CSIRT Lessons Learnt

Practical aspects of NIS implementation

CIRCL
Computer Incident
Response Center
Luxembourg

Team CIRCL

TLP:WHITE

info@circl.lu

2022-05-11 - NISDUC Conference

Co-financed by the European Union
Connecting Europe Facility

CIRCL

Computer Incident
Response Center
Luxembourg

- The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents.
- CIRCL is the CERT for the **private sector**, communes and non-governmental entities in Luxembourg.
- Under NIS regulation (duties defined in the law of 28 may 2019 defined in Mémorial A N^o 372 of the 31 May 2019).
- Leading the development of many **CSIRT tools** such as MISP, D4 Project, AIL, LookyLoo, Pandora.

Co-financed by the European Union
Connecting Europe Facility

Incident response evolution

Demands from the constituents

- In 2010, the scope was often evidence analysis, forensic analysis, **technical** data collection, malware reversing, log files analysis, DFIR tooling.
- Original main objective was to **Kick threat actor out and prevent similar attacks**.

Co-financed by the European Union
Connecting Europe Facility

Incident response evolution

Demands from the constituents

- Starting from 2016, an increase of requests from constituents regarding support for **reporting to authorities**.
  - Do I have to file a complaint?
  - What evidences do I need to file a complaint at law enforcement?
  - Do I have to report this to CNPD? Should I notify my customers?
  - How can I find out that personal data leaked?
  - To which other regulators I have to report this particular incident?
  - What are the thresholds for reporting of the regulator?

Co-financed by the European Union
Connecting Europe Facility

Technical evidences versus reporting requirements 1/5

Reporting impact on incident response

- The more reporting destinations are set, the **more technical evidence and analysis have to be conducted**.
- Reporting/**risk-based prioritization**: Fine of regulator might be higher than successive damages by threat actor(s).
- Rank regulators (national and international ones).
- False sense of security (threat actor remains in infrastructure).
  - **Focus on check box approach to satisfy reporting**.
  - Example: Are their log files → YES but the logs are incorrect the wrong date
  - No logs → no leak of personal data?

Co-financed by the European Union
Connecting Europe Facility

Technical evidences versus reporting requirements 2/5

Diversity of the reporting destinations

- Financial institutions and authorities;
- Insurrances;
- External private auditors doing audit on old incidents;
- Internal ones;
- Law enforcement;
- CNPD - National Data Protection Commission;
- CSSF - Surveillance du Secteur Financier;
- ILR - Institut Luxembourgeois De Régulation;
- HCPN - Haut Commissariat à la Protection Nationale;
- **Multiple others in case of international subsidiaries**;
- ...

Some incidents happen regularly and sometime from the same victims. Is reporting helping?

Co-financed by the European Union
Connecting Europe Facility

Technical evidences versus reporting requirements 3/5

Questions asked to satisfy the reporting forms

- **Number of users impacted** (from the law)
  - Count users in log files?
  - Search for initial infection.
- **Duration of the incident** (from the law)
  - The deeper you investigate, the longer gets the investigation.
  - Example: Exchange server compromised 64 times during 2 years by multiple threat actors.
- What was the **nature of the incident**? human error, hardware, software, procedure error
  - Pick them all in 64 times compromised Exchange server?
- **Geographic impact of the incidents** (from the law)
  - Impact and collateral damages are difficult to evaluate. (e.g. compromised infrastructure can be part of a more complex threat-actor model)
- **Intensity of service disruption**? (from the law)
- **Impact on economic and social functions**? (from the law)

Technical evidences versus reporting requirements 4/5

Questions asked to satisfy the reporting forms cont.

- Was personal data involved?
- Which personal data was leaked?
- Beginning of the breach.
- National or international interconnections.
- Description of technical measures in place.
- ...

Forensic analysis procedure should support to answer the reporting questions

Co-financed by the European Union
Connecting Europe Facility

Technical evidences versus reporting requirements 5/5

Example: Compromised Exchange of PSF telecom operator

- **Who to notify**: CNPD, ILR, CSSF,...
- Who should be notified first?
- Which **evidences must be collected**?
- Initial infection?
- Extraction of tickets from the victim (PSF telecom operator) to facilitate **metrics reporting**:
  - Count impacted users.
  - Review for personal data.
  - Do geographic classification of leaked tickets.
  - Review tickets for interconnections with other systems.
  - Compute the intensity of the incident.
  - ...
- Do you want to look if attacker did lateral movement?
- The cycle must be done again for each breach or compromised infrastructure?

Co-financed by the European Union
Connecting Europe Facility

The discrepancy of maturity in ICT services 1/3

Real answers received from suppliers handing ICT infrastructure

- Switch-off of MFA as technical measure.
- Do not apply patches as technical measure.
  - Loss of compliance of industrial, medical devices;
  - No time for testing the patches;
  - No resources to make mandatory risk assessment, pentesting or tests;

The discrepancy of maturity in ICT services 2/3

Real answers received from suppliers handing ICT infrastructure

- Apply patches only 4 times a year as technical measure or due to contractual reasons.
- Disable packet filtering as technical measure on industrial control systems:
  - On-call operators or suppliers cannot connect remotely from their networks any more
- Disable logs, do not read logs $\rightarrow$ the less you detect the less you have to report.

