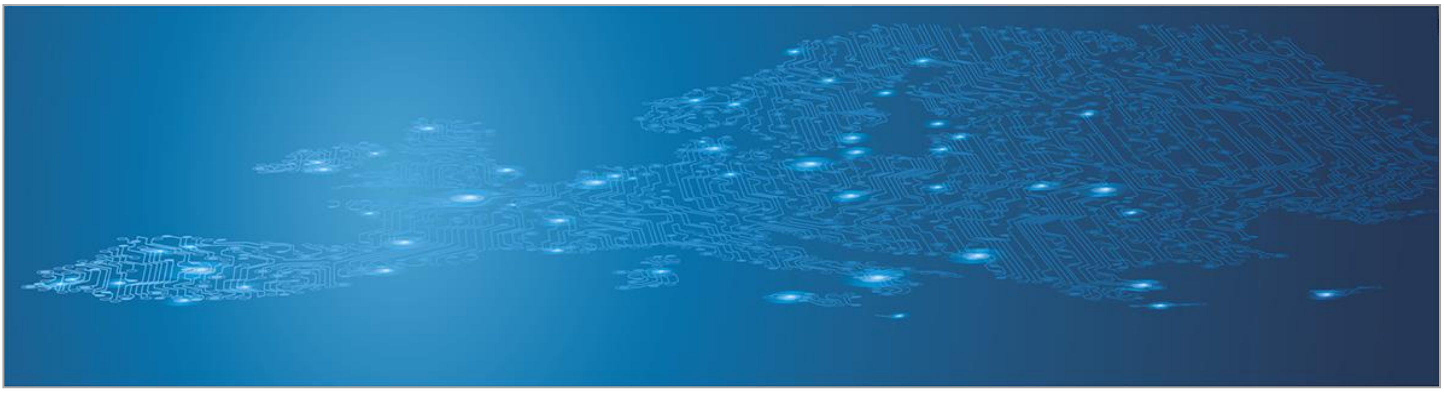

Incident handling during attack on Critical Information Infrastructure

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

In this exercise you will learn how to address incidents in critical information infrastructures (CII) and Supervisory Control and Data Acquisition (SCADA) environments

- Focus will be on dealing with organisational processes which are found commonly in SCADA environments
- Additionally some technical analysis has to be done to complete the exercise
- Both parts will be embedded into a role-play scenario

2 Exercise Task

Before the exercise starts you will be given an introduction to the topic by your trainer. According to your existing knowledge the main terms and principles of SCADA/CII will be explained

2.1 Task 1 Analyse network infrastructure and scenario introduction

You will find material related to the scenario (especially the network map shown below) in the folder /usr/share/trainee/13_CIH. Other background information and material will be given to you by the instructor as the exercise proceeds.

