GOVCERT.lu

Constituency building via essential services

Eric ROMANG

2021-10-14

TLP:WHITE

Table of Contents

GOVCERT.lu | CERT gouvernemental Luxembourg

By Grand-Ducal decree of 9 May 2018.

For state administrations and services:

- **Single point of contact** for significant incidents;
- Provide **watch**, **detection**, **alert** and **reaction** services;
- Operate an **intervention team** taking charge of **prevention** and to **response** to incidents;
- Ensure the function of **National** and of **Military CERT**;

By Grand-Ducal decree of 9 May 2018.

- **National official point of contact** for national CSIRTs and foreign governements;
- **National official point of contact** for the collection and distribution of information relating to security incidents;
- **Relay of information** to sectoral CSIRTs or directly to the victim;

By Grand-Ducal decree of 9 May 2018.

The Governmental CERT is authorized, **subject to their agreement**,to extend its field of activity to other public institutions and authorities, **public entities** and **critical infrastructures**.

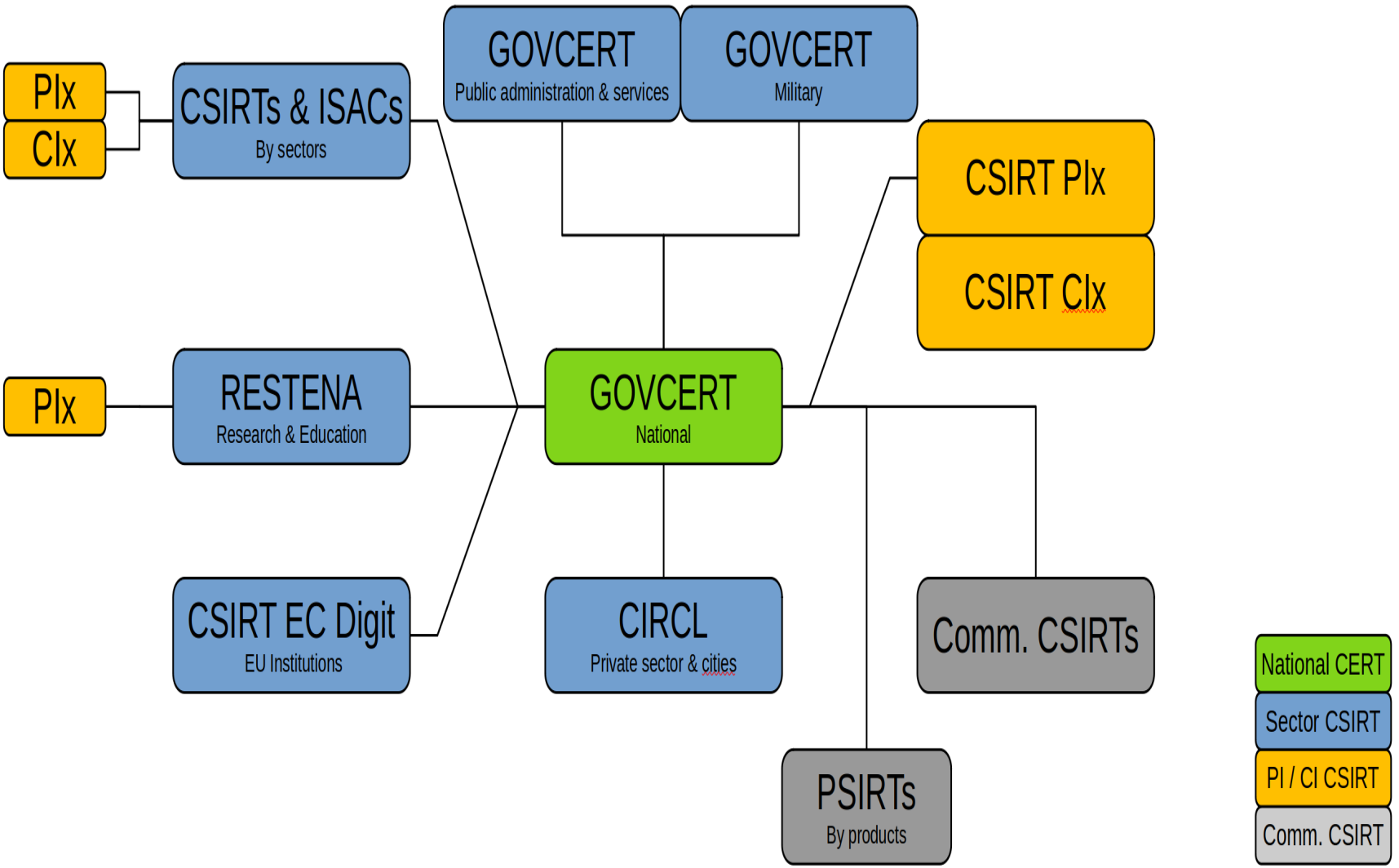
The bill **7670** will repeal the GDD, with no significant changes.

