GOVCERT.lu

NIS, OES, CI and beyond

Paul RHEIN

2022-05-11

TLP:WHITE

Table of Contents

- Grand-Ducal decree of 9 May 2018
  - **Governemental CERT** function and missions;
  - **National CERT** function and missions;
  - **Military CERT** function and missions;
- Law of May 28, 2019 (NIS transposition);
- Law of December 17, 2021 (European electronic communications code);
- Law of July 23, 2016 (High Commission for National Protection);
- ERP Cyber;

GOVCERT.LU is **not regulator** and **nor operator**, only entitled to emit **recommendations** to its constituency.

- **Bill 7670** repealing the Grand-Ducal decree, functions and missions integrated into HCPN law;
- **NIS2** and **resilience of critical entities** directives proposals;
  - Roles & responsabilities clarified between the two directives;

- July 2011: Council of Government create GOVCERT.LU, attached to the CTIE;
- February 2015: Attached to the High Commission for National Protection;
- As of today: **21 FTEs**, 10 dedicated to incident response;

Historically GOVCERT.LU has an **intrinsic relation with the CTIE**, Luxembourg government IT provider, implementing in collaboration strong **defense in depth** and **protection of the perimeter** for ministries, administration and services of the State.

GOVCERT.LU services are based on **SIM3** processes

- **Incident prevention**;
- **Incident detection**;
- **Incident resolution**;

Service catalog composed of classical CERT services, including **penetration testing**, **anti-phising** campaigns and **exercises**.

Essential services have been specificaly developed for non CI and PE.

