malware.lu CERT

Incident management

General information

Type	Policy
Sequence number	C200
Version	1.1
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	18/11/2016	N. Kasselouris	Document creation.
0.2	18/11/2016	C. Muller	Quality review.
1.0	18/11/2016	C. Harpes	Final review and validation.
1.1	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 incident management policy describes how incident management is organised at malware.lu CERT and its main objectives.

Incident management organisation include following aspects which are described in this policy:

- Incident management scheme;
- Computer security incident response team with its roles and responsibilities;
- Co-operation, interaction and disclosure of information;
- Communication and authentication;
- Awareness and training;
- Testing of incident management response plan;
- Principle of anonymity and confidentiality.

Table of contents

List of figures

List of table

1 Introduction

1.1 Context

The incident management policy is part of the incident management support offered by malware.lu CERT and extends the CSIRT service presentation document [2] (RFC 2350 from IETF: "Expectations for Computer Security Incident Response").

1.2 Objectives

The objectives of this policy are to define a methodology on how malware.lu CERT handles information security incidents reported by customers, third parties or even by itrust consulting itself.

1.3 Document structure

The chapters of this report are structured as follows:

- Chapter 2 outlines the importance of an effective and efficient incident management;
- Chapter 3 presents the incident management organisation at malware.lu CERT including the information security management scheme, the definition of the roles and responsibilities of the computer security incident response team (CSIRT), the relationships and connections with external organisations and how awareness, training and testing is organised;
- Chapter 4 clarifies the principle of anonymity and confidentiality regarding ICT-incidents.

1.4 References

[1] PRO_C010_Incident response.

[2] STA_C002_CSIRT service presentation.

[3] STA_C003_CSIRT organisational chart.

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.

2 Importance of incident management for malware.lu CERT

The gains of a structured well-planned approach to incident management are:

- Information security events are dealt efficiently, in particular in identifying whether they need to be categorised and classified as incidents or not;
- Identified incidents are assessed and responded to in the most appropriate and efficient manner.

To help achieve this, malware.lu CERT worked out a methodology which ensures that incidents are documented in a consistent manner, using appropriate standards for incident categorisation and classification, and sharing, so that metrics are derived from aggregated data over a period of time.

3 Incident management organisation

The following sections describe the incident management scheme, the roles and responsibilities and how awareness, trainings and tests are organised to ensure that malware.lu CERT members exactly know how to handle incidents according to their methodology.

malware.lu CERT addresses all types of computer security incidents which occur, or threaten to occur, in the constituency networks.

The level of support given by malware.lu CERT will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and malware.lu CERT's available resources. However, in all cases, some response will be made.

3.1 Computer security incident response team (CSIRT)

The CSIRT is a team of appropriately skilled and trusted itrust consulting staff members that provide proper responses, analysis, and prevention of various incidents that occur on computer networks.

The following table resumes the CSIRT organisation at malware.lu CERT and the different responsibilities assigned to the different roles.

Role	Responsibilities
CSIRT manager	As a leader, the CSIRT manager is responsible for managing the staffs, defining the job scope, and reporting the status to higher-level organisations.
Planning team	The responsibilities of the planning team are: • Establishing and updating the incident management security policy; • Implementing security processes; • Communicating with higher-level organisations and other third-party organisations; • Supporting administration; • Performing other activities directed by the CSIRT manager.
Response team	Incident triage: • Help investigating whether indeed an incident occurred; • Help determining the extent of the incident. Incident coordination: • Determining the initial cause of the incident (e.g. vulnerability exploited, ...); • Facilitating contact with other sites which may be involved; • Facilitating contact with appropriate law enforcement officials, if necessary; • Making reports to other CSIRTs; • Composing announcements to users, if applicable. Incident resolution: • Helping to remove the vulnerability; • Helping to secure the system from the effects of the incident; • Collecting evidence of the incident.

Table 1: Roles and responsibilities of the CSIRT.

