NISDUC parallel session - Banking and financial market infrastructure sector

Practical experience from CIRCL on sharing information

CIRCL
Computer Incident
Response Center
Luxembourg

CIRCL - *TLP:WHITE*

`info@circl.lu`

April 23, 2024

CIRCL - Computer Incident Response Center Luxembourg 1/2

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.
- CIRCL is regulated by NIS and NIS2.

CIRCL - Computer Incident Response Center Luxembourg 2/2

- CIRCL leads for several years the development of the following open-source projects
-
  - MISP https://misp-project.org
  - AIL https://ail-project.org/
- CIRCL operates more than 30 information sharing communities
- CIRCL is involved in the Generic Threat Landscape reports in the TIBER-EU framework[1]

[1] https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Guidance_for_Target_Threat_Intelligence_July_2020.pdf

Challenges in Incident Response Procedures (1/7)

The Clumsy Incident Response Procedures

- Regulatory requirements necessitate regulated entities to establish basic incident response capabilities.
- Incident Response Procedures are frequently established preemptively, prior to actual incidents occurring.
- Often, these procedures are devised by individuals lacking practical incident response experience.
- The initial response often involves creating reporting forms that must be completed by various teams.

Challenges in Incident Response Procedures (2/7)

The Clumsy Incident Response Procedures

- These forms often demand data that necessitates significant effort to generate.
- Friction commonly arises between involved teams, including incident responders, business continuity managers, and legal personnel.
- Misunderstandings are common due to differing professional backgrounds among team members.
- Agile incident responders can achieve faster reaction times.

Challenges in Incident Response Procedures (3/7)

High Workload Demands on Report Recipients

- Some information is quickly inserted into a reporting template without thorough analysis.
- Certain data requires extensive forensic analysis before completion.
- Incident response support is sometimes needed to assist entities in accessing requested information.
- Examples include geographic impact assessment and the number of affected users.

Challenges in Incident Response Procedures (4/7)

High Workload Demands on Report Recipients

- Infrastructure may lack readiness to extract required information.
- Teams may lack the technical ability to extract necessary data.
- Information requested in reporting forms can influence operational infrastructure design and policies.
- For instance, implementing additional logging with the related compliance activities.
- The usefulness of information requested in forms should be continuously evaluated.

Challenges in Incident Response Procedures (5/7)

The Curse of Detection

- Early information sharing during incident response has been proven effective in disrupting attacking activities.
- Threat actors cannot reuse the same techniques they used on other victims.
- The better the quality of threat intelligence, the more you detect.
- The more you detect, the more you have to report.
- The higher the burden of reporting, the better get the creativity to avoid reporting.

Challenges in Incident Response Procedures (6/7)

The Curse of Detection - The Story of Phishing Reporting

- Some regulated entities by CSSF (financial regulator in Luxembourg) reported phishing attacks.
- Some entities reported all kinds of phishing attempts such as dozens of attempts per day.
- There was a circular CSSF 11/504 11/504[2] addressed from the regulator to all the establishments subject to the supervision of the CSSF.

Excerpt

"It should be borne in mind that 'phishing' attacks are excluded from the perimeter and shall therefore not be reported."

[2] https://www.cssf.lu/wp-content/uploads/cssf11_504eng.pdf

Challenges in Incident Response Procedures (7/7)

The Curse of Detection - The Story of Phishing Reporting

- During incident response the origin of the incident that lead to the compromision of the infrastructure was a spear-phishing email.
- It was a targeted form of phishing.
- The attackers customize their deceptive emails to specific individuals in specific organizations.
- They included personal information to increase the likelihood of success and succeeded.
- So it is a phishing attack that does not have to be reported according circular 11/504.

Feedback on Experience of Information Sharing (1/11)

Why do we doing all of this?

- **Main goal**: Make our own lives and the lives of our constituency easier
  - Our central tool for ingesting, storing and disseminating information...
  - ...as well as to interact with organisations
  - By solving issues of other communities, we already have them prepared for information sharing with us when needed
- **Secondary**: Democratise threat intelligence for all
- **Stretch goal**: Build a full open-source tool-chain for CSIRTs / SoCs / etc
- By having useful reporting with actionable data
- By having a more complete Generic Threat Landscape Report in the TIBER-EU framework

Feedback on Experience of Information Sharing (2/11)

Tracing the Origins of Information Sharing

- During a malware analysis workgroup in 2012, we discovered that we worked on the analysis of the same malware.
- We wanted to share information in an easy and automated way **to avoid duplication of work**.
- Christophe Vandeplas (then working at the CERT for the Belgian MoD) showed us his work on a platform that later became MISP.
- A first version of the MISP Platform was used by the MALWG and **the increasing feedback of users** helped us to build an improved platform.
- MISP is now **a community-driven development** supporting different intelligence communities.

