figure 1.3: Conclusions

Conclusions

2.1.4 Lessons learned

List the limitations you have faced during this investigation process, as well as the potential benefits of an efficient collaboration with LE.

Figure 1.4: '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

2.2 CASE STUDY 2

This case study examines the collaboration between CSIRTs and LE when addressing a security incident or a cybercrime as described in a Denial of Service (DoS) attack related scenario. This scenario aims at identifying the roles of each party and thus setting out the means of effective cooperation between them.

Figure 2.1: Main objective of the case study

Main Objective	
Targeted Audience	CSIRTs and LE
Total Duration	30 minutes
Scenario	Trainee is a CSIRT member responsible for detection and mitigation of security incidents or cybercrimes. His/her goal is to address key ramifications of DoS attack.
Task 1	List the internal guidelines of identifying security incidents or cybercrimes.
Task 2	List the investigation steps that you could undertake.
Task 3	Identify the type and categories of information that you could collect and share with LE.
Task 4	Identify expected activities of relevant stakeholders by filling in the SoD matrix.
Task 5	List the conclusions that could be derived and the evidence that could be produced.

2.2.1. Objectives

In this exercise, the trainees will learn when and how CSIRT members cooperate with LE. In particular, the objectives of the exercise are to:

- Practice in identifying cybercrime cases;
- Raise the trainees' awareness regarding the differences between the legal systems of various countries and the consequences of these differences;
- Explain the legal aspects of CSIRT activity;
- Practice in writing instructions regarding the reporting of a cybercrime to LE;
- Provide information on how to advise a reporter or LE in the event of a security incident or a cybercrime.

2.2.2. Scenario

The DoS was launched through the following steps:

- **The attacker gathered information online and identified some web servers**
- **The attacker submitted some content to the web servers**
- **The web servers went "down" and do not provide their service**

2.2.2.1. Organisational profile

Your organisation is a national CSIRT responsible for the detection and mitigation of cybersecurity incidents/cybercrimes.

2.2.2.2. Before the breach

The CSIRT provided its constituency with guidelines on how to identify and report incidents.

A LEA submits an official letter to a CSIRT in order to obtain the required information and investigate an individual incident:

- List the type and categories of data that should be included in that official letter.
- Provide advice on the data requested for each individual incident and list the obligatory and the optional information that should be requested.

Please note that specific rules, policies and guidelines apply to each national LE or CSIRT constituency. For example, identify the following:

- How long is data concerning IP addresses assignments stored?
- What data should the CSIRTs provide to the LE?

2.2.3. Tasks

2.2.3.1. Investigation analysis

List the type and categories of information that could be potentially shared with LE during the investigation process of the above described scenario:

Figure 2.2: List of information to be shared with LE

Information to be shared with LE

2.2.3.2. Segregation of Duties

Use the SoD matrix (Figure 2.4) to identify, what activities can be performed or facilitated by your CSIRT, and what you expect from the LE. The SoD matrix should help you also to identify, what kinds of information and data could be useful for the LE and what kinds of data you can request from them and use for mitigating the attack.

2.2.3.3. Outcomes

Through the investigation analysis, the data collected and shared with LE, list the conclusions that you could derive and the evidence that could be collected:

Figure 2.3: Conclusions

Conclusions

2.2.4. Lessons learned

List the limitations you have faced during this investigation process, as well as the potential benefits of an efficient collaboration with LE.

Figure 2.4: '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

3. REFERENCES

ENISA. (2017). *Tools and Methodologies to Support Cooperation between CSIRTs and Law Enforcement.* Retrieved from https://www.enisa.europa.eu/publications/tools-and-methodologies-to-support-cooperation-between-csirts-and-law-enforcement

ENISA. (2017a). *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

ENISA. (2018). *Cooperation between CSIRTs and law enforcement: interaction with the judiciary.* Retrieved from https://www.enisa.europa.eu/publications/improving-cooperation-between-csirts-and-law-enforcement

ENISA. (2018a). *Review of Behavioural Sciences Research in the Field of Cybersecurity.* Retrieved from https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity/

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-01-20-174-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: 978-92-9204-333-9
DOI: 10.2824/04836