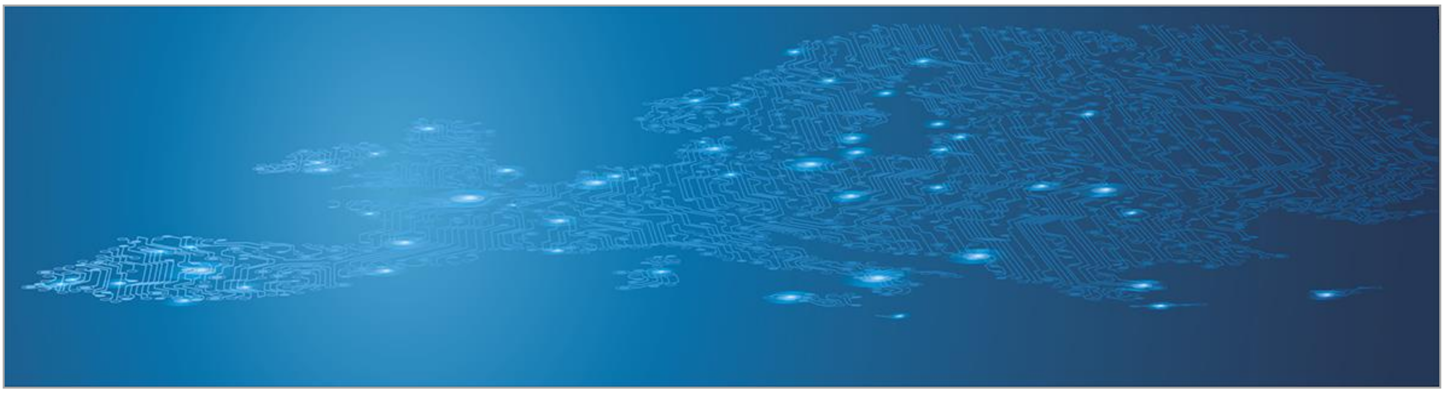

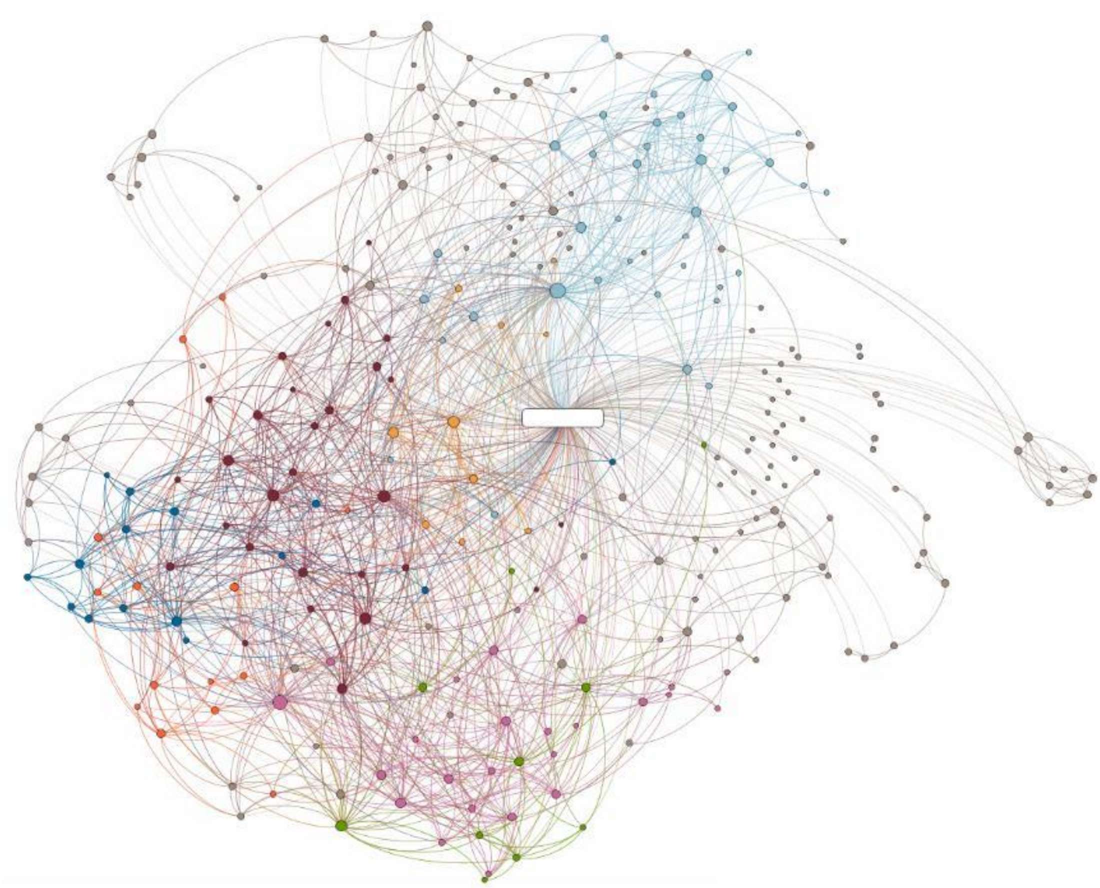

Establishing External Contact

Handbook, Document for teachers

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 Introduction

Goal

To enhance students' skills in establishing contacts with other CERTs, administrators of ISPs, and other parties responsible for the mitigation of security incidents in their networks around the globe.

Target audience

This exercise is primarily targeted at new and future employees of CERTs. It requires an understanding of Internet attacks and communication skills. The students should be also good in written and spoken English.

Course Duration

Session One: 1 hour, 10 minutes

Session Two: 50 minutes

Note: Students are required to spend additional time on monitoring the mailboxes and responding to e-mails between the sessions.

Frequency

Once per team member

Structure of this document

	Task	Duration
	Session One	
	Introduction	10 min
	Task 1: Preparatory research	30 min
	Task 2: Creating the letters	30 min
	Session Two	
	Task 3: Review	30 min
	Summary to the exercise	20 min

2 General Description

The communication and exchange of information is one of the crucial aspects of CERT work. The more effectively information is shared and exchanged between interested parties, the faster security incidents can be mitigated and less damage occurs. Thus, it is very important to have at hand, and know how to use, sources of contact information, networks of contacts and other channels for the distribution and sharing of data.

The goal of this exercise is to enhance students' skills in establishing contacts with other CERTs, administrators of ISPs, and other parties responsible for the mitigation of security incidents in their networks around the globe. The students will be asked to identify and contact proper authorities about real incidents. After finishing the exercise, the students should be able to establish and develop networks of contacts faster and more effectively.

In order to conduct the exercise you need to secure logs from a security system such as a firewall, IDS/IPS, honeypot, netflow from darknets, etc. The logs should include attack descriptions (or the attack type must be easily identifiable), timestamps including time-zone and source IP addresses. If needed, any data about the targeted host can be anonymized. The logs must not be more than five days old.

Alternatively, you may use spam e-mails as long as you know precisely how to identify the source of the message and explain to the students where to look for the offending host.

The students will also need to access and use their business e-mail accounts. It is recommended that PGP/GPG is available for these accounts.

The students should be also able to make international phone calls when necessary.

Before you start the exercise, split the logs into as many parts as the number of students taking the exercise. While doing so, try to make sure that information about sources does not overlap for different students – in other words, no two students should receive information about the same hosts.

Planning the exercise: Note that the exercise is conducted in two sessions, the second one scheduled for two or more working days after the first one. Plan your and the students' time, and book the rooms, etc, accordingly.

3 EXERCISE COURSE

3.1 Keys to the exercise

3.1.1 Session One

3.1.1.1 Introduction

Distribute logs to the students – send them by e-mail or post them on a web page for download. Ask each student to choose between three and five attacks with distinct sources from their logs. Preferably, these sources should be distributed geographically.

3.1.1.2 Task 1 Preparatory research

Ask the students to identify a responsible party (IPS, CERT, etc) that should be able to coordinate. They will find instructions for this in their book. Allow 20-30 minutes for the research. Review the findings, and ask students how they found the contacts and their reasons for choosing them.

3.1.1.3 Task 2 Creating the letters

Ask students to prepare the correspondence. Each e-mail should contain:

- an introduction - this part should include identification of the team on whose behalf the students are working);
- a description of the problem;
- evidence; and
- a request for action.

Allow 20-30 minutes for this part of the exercise. Review the contents, and then let the students send their e-mails.

Pay attention to the tone of the reports. While they should contain a clear request for action, it should not be demanding. CERT should not put itself into a role that might discourage administrators from cooperating, especially where there is no formal relationship between the CERT and the business or ISP in question.

Ask students to monitor their mailboxes regularly and to reply if needed. Inform the students about the time of the second session, which should be held at least two working days ahead in order to allow enough time for replies.

3.1.2 Session Two

3.1.2.1 Task 3 Review

Ask the students to identify a responsible party (IPS, CERT, etc.) who should be able to coordinate. Then ask each student to report on his or her results:

- How many replies did he or she get (with reference to the number of e-mails sent)?
- Was more information exchanged than in the initial e-mail?
- Was the attack mitigated?

4 Summary of the exercise

If replies were received, discuss different reactions and what triggered them. If some students were significantly more successful than others, how were their reports different?

If no replies were received, ask the students to discuss the possible reasons why:

- The e-mail did not reach the responsible person (incorrect data published or wrong sources used);
- The e-mail was filtered out;
- The problem was treated with low priority and queued;
- The ISP / CERT does not act appropriately on abuse from its network; and/or
- Other reasons.

Optionally, ask students to call parties who did not respond in a timely manner. Use information found in whois databases and on web pages (call centres?). Take time differences into consideration!

5 EVALUATION METRICS

You can use the following factors to evaluate the exercise:

- How many reports successfully reached intended recipients?
- In how many cases was positive feedback received?
- How many incidents were successfully mitigated?

When preparing for the exercise, make sure you can measure these numbers as precisely as possible. Use positive examples to motivate students, explain what could be fixed in cases of failure. Explain that no feedback does not necessarily mean unresolved incidents and that even skilled and experienced incident handlers are not able to guarantee success in resolution in all circumstances. Some negative factors beyond the control of the handler, impacting incident resolution, are:

- unresponsive administrators;
- lack of proper laws and regulations;
- lack of technical means to react beyond own network; and
- inert enforcement of the law.

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