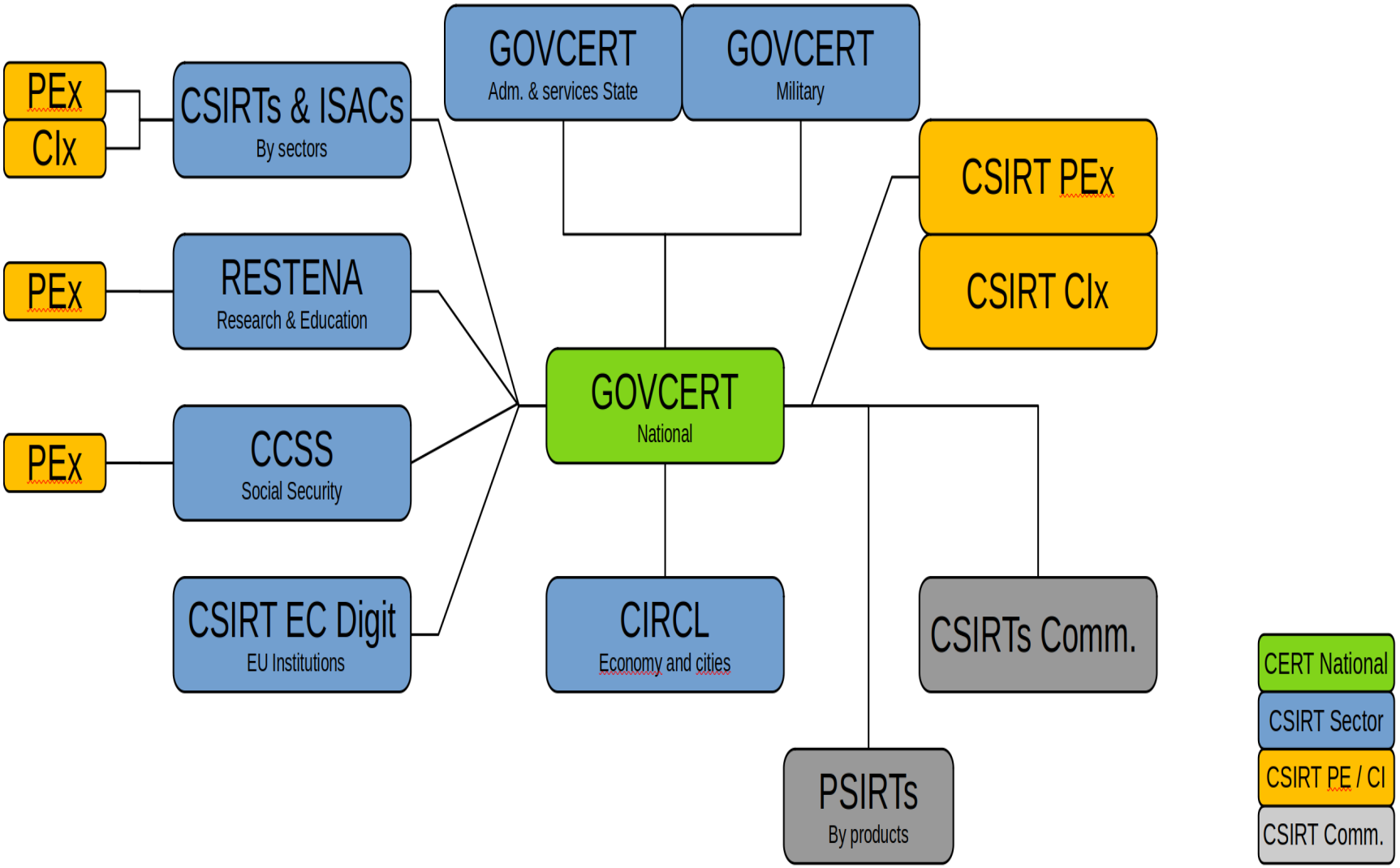
GOVCERT.LU constituency

- Civil service constituency: **31.000** agents;
- **63** public entities (on request): **27.000** employees;
  - 29 small (1 to 49 employees) - Fonds Kirchberg ...;
  - 17 medium (50 to 249 employees) - CAA ...;
  - 17 large ($>$ 250 employees) - CFL, POST ...;
- And critical infrastructures operators;

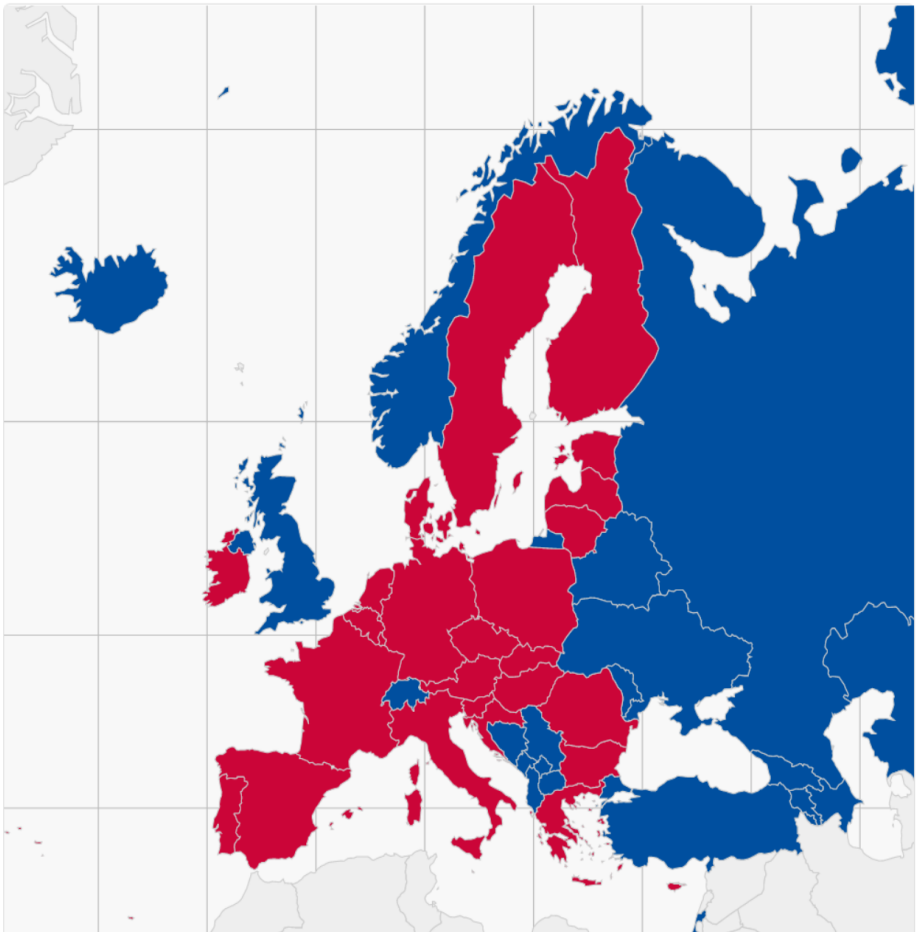
- **54%** of designated essential service operators are also critical infrastructure operators;
- **4** administrations are designated operators of essential services;
- **8** public entities are designated operators of essential services;

National CSIRT Network

GOVCERT.lu | CERT gouvernemental Luxembourg



European & International network



CSIRTs NETWORK

- ***GOVCERT membre de***
  - ***EU CSIRT Network***
  - ***Trusted Introducer (Accredited)***
- ***EU CSIRT Network***
  - ***Introduit par la Directive NIS***
  - ***39 membres***
- ***Membre FIRST (international)***

Table of Contents

March 2021 Hafnium incident:

- Multiples constituents severly impacted;
- 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 security posture with essential services;
- Collect and maintain accurate constituency contact details;

At national view level non-regulated entities represent the most incident cases impacting regulated entities.

Only for Q1 2022, around 50 luxembourg non-regulated entities had incidents impacting GOVCERT.LU constituency.

Regulated and non regulated entities are interdependent and share the same cyber space and certain cyber threats.

Essential services are composed of:

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

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;

- Security alert for **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**;

Results, constituents discover

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

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

Way forward

- **Human resources**;
- **Crypto**;
- **From "qualitative" to "quantitive"**;
- **From "Essential Services" to appropriate CS posture**;