FIRST Contribution to the IGF Best Practices Forum on Cybersecurity
Submitted Sunday, August 28th 2016

About FIRST

FIRST is an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs. At the time of writing, FIRST has 359 member teams in 77 countries. Its goal is to promote cooperation and information-sharing among computer security incident response teams through events, training and education, and working groups. For more information, visit https://www.first.org.

About this contribution

This contribution aims to share some of the experiences FIRST has had in convening the CSIRT community. It is mostly focused on how the CSIRT community cooperates internally, but we hope our learnings can contribute to identifying appropriate strategies for cooperation between different stakeholder groups.

This document does not constitute an official opinion of FIRST, nor a consensus agreement between its members. It aims to express the experience of a number of practitioners from the wider FIRST community that wished to contribute. In addition, it also includes a separate contribution by a FIRST member, CIRCL.

Methods of enhancing cooperation and collaboration

FIRST sees three high level areas of work ahead in ensuring CSIRT can cooperate more effectively both within their community, and beyond:

- **Responding CSIRTs must be able to contact the partners they need to mitigate an attack.** By themselves, CSIRTs, especially when they coordinate for more than a single constituent, do not always control computers and networks involved;
- When working with another team on an incident, both organizations must **speak the same operational language** and **have accurate expectations on the use of the information** provided.
- The community has the **tools and techniques to enable automated information sharing**. Analysts can focus on leveraging the information to truly understand the ramifications of the incident and make the right choices to reduce risk while mitigating the attack

FIRST has invested in expanding the options of CSIRT when reaching out within their community. As an example, FIRST has initiated the Fellowship program, to allow new CSIRT with less financial capability to

successfully join the community. In addition, FIRST has historically organized training, both developed by its partners and by itself, to ensure CSIRTs have a similar understanding of the issues at hand.

Finally, FIRST has convened its community to determine and publish a "CSIRT Services Framework" in the six official UN languages, which introduces a common understanding of the individual services offered by CSIRT teams.

Within its community, FIRST members have launched a number of working groups to standardize information exchange, focused on **Vulnerability Coordination**, the **Traffic Light Protocol**, and an **Information Exchange Policy (IEP)**. FIRST also maintains the **Common Vulnerability Scoring System (CVSS)**, which allows organizations to uniformly describe the impact of software vulnerabilities. While FIRST does not develop tooling for automated information exchange, our members leverage these standards in the development of their own tools.

There is an opportunity for the implementation of a similar approach between CSIRT and other stakeholders in the cyber security space. For instance, there are opportunities to train leaders in the internet community who may not be security experts, on the issues and role of incident response teams, or how to best benefit from their work. In recent years, FIRST has contributed to the Internet Governance Forum and other governance efforts to create more awareness of the CSIRT community, its role and services. Other parties have also published guidance on the CSIRT community focused on other stakeholder groups, such as the Global Public Policy Institute and New America Foundation. Focused CSIRT assisting very specific groups, such as Access Now, have also exposed incident response capability to previously unserved audiences.

Identifying the right partner for cooperation

Within our community, FIRST has long maintained its member database, a public resource for individuals to find a CSIRT and the constituency they are authoritative for. In 2015, FIRST opened up this data set through a well-structured Application Programming Interface. Network operators can leverage this tool to, in an automated manner, establish who to report a security incident to. FIRST is actively working with peer organizations in the community to extend the database beyond FIRST membership.

A well understood issue is that not every network is covered by a CSIRT. It is important for countries to support or establish a "CSIRT of last resort", which is willing to help coordinate across cultural and language barriers even if it has no official authority over the network in question to help address these gaps.

Corporations and software vendors which develop products have also increasingly stood up Product Security Incident Response Teams (PSIRT). These are increasingly part of the CSIRT community, and have a valuable role to play as the security response experts on the respective products they produce, which are increasingly becoming connected.

