Incident Handling in Live Role Playing

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

Copyright Notice

Table of Contents

1 What Will You Learn

This exercise is designed to introduce you to many different layers and aspects of incident handling, including but not limited to:

- interaction with end-users;
- interaction with administrators;
- vulnerability handling; and
- talking to the management.

It should help you to get into other people's shoes, understand their needs and expectations during the incident handling process and improve your communications with different actors.

2 Exercise Task

2.1 Task Role-playing Game

This is a role-playing game that will take you into the world of incident handling. Doesn't sound like much fun? Well, it depends on you, as you will have a lot of freedom in developing the scenario and taking turns in the actions. Try to be an as interactive as possible.

You will receive a small note with a personal description of your character. This is for your eyes only! If you decide to take some action (eg, call someone), ask the game master for permission. He has the power to give or take back any information, fast forward or revert the time, and influence your decisions. However, keep in mind that you should not try to speculate on the decisions of other players and vice versa – you should not let others decide for you (unless they are your bosses, of course).

You can exchange information with other characters by meeting them face to face, making calls, sending emails, etc. Just describe what you are doing and interact with your partner. Remember that you cannot use any information that you heard when other characters talked unless your character was in the same room; the same rule applies to the other participants.

At the end of the game you will be asked to share your opinions, so keep them for then. You can make notes on how you would proceed if you knew something in advance or if you were playing another character, and share them with everyone later.

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