The up-to-date CSIRT organisational chart [3] showing the roles of the different staff members can be requested if necessary.

3.2 Incident management scheme

The incident management scheme of malware.lu CERT consists of five phases (see Figure 1) described in the following sub-sections. The used technologies and incident response plan are described in malware.lu CERT's operational procedures [1].

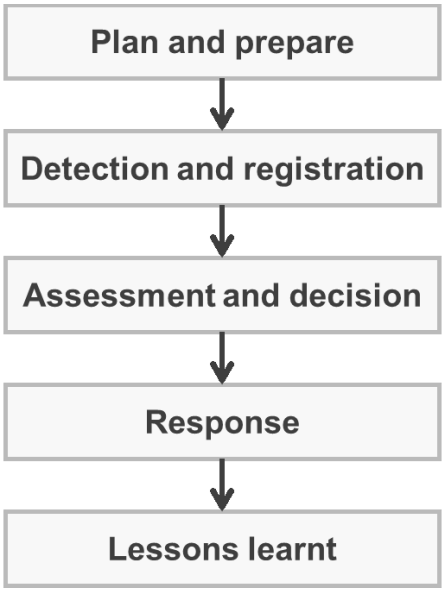

Figure 1: Incident management phases.

3.2.1 Plan and prepare

Effective incident management requires appropriate planning and preparation. Hence, malware.lu CERT completed a number of preparatory activities after the necessary planning.

This includes:

- A standardised approach to events/incident categorisation and classification;
- An information security event/incident database structured in standardised formats for the exchange of information, which is likely to provide the capability to share reports/alerts, compare results, improve alert information and enable a more accurate view of the threats to, and vulnerabilities of information systems;
- Procedures to be followed to ensure that all incident management activities are properly logged;
- Procedures for forensics analysis;
- The scheme of organisational structure for incident management;
- The terms of reference and responsibilities of the CSIRT as a whole, and of individual members;
- Important contact information.

3.2.2 Detection and registration

The second phase of incident management involves the detection of, collecting information associated with, and registration of security events.

All employees and contractors should be made aware of their responsibility to report information security events as quickly as possible and of the point of contact to which the events should be reported. Reporting

of security events should be done using the company's information systems and services for any observed or suspected information security weaknesses in systems or services.

Reporting procedures should include the following:

- Preparing information security event reporting forms;
- Procedures detailing the reporting details for logging of an information security event;
- Established formal disciplinary process for dealing with employees who commit security breaches;
- Feedback processes ensuring that people reporting information security events are notified of results after the issue has been managed.

3.2.3 Assessment and decision

The third phase of incident management involves the assessment of information associated with occurrences of security events and decision on if it is a security incident.

All information collected pertaining to an event or incident is stored in the event/incident database managed by the CSIRT. The information reported during each activity should be as complete as possible at the time, to ensure that there is a good base available for the assessments and decisions to be made, and, of course, the actions taken.

3.2.4 Response

The fourth phase of incident management involves the making of responses to incidents in accordance with the actions agreed in the "assessment and decision" phase.

Dependent on the decisions the responses could be made immediately, in real -time or in near real time.

3.2.5 Lessons learnt

The fifth phase of operational use of the incident management scheme follows when incidents have been resolved/closed, and involves learning the lessons from how incidents have been handled and dealt with. Based on these findings, related procedures and methodologies used by the CSIRT should be continually adapted and ameliorated.

3.3 Co-operation, interaction and disclosure of information

malware.lu CERT exchanges all necessary information with other CSIRTs as well as with affected parties, administrators.

All sensible data (such as personal data, system configurations, and known vulnerabilities with their locations, etc.) are encrypted if they must be transmitted over unsecured environment. Based on the need of protection (confidentiality/ integrity/ non-repudiation), the parties involved in the communication shall in advance clarify on the cryptosystem and exchange format to use.