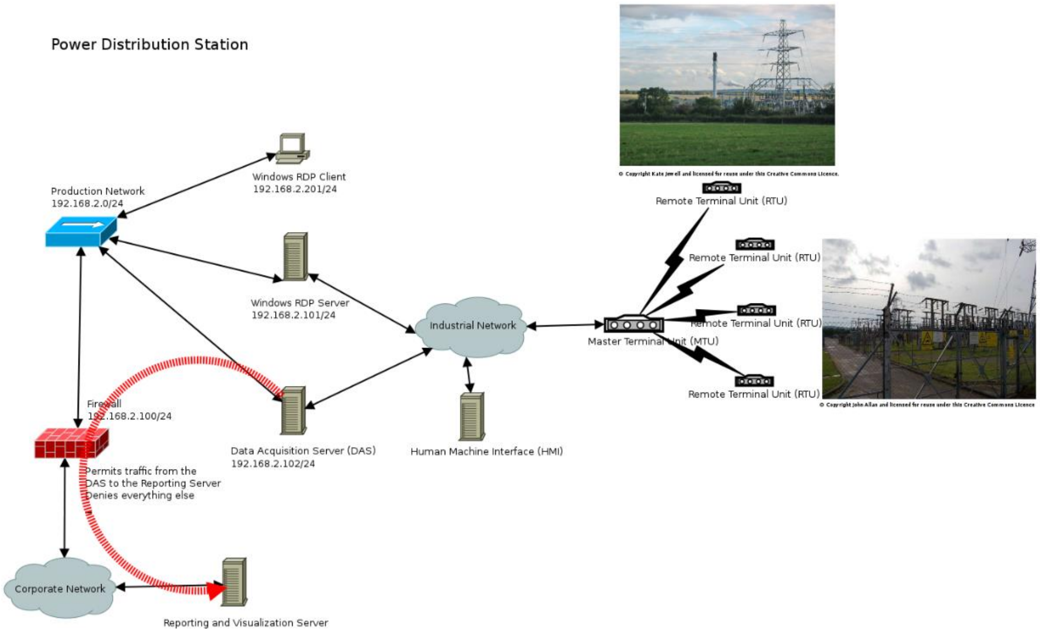
Power Distribution Station
© Copyright Kate Jewell and licensed for reuse under this Creative Commons Licence.
Remote Terminal Unit (RTU)
Windows RDP Client
192.168.2.201/24
Production Network
192.168.2.0/24
Remote Terminal Unit (RTU)
Windows RDP Server
192.168.2.101/24
Industrial Network
Master Terminal Unit (MTU)
Remote Terminal Unit (RTU)
Remote Terminal Unit (RTU)
© Copyright John Allan and licensed for reuse under this Creative Commons Licence
Firewall
192.168.2.100/24
Data Acquisition Server (DAS)
192.168.2.102/24
Human Machine Interface (HMI)
Permits traffic from the
DAS to the Reporting Server
Denies everything else
Corporate Network
Reporting and Visualization Server

Figure 1: Map of SCADA network

The instructor will introduce the scenario with background information and hand-outs like the network map shown above. You will also be asked to define different roles in your team, like these:

- CERT Manager

The manager should supervise the incident handling process and be ready to take action if necessary or when the team escalates action items.

- Handlers/Analysts

The investigation must be documented and reported to the team manager. There might be situations where the team has to escalate issues to the manager (like overriding an uncooperative CII Admin). Tasks in regard to the team include:

- Handler on duty Initial contact for any indication of an incident. Responsible for triage and keeping track of all actions.

- Liaison officers

Optional role for contacts towards third-parties

- Specialized Analysts

You might decide to implement specialised roles for network analysis, malware analysis etc.

Other roles will be played by the instructor or some third party:

- National CERT
- CII Admin

2.2 Task 2 Accessing and analysing incident data

Events during the role-playing will be controlled by the instructor. Evidence and background information will be delivered as seems adequate by the instructor. Main steps during the incident handling are (explanations made by the instructor during the introduction as necessary):

1. Receive notification

   Notification will come in the way of two mails (text below):

First email:

Dear colleagues,

We inform you about verified threats regarding critical information infrastructures in central Utopia. We have been informed by our sources that combined physical and non-physical attack vectors might be used to disrupt production processes in the industrial complex in this area.

With kind regards,

National CERT

Second email:

> Hello colleagues,
>
> Personally I don't think its business for you, but my boss told me to inform you anyway. At one of our substations we experienced some issues with the electric tension at the output. There are minor variances, which have caused problems at some of our customer's equipment. So far, we have not been able to track the cause.
>
> You may contact me via company internal phone number: 2442-3646
>
> Regards,
>
> CII Admin

2. Verification and data acquisition
3. Analysis
4. Containment
5. Mitigation

2.3 Task 3 Discussion of findings

You should at least be able to answer the following questions after the investigation:

1. Who is responsible for the attack?
2. What actions were conducted?
3. Which assets were affected?
4. How were these assets affected?

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