Incident Reporting Guidelines for Constituents (Public)

Version 3.0 - 2016.01.19 (Final)

Procedure (PRO 301)

TLP: TLP:WHITE

Classification: PUBLIC

Department: GOVCERT.LU

Contents

1 Introduction **3**
1.1 Overview . . . 3
1.2 Purpose . . . 3
1.3 Scope . . . 3
1.4 References . . . 3
1.5 Abbreviations . . . 3

2 Definition **4**
2.1 Event . . . 4
2.2 Information Security Incident (or Incident) . . . 4
2.3 Information Security Event . . . 4
2.4 Critical System . . . 4
2.5 Non Critical System . . . 4

3 Incident Reporting Guidelines **5**

4 Incident Reporting Timeframe **5**

5 Service Level Agreement (SLA) **6**

6 Incident Categories **6**

7 Disclosure Policy **8**

8 Annexe **9**

Bureaux: 50, rue du Château
L-6961 Senningen
Adresse postale: B.P. 11
L-6905 Niederanven
Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964
http://www.govcert.lu
info@govcert.etat.lu

1 Introduction

1.1 Overview

The response to an incident is dependent on the quality of the information reported by the constituent, on the reporting timeframe and on the capacity of the organisation in charge of the incident to solve the problem. This procedure defines a reporting method to help the constituent to report an incident to GOVCERT.LU within the required timeframe and a common set of terms between GOVCERT.LU and its constituency.

1.2 Purpose

The aim of this procedure is to define guidelines for reporting an incident.

1.3 Scope

This procedure concerns GOVCERT.LU members and its constituency.

1.4 References

1. *FRM702.301 - Incident Reporting Form*
2. *POL204 - Information Disclosure Policy*
3. *PRO303 - Incident Categories*

1.5 Abbreviations

Abbreviation	Definition
CERT	Computer Emergency Response Team
GOVCERT.LU	CERT Governmental of Luxembourg
NIST	National Institute of Standards and Technology
CAT	Incident category
IDS	Intrusion detection system
DNS	Domain name system
IP	Internet protocol

Table 1: Definitions and Abbreviations

Bureaux: 50, rue du Château
L-6961 Senningen
Adresse postale: B.P. 11
L-6905 Niederanven
Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964
http://www.govcert.lu
info@govcert.etat.lu

2 Definition

2.1 Event

An event is an occurrence or change of a particular set of circumstances:

- (NOTE 1) An event can be one or more occurrences, and can have several causes.
- (NOTE 2) An event can consist of something not happening.
- (NOTE 3) An event can sometimes be referred to as an “incident” or “accident”.

2.2 Information Security Incident (or Incident)

An information security incident (or incident) is a single or a series of unwanted or unexpected information security events (section 2.3) that have a significant probability of compromising business operations and threatening information security[1].

2.3 Information Security Event

An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

2.4 Critical System

A critical system is a system, application, data, or other resources that is essential to the survival of an organisation. When a critical system fails or is interrupted, core operations are significantly impacted.

2.5 Non Critical System

Non critical system is a system, application, data, or other resources which don’t have strong impacts to the good operation of the constituent if compromised.

[1] where *information security* means preservation of confidentiality, integrity and availability of information

Bureaux: 50, rue du Château
L-6961 Senningen
Adresse postale: B.P. 11
L-6905 Niederanven
Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964
http://www.govcert.lu
info@govcert.etat.lu

3 Incident Reporting Guidelines

Incident reports should include a description of the incident or event, using the appropriate taxonomy, and as much of the following information as possible; however, **reporting should not be delayed in order to gain additional information**:

- Constituent name
- Point of contact information including name, telephone, and email address
- Incident Category Type (e.g., CAT 1, CAT 2, etc., see table 3)
- Incident date and time, including time zone
- Location and name of the system(s) involved in the incident
- Method used to identify the incident (e.g., IDS, audit log analysis, system administrator)
- Actions* done (date, time, result)
- Impact
- Resolution
- Criticality of the system (national or local system, classified system, etc.)

Constituent should utilise this model when reporting incidents to GOVCERT.LU. Depending on the criticality of the incident, it is not always feasible to gather all the information prior to reporting. In this case, constituent should continue to report information as it is collected.

To help the constituent to report an incident to GOVCERT.LU, a reporting form is available on the website of GOVCERT.LU (http://www.govcert.lu).

After having filled out the reporting form, send it within the required timeframe (see table 3) by email to address: soc@govcert.etat.lu or by FAX (unsecured fax). Emails when possible or needed, shall be encrypted. The anonymous form can be used.

For general questions except for reporting incidents, you can also write directly to email address info@govcert.etat.lu or by phone to our Hotline.

*** In order to preserve evidences and keep investigation capacity for GOVCERT.LU, the actions done for containing the incident shall be limited to the strict minimum (no re-install of system or of software).**

4 Incident Reporting Timeframe

The reporting timeframe of an incident defined in table 3 correspond to timeframe in which the constituent should report the incident. Once this timeframe exceeded, GOVCERT.LU cannot assure that the incident will be solved efficiently.

