itrust consulting

malware.lu CERT

Computer Emergency Response Team

General information

Type	Policy
Sequence number	Cooo
Version	1.0
State	Final
Approved by	C. Harpes
Date	27/02/2017
Classification	Public

Distribution list

The current version of the incident management policy is available from the malware.lu website; its URL is http://www.malware.lu.

Changes to this document are not distributed by a mailing-list, RSS or any other mechanism. Please address any specific questions or remarks to malware.lu CERT e-mail address to cert@malware.lu.

Document history

Version	Date	Author	Modifications
0.1	20/02/2017	T. Mouelhi	Document creation.
0.2	23/02/2017	N. Kasselouris	Document review.
0.3	23/02/2017	C. Muller	Quality review.
1.0	27/02/2017	C. Harpes	Validation.

Working group

Name	Organisation
C. Muller, T. Mouelhi, N. Kasselouris, C. Harpes	itrust consulting

Approbations

Name	Role	Responsibility	Date	Signature
N. Kasselouris	Head of ethical hacking	Content agreement	27/02/2017	See printed version managed by CISO.
C. Muller	CISO	Quality agreement	27/02/2017	See printed version managed by CISO.
C. Harpes	Managing Director	Applicability	27/02/2017	See printed version managed by CISO.

Management summary

The Computer Emergency Response Team (CERT) policy describes organisation as well as main objectives of the CERT and provides an overview of the other main sub-policies.

It includes following aspects which are described in this document:

- CERT roles and objectives;
- Incident management scheme;
- Vulnerability disclosure.

Table of contents

1 Introduction

1.1 Context

The malware.lu CERT provides incident response services for itrust consulting customers and third parties located in Luxembourg in addition to itrust consulting staff itself.

1.2 Objectives

The objectives of this policy are to provide an overview of the malware.lu CERT roles and objectives, how incidents are handled and how vulnerabilities are disclosed.

1.3 Document structure

The chapters of this report are structured as follows:

- Chapter 2 presents the role and objectives of the malware.lu CERT;
- Chapter 3 discusses the incident management organisation;
- Chapter 4 introduces the vulnerability disclosure.

1.4 References

[1] POL_C100_malware.lu CERT vulnerability disclosure.
[2] POL_C200_Incident management.
[3] PRO_C010_Incident response.
[4] PRO_C020_Collection of evidence.
[5] STA_C002_CSIRT service presentation.
[6] STA_C003_CSIRT organisational chart.
[7] STA_C004_Incident categories.
[8] STA_C005_malware.lu CERT incident reporting form.
[9] STA_C006_malware.lu roles and skills.
[10] STA_C007_On-demand malware analysis template.
[11] STA_C008_malware analysis methodology.

1.5 Glossary

Terminology	Description
Computer security incident response team (CSIRT)	Team of appropriately skilled and trusted members of the organisation that handles information security incidents during their lifecycle.
Information security event	Occurrence indicating a possible breach of information security policies or failure of controls.
Information security incident	One or multiple related and identified information security events that may harm an organisation's assets and/or compromise its operations.
Information security incident management	Exercise of a consistent and effective approach to the handling of information security incidents.
Incident handling	Actions of detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.
Incident response	Actions taken to protect and restore the normal operational conditions of an information system and the information stored in it when an information security incident occurs.

1.6 Acronyms

Acronym	Definition
CERT	Computer Emergency Response Team.
CSIRT	Computer Security Incident Response Team.
MMS	Multimedia Messaging Service.
PGP	Pretty Good Privacy.
RSS	Rich Site Summary.
SMS	Short Message Service.
SCADA	Supervisory Control and Data Acquisition.

2 Objectives and organisation of the malware.lu CERT

The main role of the malware.lu CERT is to address all types of computer security incidents. The incident responses are adapted to the different incident types (depending on incident classification as described in [7]). In addition, incident response takes into consideration other aspects including the available resources and incident impact.

The malware.lu CERT aims at addressing incidents occurring in SCADA systems and providing assistance to the affected organisations. SCADA systems are becoming more and more important and the potential impact of these incidents can be significant. Required expertise to tackle this kind of incidents is currently being acquired by the CERT team through trainings in this area.

malware.lu CERT is officially listed as a trusted introducer since 17 December 2012.

The malware.lu CERT team is organised as follows:

- CSIRT manager: defines job scope and reports to the top management;
- Planning team: maintains the CERT policies and implements the security processes in addition to reporting to the top management. It is also in charge of communication to other third party and high level organisations;
- Response team: performs the incident triage, coordination and resolution.

The current malware.lu CERT organisation chart is maintained in [6]. Further details regarding the malware.lu CERT team roles and skills are also presented in [9].

3 Incident management

The incident management process involves the following steps:

- Plan and prepare: involves the preparation of the appropriate processes/procedures for incident classification, storage, response logging, and forensics analysis procedures. Internal organisation of the malware.lu CERT and important contact information must also be documented. The current contact information listing is maintained in [5].
- Detection and registration: involves the process of reporting and storage. All itrust consulting employees and contractors are in charge of reporting any information security events as soon as possible. The information security incident reporting form is available at [8].
- Assessment and decision: involves the evaluation of all collected information to assist in high quality assessment and appropriate decision on how to tackle the incident. The collection of evidence is described in [4]. In addition, the malware.lu CERT relies on a well-defined process for performing the assessment [11].
- Response: involves the final action towards handling the incident based on the previous assessment and decision. It is described in [3].
- Lessons learnt: involves improving current processes and procedures based on how the incident was handled.

Incident management is also described in detail in the related policy [2].

4 Vulnerability disclosure

Managing director approval is required before any vulnerability disclosure. In addition, the vulnerability disclosure takes into consideration the CERT constituency security aspect as well as the need of vendors to have enough time to provide security patches.

The publication schedule is always negotiated with the impacted software vendors or community (in case of open source systems).

Vulnerability disclosure is presented in detail in [1].