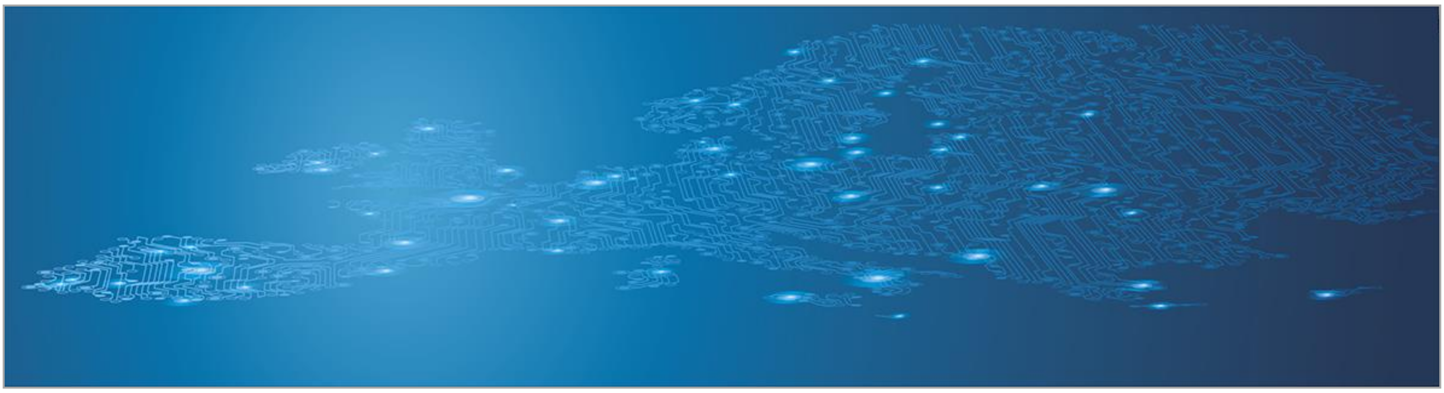

CERT participation in incident handling related to the Article 13a obligations

Toolset, Document for students

September 2014

enisa

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

Table of Contents

1 What Will You Learn

During this exercise you will learn about rules, procedures and best practice in handling incident related to obligation for Internet Service Providers described in the Article 13a of the European Telecom Package[1]. The exercise will last approximately 3 hours and it consists three tasks.

The purpose of this exercise is to prepare you to be ready to analyse a set of data related to the Internet attacks. The proposed type of attacks, which you will deal with, will be typical attacks which should be reported to the Regulatory Authority according to the rules and obligations for Internet Service Providers described in the Article 13a of the European Telecom Package.

Particularly during the exercise you will learn:

- How to analyse network traffic data related to the attack
- What kind of information can be obtained from network traffic data
- How to prepare the report which should be used for reporting security incident according to the Article 13a

2 Exercise Task

Listen to introduction to the attack provided by the trainer. Imagine that you play role of representative of ISP CSIRT team, which is responsible along with other duties for analysing network monitoring data and preparing an incident security report for National Regulatory Authority.

From the trainer introduction especially remember that there are three different levels of incident notifications and obligations related to them2:

- Service provider reporting to National Regulatory Authority
- National Regulatory Authority reporting to other National Regulatory Authorities
- National Regulatory Authority reporting to ENISA

[1] *„DIRECTIVE 2009/140/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL" - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF*