Table of Contents

GOVCERT.lu | CERT gouvernemental Luxembourg

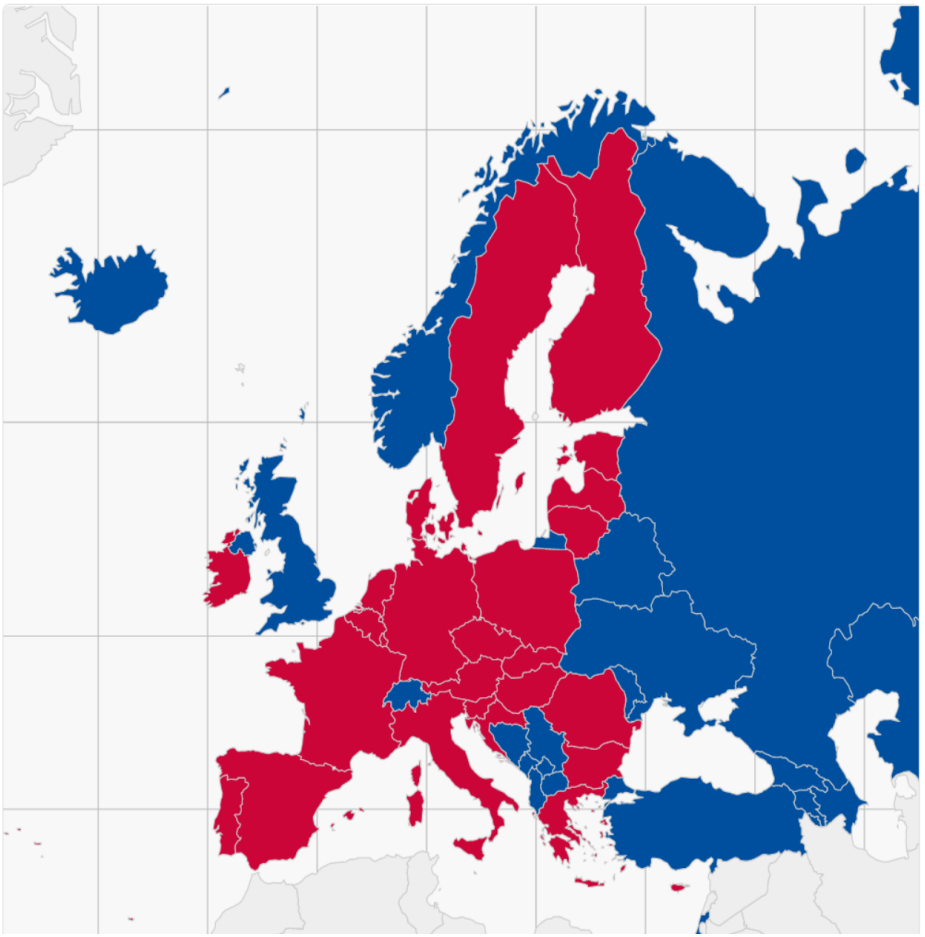
National CSIRT Network

GOVCERT.lu | CERT gouvernemental Luxembourg



European & International network

GOVCERT.lu | CERT gouvernemental Luxembourg



CSIRTs NETWORK

- ***GOVCERT member of***
  - ***EU CSIRT Network***
  - ***Trusted Introducer (Accredited)***
- ***EU CSIRT Network***
  - ***Introduced by NIS Directive***
  - ***39 members***
- ***FIRST member (international)***

Table of Contents

The foreseen Grand-Ducal decree expansion of constituency is formalized through collaboration agreements.

These collaboration agreements resume:

- Subscribed services;
- Service level agreements;
- Roles and responsibilities;
- Information exchange modalities;

Table of Contents

GOVCERT currently offers various services to its constituents based on the "Security Incident Management Maturity Model" named **SIM3**.

GOVCERT is regularly audited and is certified.

SIM3 defines three precise processes:

- Incident prevention process;
- Incident detection process;
- Incident resolution process;

Table of Contents

March 2021 Hafnium incident:

- Multiples constituents had severe impacts;
- Intervention team deployed in parallel at multiple constituents;

Lessons learned, for certain cases

- Risks not visible to constituents;
- Inappropriate cyber hygiene and resource allocation;
- Inaccurate contact details;

GOVCERT response

- Align constituency cyber posture with essential services;
- Collect and maintain accurate constituency contact details;

GOVCERT direct constituency is composed of:

- Luxembourg State civil service: 31.000 agents
- 64 public entities: 27.000 employees
  - 29 small (10 to 49 employees)
  - 17 medium (50 to 249 employees)
  - 18 large ($>$ 250 employees)
- And critical infrastructures operators

Table of Contents

Essential services are composed of:

- Vulnerability detection;
- Security alerts;
- Support request;

Table of Contents

Vulnerability detection

Vulnerability notification:

- Surveillance of defined product vulnerabilities;
- For defined vulnerability levels;

Vulnerability analysis:

- Vulnerability scan at defined frequency;
- On constituent internet facing services;

Results, constituents discover exposed on Internet

- unknown products;
- unknown critical vulnerabilities;

Table of Contents

- Security alert **for relevant critical vulnerability exploited in the wild**;
- Security alert **for constituent detected as compromised**;
- Security alert **for leaked information detection**;
- Security alert **for event of interest to the entire constituency**;

Results, constituents discover

- Compromised computers in their network, compromised employees personal and providers computers;
- Unknown credentials data leaks

Table of Contents

Support request

GOVCERT can support its constituency, in its capacities and means, when doubt or analysis is necessary on specific events (example: suspicious e-mail or document, suspicion of intrusion).

Table of Contents

Thank you

Thank you for your participation to Cyberday

GOVCERT.lu | CERT gouvernemental Luxembourg

Comments or questions ?