The discrepancy of maturity in ICT services 3/3

Real answers received from suppliers handing ICT infrastructure

- Logs are from the wrong day $\rightarrow$ no evidence of lateral movement.
- Only keep backups on online servers, because it's easier to manage.
- CERT asks if forensics report was done and a report from an AV scan was sent by the supplier.
- CERT informs about a compromised server due to a missing patch and supplier answers "Now patched, all good".
- CERT tells that a compromised patched server is still a compromised server and receive a report from an AV scan.

Heterogenity of reporting formats 1/2

- CSSF has XLS[1]
- PSD2 has some structured format with codes[2]
- CNPD has DOCX[3]
- IRL has PDF[4]
- GovCERT has FRM 702 in Text and DOCX[5]

[1] https://www.cssf.lu/en/Document/major-incident-reporting-1/

[2] https://assets.ilr.lu/telecom/Documents/ILRLU-1461723625-87.pdf

[3] https://cnpd.public.lu/content/dam/cnpd/fr/formulaires/formulaire-cnpd-data-breach-notification-EN-V2.docx

[4] https://assets.ilr.lu/telecom/Documents/ILRLU-1461723625-87.pdf

[5] https://www.govcert.lu/docs/FRM702.301_Incident_Reporting_Form_(Public)_5.0.docx

Heterogenity of reporting formats 2/2

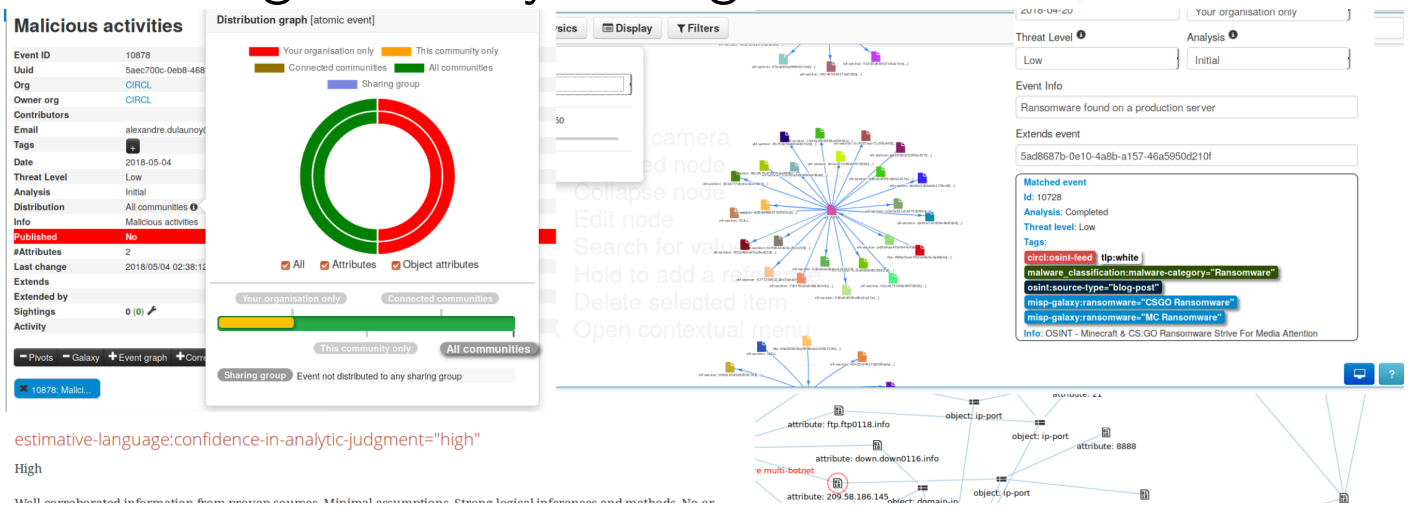
Challenges with unstructured formats

- How to **improve the reporting formats** and processes:
  - Structured and standard format;
  - Machine and human readable;
  - Automated correlation of values and reporting information;
  - Automated actions and workflow on report processing;

Co-financed by the European Union
Connecting Europe Facility

Reporting through MISP

- MISP is used among CSIRTs and other communities to structure information and **enable information sharing**;
- MISP standard format[6] allows the **creation of structured objects** and sharing efficiently among communities;



[6] https://www.misp-standard.org/

Conclusion

- Improving the mandatory reporting with the technical investigations;
- Better sharing of information to **combine metrics, investigation, impacts and technical reports**;
- Supporting victims of breaches or incident to understand the impact and use the experience to improve security;

Co-financed by the European Union
Connecting Europe Facility

Contact

- https://www.misp-project.org/
- https://www.circl.lu/

Co-financed by the European Union
Connecting Europe Facility