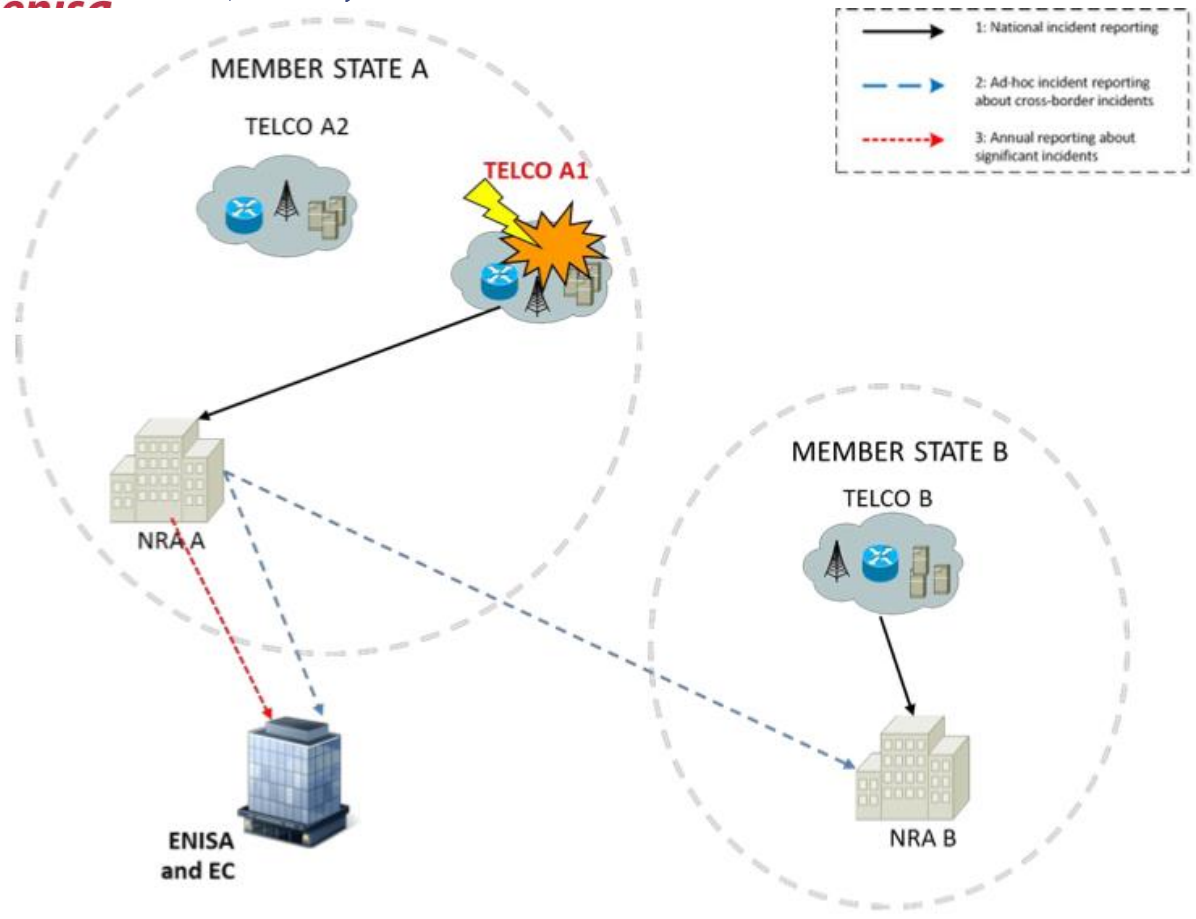
1: National incident reporting
2: Ad-hoc incident reporting about cross-border incidents
3: Annual reporting about significant incidents
MEMBER STATE A
TELCO A2
TELCO A1
NRA A
ENISA and EC
MEMBER STATE B
TELCO B
NRA B

Figure 1: Reporting schemes of Article 13a[2]

These obligations are described in the paragraph 3 of the Article 13a[3]:

"Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services."

In practice it means that the provider (mainly it will relate to Internet Service Providers) should continuously monitor the level of the security of their telecommunication resources. Detection and especially reaction and handling to observed incidents should be based on the best practices related to incident handling activities[4], what means that incident handling capability should exists in all providers.

[2] *„Technical Guideline on Reporting Incidents – Article 13a Implementation." - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents%20reporting/Technical%20Guidelines%20on%20Incident%20Reporting/incidents-reporting-to-enisa/technical-guideline-on-incident-reporting*

[3] *http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf*

[4] *ENISA Good Practice Guide for Incident Management: http://www.enisa.europa.eu/activities/cert/support/incident-management*

Where appropriate, the national regulatory authority concerned shall inform the national regulatory authorities in other Member States and the European Network and Information Security Agency (ENISA). The national regulatory authority concerned may inform the public or require the undertakings to do so, where it determines that disclosure of the breach is in the public interest.

In particular case, when the security incident could have a significant influence on level of security in other countries than country of incident origin, cooperation and effective communication between national regulatory authorities is very important. Thanks to this cooperation an appropriate warning and alerting in other countries is possible. It is worth to add that this internal country warning and alerting activities very often base on CERT involvement in these processes.

What is the meaning of where appropriate and what is the timeframe? Once a year, the national regulatory authority concerned shall submit a summary report to the Commission and ENISA on the notifications received and the action taken in accordance with this paragraph."

This activity is for gathering relevant information about Internet network breaches. The assumption is that it will help to better understand new trends and mechanisms in Internet threats as well as it will be an important element for making Internet security awareness for public.

There is the security incident related to the ISP network: the online service for customers is not available due to ongoing DDoS (Distributed Denial of Service) attack. There is no clear information how long it could last, what could be requests from customers in case they have no access to their data and possibility to change business.

2.1 Task 1 Building technical environment for analysing network monitoring data

Your task is to install software tools which you will need to perform the analysis of network monitoring data. You should install the Wireshark software (http://www.wireshark.org). The Wireshark application installation guide can be found in the "Wireshark User's Guide" in the chapter 2: "Building and Installing Wireshark". Additionally as a recommended tool you should install and use the tcpdump tool (http://www.tcpdump.org).

The pcap file which will be analysed will be provided to you by the trainer.

