Cooperation with Law Enforcement Agencies - Advising in Cyber Crime Cases

Toolset, Document for students

September 2014

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Acknowledgements

Contributors to this report

We would like to thank all our ENISA colleagues who contributed with their input to this report and supervised its completion, especially Lauri Palkmets, Cosmin Ciobanu, Andreas Sfakianakis, Romain Bourgue, and Yonas Leguesse. We would also like to thank the team of Don Stikvoort and Michael Potter from S-CURE, The Netherlands, Mirosław Maj and Tomasz Chlebowski from ComCERT, Poland, and Mirko Wollenberg from PRESECURE Consulting, Germany, who produced the second version of this documents as consultants.

Agreements or Acknowledgements

ENISA wants to thank all institutions and persons who contributed to this document. A special 'Thank You' goes to the following contributors: Anna Felkner, Tomasz Grudzicki, Przemysław Jaroszewski, Piotr Kijewski, Mirosław Maj, Marcin Mielniczek, Elżbieta Nowicka, Cezary Rzewuski, Krzysztof Silicki, Rafał Tarłowski from NASK/CERT Polska, who produced the first version of this document as consultants and the countless people who reviewed this document.

Contact

For contacting the authors please use CERT-Relations@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2013

Reproduction is authorised provided the source is acknowledged.

Table of Contents

1 What Will You Learn

During this exercise you will learn how to advise in a cyber-crime **case, as well as when and how** to effectively cooperate with an LEA. In particular, you will:

- practice the identification of cyber-crime cases;
- discuss differences in the legal systems of various countries and the consequences of these differences;
- practice writing instructions regarding the reporting of a cyber-crime to an LEA;
- improve your skills in advising a reporter or an LEA in a cyber-crime case; and
- develop your ideas about what kinds of training could be useful for an LEA.

2 Exercise Task

2.1 Task 1 Identifying and reporting cyber crimes

Imagine that the following incidents have been reported to you. Which would you consider to be cyber-crimes according to the cyber law of your country? Name each type of the identified cyber-crimes (e.g., computer intrusion, etc.).

1	Reposting a personal message to a mailing group	
2	Multiple login attempts by an unauthorised user	
3	Discovering the weak points of a computer system by scanning	
4	Observing and recording network traffic (wiretapping)	
5	Attempting unauthorized remote or local access to someone's computer	
6	Sending mails with abusive content	
7	Attempting to use an unknown exploit	
8	Forwarding or re-posting a message received with word changes	
9	Selling or installing copies of unlicensed commercial software or other copyright protected materials	
10	Attempt to acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication	
11	A successful compromise of a system or application by exploiting vulnerabilities	
12	Using someone's FTP site to deposit materials which somebody else wants other people to pick up	
13	Including, or inserting into a system, software intended for a harmful purpose	
14	Limiting the availability of someone's computer resources by sending lots of packets	

15	Sending large amounts of unsolicited mails to people	

2.2 Task 2 CERT advises an incident reporter in a cyber-crime case

Read the following descriptions of three incidents reported to CERT:

- A user reports that he receives e-mails with viruses from one particular address. (The reporter suspects that they are sent on purpose.) The reporter provides the details of his mailbox (login and password) with a request for it to be checked with the CERT's help.
- A server administrator at the University reports that its web server (IP given) has become the target of a massive DDoS attack. The number of connections from the attacking hosts exceeded 35,000 in the first days, but on that day, the attacks were boosted and occurred 4 times a day for 2 to 3.5 hours each time and the number of connections (recorded in firewall logs) was more than 130,000. The total number of attacking hosts was likely of more than 1,000. They had already blocked about 450 of the attacking networks. In most cases, attacks originated from the network in France, the Netherlands and Germany.
- A bank reports that it has been informed that there is a website hosted by some company which is involved in a phishing scheme to obtain personal account information from the customers of this bank.

Write separate instructions for the victims of these incidents, including your advice and an explanation on how to report the incidents to an LEA.

2.3 Task 3 CERT advises LEA in a cyber-crime case

The trainer asks you what kind of aspects should be addressed in cooperation with an LEA. Then, he or she asks you to think about what a CERT could advise when it receives a call from an LEA regarding a case of suspected cyber-crime.

What would you do in cases involving:

a) a denial of service attack,

b) phishing, and

c) cyber defamation?

1. What kind of information should the LEA provide you with?
2. How could you identify the source of the crime?
3. What could you advise the LEA to do?

2.4 Task 4 CERT prepares training for LEA

The trainer asks you to think about proposals for CERT training for an LEA. What kind of training will it be? What kind of advice should this training contain?

Below are some examples of queries from an LEA:

- The LEA asks you to establish the owner of an e-mail address.
- The LEA sends you a letter without the return address.
- The LEA asks questions without proper authorization or an appropriate signature.

- The LEA asks for a list of log entries that could help identify users connecting to the Internet using a computer with an IP address xxxx.
- The LEA asks for the identity of the user who was assigned IP address xxxx during a specific period of time a few years ago.
- The LEA asks for log entries containing a list of all connections established on a particular day.

Think about proposals for CERT training for an LEA which would decrease the number of such questions.

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu