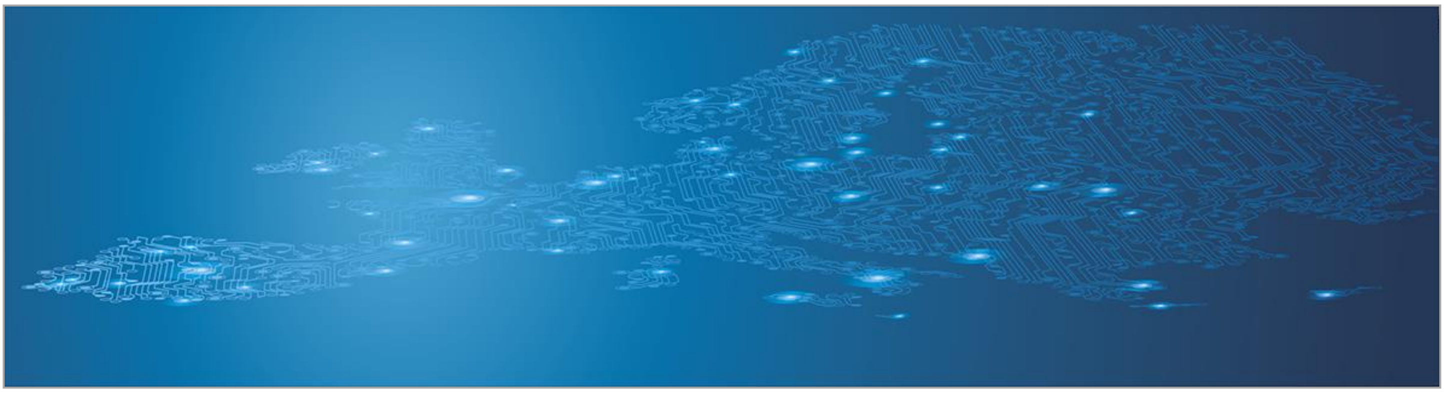

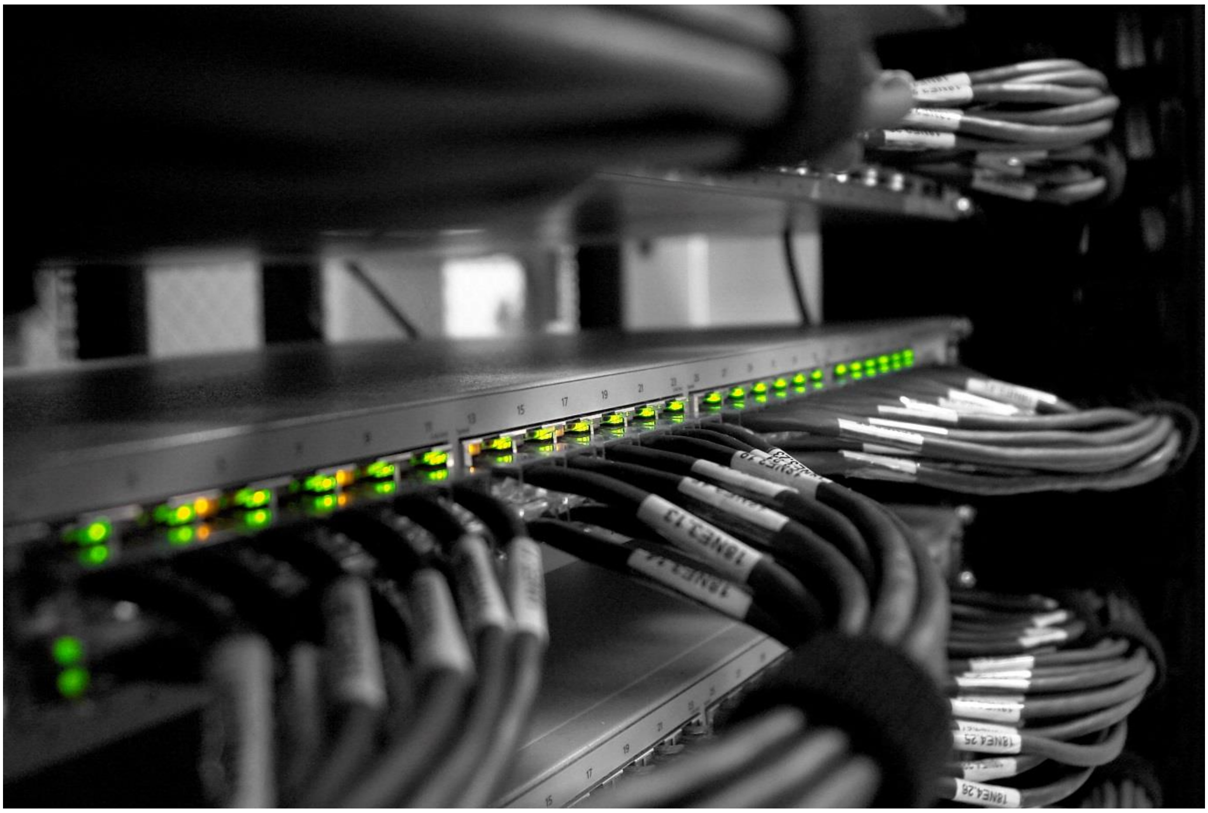

Developing CERT Infrastructure

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

Table of Contents

1 What Will You Learn

The aim of this exercise is to provide you with an understanding of the software tools and hardware required by a CERT in order to offer a service.

2 Ecercise Task

Although the roles and functions of CERTs vary, there are many common services provided by different CERTs. The trainer will give you a general introduction to common CSIRT service models. A suggested model for this exercise is presented at http://www.cert.org/csirts/services.html. You will create a concept for providing these services. The trainer will act as a mentor, asking leading questions to help you find your way. An example service – Incident Handling – Incident Analysis – will be completed at the beginning, with the trainer playing a more important role to give you a better understanding how you should proceed. Handouts with network diagrams will be provided to make your task easier.

2.1 Task 1 Incident Handling – Incident Analysis

Attached below you will find diagrams showing the infrastructure of a new CERT. This CERT is expected to provide an incident handling service. Your task is to answer the questions of the trainer regarding the infrastructure needed to provide the service. Is the architecture, as presented, sufficient? Do you have ideas on what software will be required? Any suggestions for improvements?

2.2 Task 2 Further 3-5 services

Together with the trainer, choose 3-5 services as described in the CERT document. Modify and expand the existing infrastructure shown in the diagrams below in order to achieve your desired goal of providing these services. Enumerate the software you would use.

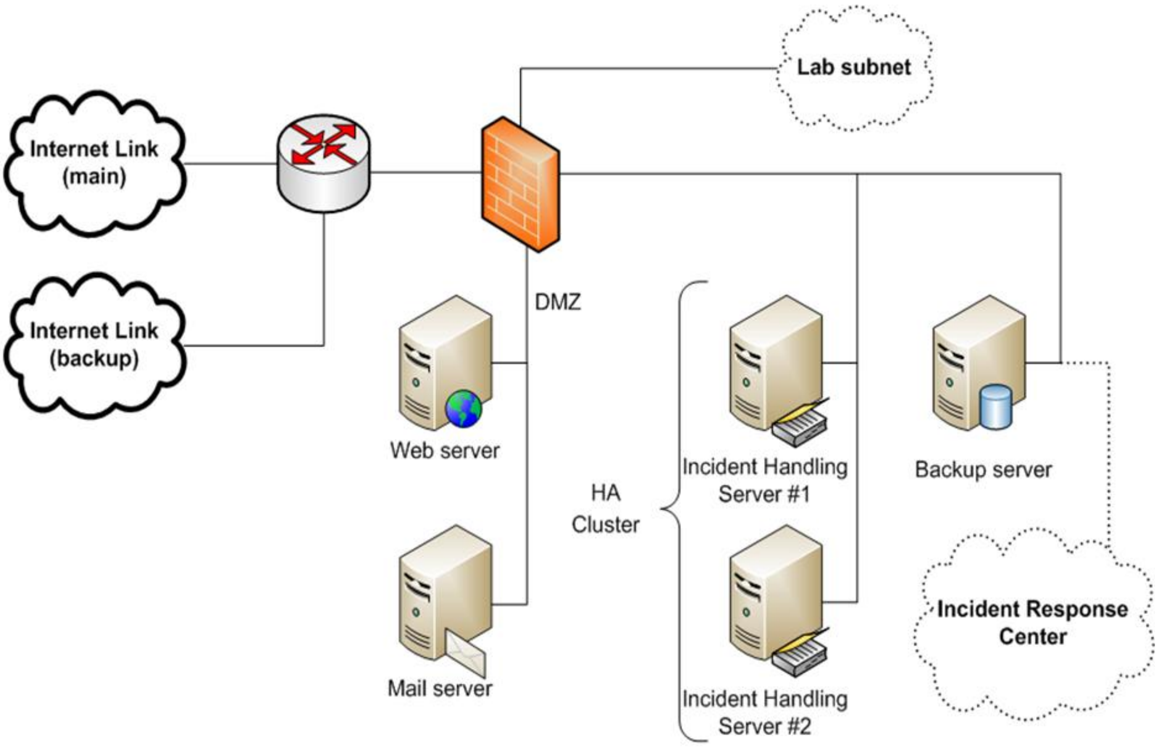

Figure 1: Sample CSIRT network infrastructure

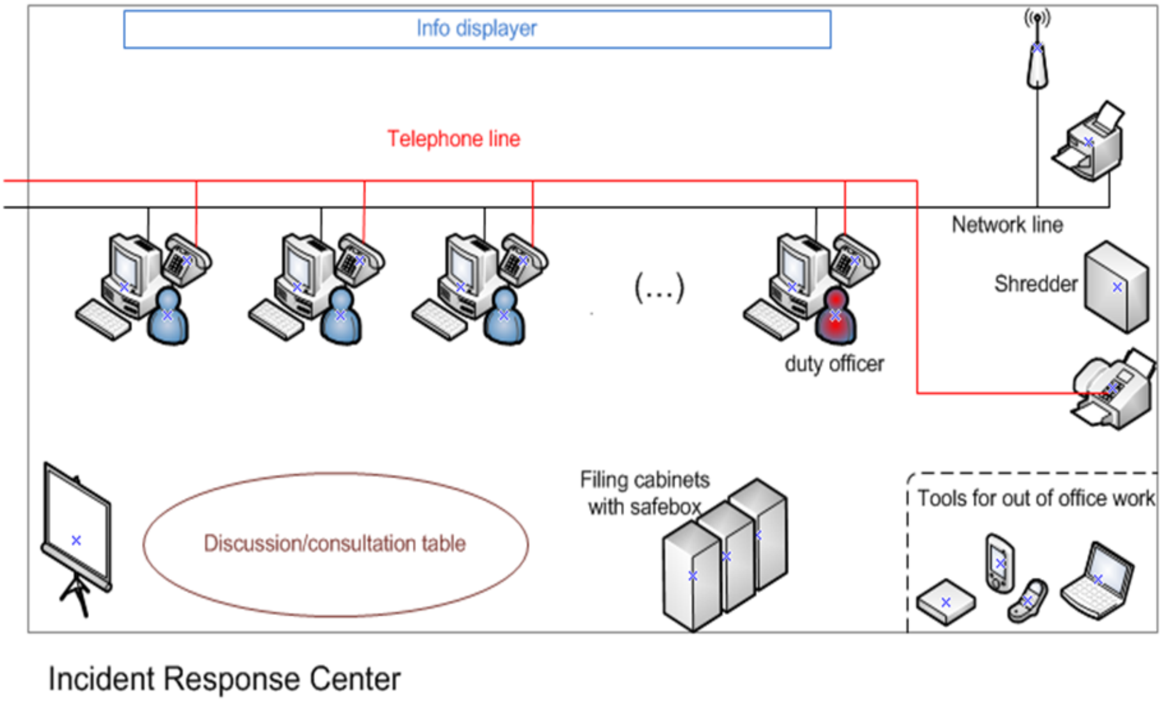

Figure 2: Incident Response Center

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