Bureaux: 50, rue du Château
L-6961 Senningen
Adresse postale: B.P. 11
L-6905 Niederanven
Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964
http://www.govcert.lu
info@govcert.etat.lu

5 Service Level Agreement (SLA)

Once the incident has been recorded by GOVCERT.LU, a notification email is automatically sent to the requestor. This email informs the requester (1) that the incident has been taken into account by GOVCERT.LU and (2) about the incident ticket number which shall be used for each related communication with GOVCERT.LU.

Once the incident ticket created, GOVCERT.LU starts the incident identification phase (incident categories and priority allocation). This phase is followed by the incident response phase which consists in the resolving the incident.

Depending on the incident priority, GOVCERT.LU agrees to meet the following SLA **for starting** the incident response phase (threats containment and eradication, recovery of the targeted information system):

Levels	Maximum timeframe for starting incident response phase[2]
Priority 1	24h after the incident registering
Priority 2	16h after the incident registering
Priority 3	8h after the incident registering
Priority 4	4h after the incident registering

Table 2: Priority Levels

6 Incident Categories

In order to clearly communicate incidents and events (any observable occurrence in a network or system) throughout the supported organisations, it is necessary for GOVCERT.LU and its constituency to adopt a common set of terms and relationships between those terms.

Below find a high level set of concepts and descriptions to categorise information security incidents:

The reading order of table 3 is top to bottom and the first category which matches with the incident is chosen (first match basis).

Warning: This table is an extract of the *PRO303 - Incident Categories*

[2]Hours included in a business day.

Bureaux: 50, rue du Château
L-6961 Senningen
Adresse postale: B.P. 11
L-6905 Niederanven
Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964
http://www.govcert.lu
info@govcert.etat.lu

Category	Name	Description	Reporting Timeframe	
			Critical system	Non critical system
CAT 1	Compromised information	Successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.	Within one (1) hour of discovery/detection.	Within four (4) hours of discovery/detection.
CAT 2	Compromised Asset	Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.	Within one (1) hour of discovery/detection.	Within one (1) hour of discovery/detection.
CAT 3	Unauthorised Access	In this category an individual (internal or external) gains logical or physical access without permission to a national or local network, system, application, data, or other resource.	Within one (1) hour of discovery/detection.	Within four (4) hours of discovery/detection.
CAT 4	Malicious Code	Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Organisations are NOT required to report malicious logic that has been successfully quarantined by antivirus (AV) software.	Within one (1) hour of discovery/detection if widespread across organisation otherwise one (1) day.	Within four (4) hours of discovery/detection if widespread across organisation otherwise one (1) day.
CAT 5	(Distributed) Denial of Service	An attack that successfully prevents or impairs the normal authorised functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the organisation is unable to successfully mitigate activity.	Within four (4) hours of discovery/detection if the successful attack is still ongoing and the organisation is unable to successfully mitigate activity.

Bureaux: 50, rue du Château
L-6961 Senningen
Adresse postale: B.P. 11
L-6905 Niederanven
Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964
http://www.govcert.lu
info@govcert.etat.lu

Category	Name	Description	Reporting Timeframe	
			Critical system	Non critical system
CAT 6	Theft or Loss	Theft or loss of sensitive equipment (Laptop, hard disk, media etc.) of organisation.	Within one (1) day of discovery/detection.	Within one (1) week of discovery/detection.
CAT 7	Phishing	Use of fraudulent computer network technology to entice organisation's users to divulge important information, such as obtaining users' bank account details and credentials by deceptive emails or fraudulent web site	Within four (4) hours of discovery/detection.	Within one (1) day of discovery/detection.
CAT 8	Unlawful activity	Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.	Within six (6) hours of discovery/detection.	Within one (1) day of discovery/detection.
CAT 9	Scans/Probes/ Attempted Access	This category includes any activity that seeks to access or identify an organisation computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Within one (1) hour of discovery/detection.	Within two (2) weeks of discovery/detection.
CAT 10	Policy Violations	Deliberate violation of Infosec policy such as: - Inappropriate use of corporate asset such as computer, network, or application. - Unauthorised escalation of privileges or deliberate attempt to subvert access controls.	Within six (6) hours of discovery/detection.	Within one (1) week of discovery/detection.

Table 3: Information Security Incident Categories

7 Disclosure Policy

All information addressed to GOVCERT.LU is processed in accordance with the Disclosure Policy (*POL204 - Information Disclosure Policy*) of GOVCERT.LU documented on the website of GOVCERT.LU (http://www.govcert.lu).

Bureaux: 50, rue du Château
L-6961 Senningen
Adresse postale: B.P. 11
L-6905 Niederanven
Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964
http://www.govcert.lu
info@govcert.etat.lu

8 Annexe

List of Documents Created for this Procedure	
FRM702.301	Incident Reporting Form (.DOCX and .TXT)

Table 4: List of the Documents Created for this Procedure

Bureaux: 50, rue du Château
L-6961 Senningen
Adresse postale: B.P. 11
L-6905 Niederanven
Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964
http://www.govcert.lu
info@govcert.etat.lu