Feedback on Experience of Information Sharing (3/11)

Information Sharing Communities

- Communities are groups of users sharing within a set of common objectives/values.
- CIRCL operates multiple MISP instances with a significant user base (more than 2k organizations with close to 5k users).
- **Trust groups** running MISP communities in island mode (air gapped system) or partially connected mode.
- **Financial sector** (banks, ISACs, payment processing organizations) use MISP as a sharing mechanism.
- **Military and international organizations** (NATO, military CSIRTs, n/g CERTs,...).
- **Security vendors** running their own communities.
- **Sectorial communities** Telcoes, ISPs, Medical, ATF, ...
- **Topical communities** set up to tackle individual specific issues (disinformation, SIGINT, COVID-19, ...)

Feedback on Experience of Information Sharing (4/11)

Information Sharing based on practical user feedback

- There are many different types of users of an information sharing platform like MISP:
  - **Malware reversers** willing to share indicators of analysis with respective colleagues.
  - **Security analysts** searching, validating and using indicators in operational security.
  - **Intelligence analysts** gathering information about specific adversary groups.
  - **Law-enforcement** relying on indicators to support or bootstrap their DFIR cases.
  - **Risk analysis teams** willing to know about the new threats, likelyhood and occurences.
  - **Fraud analysts** willing to share financial indicators to detect financial frauds.
  - **Military** sharing highly specialised information.

Feedback on Experience of Information Sharing (5/11)

Many objectives from different user-groups

- Sharing indicators for a **detection** matter.
  - 'Do I have infected systems in my infrastructure or the ones I operate?'
- Sharing indicators to **block**.
  - 'I use these attributes to block, sinkhole or divert traffic.'
- Sharing indicators to **perform intelligence**.
  - 'Gathering information about campaigns and attacks. Are they related? Who is targeting me? Who are the adversaries?'
- → These objectives can be conflicting (e.g. False-positives have different impacts)

Feedback on Experience of Information Sharing (6/11)

Sharing Difficulties

- Sharing difficulties are not really technical issues but often it's a matter of **social interactions** (e.g. **trust**).
- Legal restriction[3]
  - ○ "Our legal framework doesn't allow us to share information."
  - ○ "Risk of information-leak is too high and it's too risky for our organization or partners."
- Practical restriction
  - ○ "We don't have information to share."
  - ○ "We don't have time to process or contribute indicators."
  - ○ "Our model of classification doesn't fit your model."
  - ○ "Tools for sharing information are tied to a specific format, we use a different one."

[3] `https://www.misp-project.org/compliance/`

Feedback on Experience of Information Sharing (7/11)

Addressing Sharing Difficulties

- Provide technical safeguards to avoid information leaks.
- Provide easy-to-use tools to reduce the time required to share information.
- Provide simple ways to contribute taxonomies.
- Be open to multiple formats.

Feedback on Experience of Information Sharing (8/11)

Addressing Sharing Difficulties

- Provide ready-to-use legal and compliance templates.
- Share best practices on how these issues have been addressed in practice.
- Utilize open-source methodology to generate these legal and compliance templates.
- Examples include GDPR and NIS.
- Available on the MISP Compliance GitHub repository. There are 18 forks and contributions of 5 organizations.
- `https://www.misp-project.org/compliance/`

Feedback on Experience of Information Sharing (9/11)

Addressing Sharing Difficulties

- The sharing communities that works best are those that are less regulated
- Ranking of information sharing agreements
  - Gentlemen's agreement
  - MoU
  - Code of conduct
  - NDA
  - Subscriber agreement

Feedback on Experience of Information Sharing (10/11)

Legal restrictions: Benefits of DORA

Art. 45(2) - Information sharing arrangements

For the purpose of Art. 45(1)(c), the information sharing arrangements shall define the conditions for participation and, where appropriate, shall set out the details on the involvement of public authorities and the capacity in which the latter may be associated to the information-sharing arrangements, on the involvement of ICT third-party service providers, and on operational elements, including the use of dedicated IT platforms.

Feedback on Experience of Information Sharing (11/11)

Legal restrictions: Benefits of DORA

- It enables sharing information in organizations where a regulatory framework is required.
- It enables structuring information sharing, such as the usage of common taxonomies.
- It enables automating information sharing on dedicated platforms such as MISP.
- `https://www.misp-project.org/`
- `https://github.com/MISP/misp-taxonomies`