2.2 Task 2 Analysing of network monitoring data

Network monitoring data, which you are provided in this exercise, includes different types of network TCP/IP protocol data like: ICMP flows, UDP flows. You should make the following types of analysis:

*Subtask 1 – **determination of time and volume of the attack***

Firstly, please create a short summary including basic information of each pcap file they have. They should check:

- start and end time of capture,
- size of captured packets,
- total number of packets as well as average packet/byte rates.

This information should give general overview of the size of data, which are going to be analysed.

*Subtask 2 – **determination of types of DDoS attacks in terms of their technical specification***

In the next step you should examine captured traffic and try to determine what kind of a DDoS attack was performed. Usually during a DDoS attack it's used more than one DDoS technique or there are separate and distinct attack sources. At this point you should try to create

Wireshark or tcpdump BPF (Berkeley Packet Filter) filter that would allow filtering out each type of DDoS attack stream.

In fact there are two kinds of attacks and this should be found by participants (see below).

1. ICMP flood: All ICMP packets were type 3 (Destination Unreachable) with codes 3 (Destination Port Unreachable) and a few cases of code 1 (Destination host unreachable) and 13 (Communication administratively prohibited).
2. UDP flood: UDP flood consisted of many fragmented IP packets. For all of them protocol field was set to UDP and for most of them there was either MF flag set or fragment offset was greater than zero. Not surprisingly all IP fragments were received for no UDP packet. Please use Wireshark and Tcpdump filters to determine both DDoS attacks types (ICMP flood and UDP flood).

If you have a problem with developing correct filters, please ask the trainer for assistance.

Your next task is to recognize what distinct streams DDoS attack consisted (either different attack methods/techniques or clear source distinction). You can analyse input/output statistics for those streams in comparison to normal server traffic. To complete this task they should:

1. Open PCAP file in Wireshark
2. Choose Statistics → IO Graph
3. Use display filters created in previous point to create separate graphs.
4. Adjust other options if needed (X & Y axis scale, line style, etc.)

Subtask 3 ***– Determination of endpoints' addresses of hosts***

In this subtask you should determinate endpoints' addresses of analysed hosts. There are various ways to export such addresses – again you can do this using either Wireshark or tcpdump.

As soon as you successfully determinate endpoints, please produce the list of unique IP addresses (ddos_ip.uniq). It is practical, because you can use such list for finding more information, e.g. autonomous systems. To get list of autonomous systems associated with these addresses you can use free service available at The Shadowserver Foundation:

http://www.shadowserver.org/wiki/pmwiki.php/Services/IP-BGP

All information gathered in during the subtasks should be used to prepare the full report (see Task 3)

2.3 Task 3 Preparing report according to the article 13a template report

After collecting all information from network monitoring data, you should prepare security incident report for NRA. For better preparation of this report firstly you should learn more about reporting schema template. Please get familiar with the template below. Listen to the trainer explanation and try to understand in details fields. For further reading you can use the guide from the ENISA document: "Technical Guide on Reporting Incidents" . In your example report, please use one of the ISP providers which you know the best. The name of ISP can be fictitious.

Field	Description	Tip for fulfilling
Country	The country that sends the report to NRA.	Choose the country of a group choice
Date and time	Details of the date and time when the incident took place (in national time). It can be interpreted as the time the incident was discovered. Time should be expressed in both CET and local time.	According to analysed logs
Impacted services	The affected service: the service rendered unavailable to the end-user. This field includes a description of the service whose continuity and availability are affected by the impact level. It should be noted that assessing the LoS (Level of Service) and QoS (Quality of Service) introduces complexity into the analysis criteria and can become subjective. The possible choice is: fixed telephony, mobile telephony, (short) message services, internet, and email.	According to participants' knowledge about online service functionality and services
Number of users affected	The total number of users affected when an incident occurs. (% of all affected users of that service in a given country). The national report to the NRA may include absolute number which the NRA would have to translate to percentages for inclusion in the annual report to ENISA and the EC.	According to participants' knowledge about online service functionality and services.
Duration	The duration of the incidents	According to analysed logs

Geographic spread/region	If available the region impacted by the incident.	According to the participants’ choice of ISP geographical location. Add information about geographical location of attacking parties.
Impact on Emergency calls	If available emergency service impacted by the incident.	For the purpose of the exercise the real data of CSIRTs which are represented by participants
Description	Fill in any further information you can share of the impact of the incident.	According to the findings from logs analysis.
Root cause	What kind of disaster or reason caused the security problem. The potential choices are: natural disaster or phenomena, human error, malicious attack, hardware or software failure, failure at third party or external party.	According to participants’ knowledge about the source of incident. The description and findings can be changed during the analysis.
Other incident information	A general description of the incident. Also the description of the all incident handling actions and activities undertaken by a handler and post incident actions. In this part of the report there is information about other possible parties affected by an incident. Other descriptive information about an incident is: lessons learnt from an incident and further remarks. There is one more particular information requested – “NRA’s contacted (in case of a cross –border incident). This one is especially dedicated for NRA. From the perspective of ISP and its CERT it is included in information about cooperation and contact with other parties.	

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