Common problem areas in enhancing cooperation and collaboration

For CSIRTs to effectively work with each other, or other peers within the community, trust is a crucial requirement. Trust is typically not established through legal agreements, but through a history of working with each other. This work contributes to building trust in at least two ways:

- **It ensures both organizations have an accurate understanding of the actions the other organization will take.** For instance, when indicators of a security incident are provided, a CSIRT can trust the information will be used to remediate the source of the incident, rather than purely for investigative or intelligence purposes, which may not assist the CSIRT in mitigating the incident.
- **It ensures organizations have an understanding of the effectiveness and capability of the other CSIRT**. If multiple reports have not led to successful remediation, or led to action which was counterproductive (for instance simply taking down malicious content, which continues to reappear, rather than addressing the issue comprehensively), a CSIRT may be less inclined to share information in the future. At the very least, it will need to check that both parties have a common understanding of the incident response services being offered and provided.

Maturity and trust help avoid these misunderstandings. Problems can often arise when there is no CSIRT present, but the incident response role is performed on an ad-hoc basis. For instance, in the product security world, organizations may react defensively, or even threaten legal action, when a security vulnerability is reported, rather than implementing and executing on known vulnerability coordination steps, such as defined by ISO 29147:2014. Building incident response maturity helps address and prevent these issues.

In our experience, developing trust is easiest when the objectives of both organizations align. When both organizations have as goal to remediate the incident and restore operations, they both see value in the information exchange. Trust does not develop when one or both organizations are perceived as having a different goal, an issue which sometimes appears when a CSIRT is established within a law enforcement or intelligence agency.

Typical communication mechanisms

The communications mechanisms used by CSIRT to interact with their constituency and peers are diverse. Most CSIRT communications involve notifying others of problems or vulnerabilities: asking others to disclose information about perpetrators is a role for law enforcement agencies. Law enforcement reduces the number of criminals: CSIRTs reduce the opportunities for committing crimes. Below we are referencing a small set of messages that are in use by the CSIRT community:

- Standardized protocols, such as the Network Abuse Reporting framework **X-ARF** are used by the community to report abuse originating from a particular network. Participants in the incident response community can develop X-ARF messages to flag a particular host as emanating malicious traffic, and send these reports for automated or semi-automated processing by the network owner;
- Within the CSIRT community, several tools are in use to collect, assess and redistribute information to the correct stakeholders. Examples include **AbuseHelper**, which allows automated processing of incident notifications, and the **Malware Information Sharing Platform (MISP)** which allows automated exchange of incident indicators.
- **E-mail** is still a common method for reporting security incidents. A CSIRT may both receive messages from other network owners or data sources on events that originate or occur within its constituency (e.g. compromised web sites, phishing, or a malicious host scanning another network), or may send them (e.g. notifications of a phishing site that affected a constituent).

Confidentiality of information is typically important, especially when working with a stakeholder that is in the process of mitigating a security incident. Early knowledge of such an incident by either the adversary, or others could make an effective response more difficult. Within the community, standardized protocols such as Transport Layer Security (TLS) are most often used for automated tooling, and Pretty Good Privacy (PGP) is the de facto standard for e-mail communication.

As a community, automating information exchange where possible, and ensuring CSIRT's ability to process information at an increasing pace is extremely important. CSIRT can often be resource constrained in terms of qualified analysts, and allowing them to focus on harder problems that require expert review is critical.

However, it is important to clarify that prior to any automated exchange taking place, it is crucial for stakeholders to set expectations around how the data will be used. Sharing indicators may not be helpful if they are not used correctly, or are used for different purposes than intended. While there are typically many technical means of addressing a security incident, it is most important that goals are aligned and expectations are clearly set.

Several members of the wider incident response community have built specific partnerships and programs to enable them to work effectively with other parties on similar problems. Examples of these are well described in Proactive detection of Network Security Incidents, published by the European Network and Information Security Agency.

Contributors:

Andrew Cormack, **Jisc**
Adli Wahid, **FIRST**

Cristine Hoepers, **CERT.br/NIC.br**
Maarten Van Horenbeeck, **FIRST**
Serge Droz, **FIRST**

Appendix A: Contribution by Computer Incident Response Center Luxembourg

Courtesy of Pascal Steichen of CIRCL

CIRCL (Computer Incident Response Center Luxembourg) is a government-driven initiative designed to gather, review and respond to computer security threats and incidents. It's the CERT for the private sector, communes and non-governmental entities in Luxembourg.