3.4 Communication and authentication

itrust consulting's "Inventory management and asset classification" procedure is applied:

- In view of the types of information that malware.lu CERT deals with, telephones will be considered sufficiently secure to be used even unencrypted;

Note: telephones in this sense are used to perform phone calls and does not include mobile phone features like SMS, MMS, email, etc;

- Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data;
- If it is necessary to send highly sensitive data (i.e. information classified as confidential) by e-mail, encryption (preferably PGP) will be used;
- All e-mail or data communication originating from malware.lu CERT will be digitally signed, using a generic PGP key of malware.lu CERT, or the malware.lu CERT's team members own signature keys.

3.5 Awareness and training

Incident management is a process that involves not only technical means but also people. Thus, it shall be supported by appropriately trained individuals within malware.lu CERT.

There exists a specific training program for the CSIRT members as necessary. Each group of people involved directly with the management of incidents may require different levels of training, depending on the type, frequency and criticality of their interaction with the incident management scheme.

Before the incident management scheme becomes operational, malware.lu CERT ensures that all relevant personnel are familiar with the procedures involved in the handling of events, and selected personnel are very knowledgeable about the subsequent activities.

Mainly the training of CSIRT members consists of specific exercises and testing on how to manage incidents following the incident management scheme in place.

3.6 Testing

malware.lu CERT regular checks and tests the incident management processes and procedures to highlight potential flaws and problems that may arise during the management of events and incidents. Periodic tests are organised to check processes/procedures and to verify how the CSIRT responds to severe, complex incidents, through the simulation of realistic attacks, failures or faults. Particular attention should be paid to the creation of the simulated scenarios, which should be based on real threats. Tests should involve not only the CSIRT, but all the internal and external organisations that are involved in the management of incidents.

4 Anonymity and confidentiality

4.1 Information disclosure

All members of malware.lu CERT have responsibility to protect the confidentiality of managed data, regardless of its format and of the medium on which the data is stored or over which it is transmitted.

In order to avoid any leakage of sensitive information, members of malware.lu CERT disclose information only if necessary and in compliance with the following rules.

4.2 Information protection

malware.lu CERT complies with the need-to-know principle when exchanging information: information which is not public will NOT be freely delivered, and will ONLY be shared with those who need to know.

Information will be disclosed according to the original level of confidentiality.

malware.lu CERT respects the information classification allocated by originators of information communicated to malware.lu CERT.

The disclosure of sensitive information will be done **only if needed** for resolving an incident. The subsection "Anonymisation" below, states principles followed by malware.lu CERT to disclose such information.

Frequently, malware.lu CERT interacts with multiple groups including, but not exclusively, other CSIRTs and parties concerned, administrators, vendors, law-enforcement agencies, press, or others. Information disclosure to these groups are managed individually and commensurately with the risk involved in information disclosure.

malware.lu CERT reserves the right to make sign the non-disclosure agreements before any information exchange.

When communicating with other CSIRT and sites, malware.lu CERT ensures that the information which is made available to others:

- Is signed for non-repudiation assurance and;
- Is encrypted for confidentiality protection whenever deemed necessary according to the rules mentioned here.

4.3 Private data protection and legal aspects

malware.lu CERT releases information to governing authorities or to the authorised third parties whenever there is a legal obligation to do so. However, malware.lu CERT delays this action until such a circumstance has been established irrevocably, e.g. by court order.

malware.lu CERT notifies always in such cases the persons or organisations concerned.

Every case of processing and communicating personal data fulfils in form and content the requirements defined by the CNPD and the Luxembourgish Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data.

4.4 Anonymisation

Sensitive information is anonymised before it is shared with third parties. Neither personal information (which could specifically identify an attack target or any individuals), nor extra data will be exchanged unless explicitly authorised by the owner of the data or appropriately anonymised.

Where anonymising information would not be practical or counterproductive with regard to the handling of the incident, malware.lu CERT reserves the right to share specific non-anonymised information with trusted closed groups. These exchanges are done with respect to the applicable laws and with the explicit approval of the owner of the information to be exchanged.