CIRCL is operated by SECURITYMADEIN.LU, which has even broader missions in the area of cybersecurity, from awareness raising, both via national campaigns as well as by dedicated sessions with specific target audiences (children, youth, elderly people, etc.) (e.g. https://silversurfer.lu/); via organisational security through the federation of risk management methodologies and other information security governance tools (e.g. MONARC - https://www.cases.lu/index-quick.php?dims_op=doc_file_download&docfile_md5id=56ee6ff569a40a5b52bed0e526a6a77f); up to fostering the cybersecurity ecosystem in Luxembourg, mainly by promoting information sharing, collaboration and co-operation among stakeholders (e.g. https://securitymadein.lu/cybersecurity-breakfast/).

The set-up of SECURITYMADEIN.LU, 6 years ago, with its three-fold mission, covering behavioural, organisational and technical aspects of cybersecurity, has become the de facto centre of excellence in this area for Luxembourg. Communication-wise, the different stakeholders are addressed in a regular fashion, via press and media coverage (e.g. http://www.itnation.lu/62000-cyberattaques-au-luxembourg/), awareness campaigns (e.g. https://www.bee-secure.lu/fr/outils/campagnes/clever-cloud-user), conferences (e.g. https://2016.hack.lu/) and training (e.g. https://circl.lu/services/misp-training-materials/).

Over 4 years of experience in malware and threat sharing, via MISP (https://circl.lu/services/misp-malware-information-sharing-platform/) shows that co-operation and collaboration is key in cybersecurity, not only to avoid duplicate work and analysis, but also in respect to less mature entities, being able to profit from the experience and expertise of others and as such develop faster thereafter. MISP brings together specialists from different areas, like malware reversers, security analysts, intelligence analysts, law enforcement, risk managers and banking fraud analysts. Legal restrictions, like law enforcement frameworks, but also practical issues, high risk of information leakage, a "nothing- to-share" mentality or alike are difficulties that we encountered.

Nonetheless SECURITYMADEIN.LU continues its investment, development and promotion of MISP as well as MONARC, because we believe in the "sharing is caring" principle and especially focus on bringing together specialists with different competences and knowledge.

A nice example is the "committee C", as we call it, which is a regular meeting of the local CERT community, law enforcement, attorneys and judges as well as intelligence people to exchange on relevant information and co-operate on common cases.

At the level of organisational Cybersecurity, risk management has become the main driver, not only because the European legislator has seen its usefulness and integrated aspects of risk-based approaches in recent directives (e.g. NIS directive) and regulations (e.g. GDPR), but also businesses need to get better knowledge and grasp on their risks. MONARC builds on this and especially focuses on providing a solution to empower SMEs with efficient tools and access to the expertise needed, by reducing the time for a risk analysis by up to 80%. These figures were achieved in the area of local government and municipalities in Luxembourg, due to extreme overlapping needs and procedures. Currently other sectors are being addressed with this same mutualisation scheme to achieve similar efficiency.

Tools, platforms and other technological "helpers" are often modelling how people and organisations work together. Especially in cybersecurity, tools are critical to conduct incident response, make information sharing easy and enhance proactive notification. All these tasks involve huge volumes of data and can only be efficient with performing and adequate tools. When designed and operated by the "user community" itself, tools tend to better support the work of the community and especially security-wise do a proper job.

Our two main platforms, MISP and MONARC, needed improvements in many different areas and by reducing the development cycle, the communities could benefit from their feedback in a timely fashion. Tools, if heavily used and appreciated by the communities, can even influence the legal framework or highlight current limitations of a specific regulation.

Something else that we have seen in our past experiences is the importance in the distribution of the tools. Only those that are widely available and not restricted by complex confidentiality agreements, have succeeded and got high acceptance of their user communities.

Beyond these considerations, guidelines to build a "culture of security" for economic and social prosperity are depicted nicely in the 2002 and 2015 OECD documents on security (please find them attached for your convenience). They are both still valid and give great insight for large-scale or national cybersecurity strategies.