Summary

GFCE Expert Meeting CSIRT Maturity, 12 June 2016, Seoul

Overview

On 12 June, representatives of the members of the Global Forum on Cyber Expertise came together in Seoul for the expert meeting on CSIRT Maturity. Among them were policy advisors, representatives of the private sector and academics. They represented inter alia EU Member States, United States, South-Korea, Japan, New-Zealand, ITU, FIRST, African tech community, IBM, Microsoft, Siemens and Cisco.

Outcomes and next steps

- Regarding the Adoption of the Cyber Maturity Kit:
  - Participants are requested to comment on the current draft before the end of July
  - Subsequently a final draft will be made available before the end of August
- Support within the GFCE will be further harmonized: who can support what and under what conditions
- Proposal baseline national/governmental CSIRTs will be ready by the end of year
- Proposal for toolbox to go with baseline will be ready by the end of year
- Next expert meeting will be organized end 2016 / early 2017

Opening and introduction on the GFCE CSIRT Maturity Initiative

By Prof. Dr. Klaus-Peter Kossakowski, HAW Hamburg & CEO DFN-CERT and Petra Nijenhuis-Timmers, Coordinating Policy Advisor, Ministry of Foreign Affairs of the Netherlands.

In the opening the importance of an open, free and secure digital domain was emphasized which will stimulate more democracy, freedom, innovation and social and economic growth. Besides that, capacity building is important because of the idea that there is a strong relation between internal and external security. Some countries have developed substantial cyber capacities, while in particular countries with fast developing economies, are increasingly dependent on the Internet but do not yet have the capabilities to defend themselves against cyber threats. Precisely by

increasing the level of cyber capacities in these countries, the potential disruption of cyber operations can be reduced. If you look at the technological developments and the pace with which the problems are spreading, the GFCE is of great importance to deal with these problems by sharing knowledge, experiences and good practices between different stakeholders within initiatives. The aim of the GFCE CSIRT Maturity initiative is to enhance the capacity of CSIRTs, which have a preventive function and can restore damage after a cyberattack. These services are vital for a safe and secure future of the Internet.

CSIRT Typology

By Maarten van Horenbeeck, FIRST boardmember.

CSIRTs come in different types: national, governmental, research & education, commercial teams in various sectors, IT service providers, etcetera. The typology currently most used grew organically over the past 25 years, and has some serious flaws. A good typology is important, because from various perspectives (e.g. political, maturity, financial) it indeed does matter what 'type' a CSIRT is. Hence it is important to jointly further define the various types of CSIRTS, which can enhance international cooperation for a secure future of the Internet.

The types of CSIRT proposed by Maarten van Horenbeeck were: product / enterprise / multi-party / regional / sectoral / national. This typology raised some questions among the participants regarding enterprise CSIRTs and national CSIRTs. It was argued that enterprise CSIRTs would not be the right name for teams that are responsible for incident management for a non-commercial entity. Furthermore, the definition of national CSIRTs was deemed to be insufficiently defined because even a governmental team would not clearly fit in the definition. To conclude, it would be helpful to further clarify these types of CSIRTs.

FIRST CSIRT Services Framework – state of affairs

By Peter Allor, FIRST Boardmember and Luc Dandurand, Head ICT Applications and Cybersecurity Division ITU.

First of all, Allor and Dandurand stressed the importance of having a clear picture of which services are provided by every CSIRT. Experience has shown that it is better, especially in the starting phase, to start with a small amount of services and focus on good performance.

An important part of the CSIRT best practices is that CSIRTs need to be very clear on what they do for their constituency, and what they do not. We refer to that as CSIRT services. PSIRTs are product security teams, similar to CSIRTs, but focused on improving the security of IT products. The CSIRT services framework has been developed by the global incident response community under the guidance of FIRST and seeks to provide a reference standard for both CSIRT and PSIRT services. Peter Allor, FIRST Board member, has been one of the drivers of this effort. He presented the current status and the challenges still to be solved.

As a result of the morning session about this framework, the CSIRT version is meant to be in a stable version. There will be a PSIRT version as a separate document later this year. The last review round for the CSIRT version has started now. Comments due end of June, rounding up end of July, if possible.
Another result of the morning session is the new preference to talk about *proficiency* instead of *maturity* where the maturity aspect of services is concerned. However, this topic is currently not in the framework and will be addressed no sooner than early 2017.
Furthermore, Peter stressed that in order to define good training programs, you first need to properly document proficiency and maturity. Others suggested that it is not always necessary because there are many topics than can be taught already and can be fitted in a framework later. Besides that, there will always be a clear need for basic CSIRT trainings and specific trainings on topics such as forensics, netflow, malware analysis and many more.

Furthermore, Luc Dandurand presented ITU's vision on the CSIRT services framework, which is part of the CSIRT Maturity framework but focuses more in depth on services. This CSIRT services framework will alongside the CSIRT Maturity Framework further being distributed inside the GFCE. In short, different types of CSIRTs will make a different selection from this collection of services, based on the needs of their constituency.

CSIRT best practices

By Don Stikvoort, Representative of the National Cyber Security Centre of the Netherlands.
The cyber threat landscape is constantly changing and the responsibility to prevent, detect and respond to incidents is ever more challenging. To remain effective and meet these challenges, we must focus on capacity building, assisting others and exchanging knowledge. This not only benefits an individual CSIRT, but also benefits the entire community: cyber security is a shared responsibility and requires joint effort. Therefore, to enhance CSIRT Maturity is an important element in capacity building.
During this session Don Stikvoort further elaborated on the CSIRT Maturity Kit. The CMK is developed in close cooperation with various representatives of the CSIRT community, inter alia from the US, EU, Japan, Brazil and the regional African CSIRT. It will be regularly updated and will focus inter alia on the legal base of CSIRTs, staff and organization structures (staff requirements, services of a CSIRT), tools (software/hardware) and the processes of incident response and detection. The purpose of the CMK is to help emerging and existing CSIRTs increase their maturity level. The CMK has a set of best practices embedded in a 5-tier framework based on the SIM3 CSIRT Maturity Model: Organization, Human, Tools, Processes and Foundation. This work has been reviewed by a global review committee of experts, and continues to be updated and improved.

Lastly, GFCE members expressed their appreciation for the CMK and would support the idea to further develop this. Besides that, GFCE members stated that more CSIRTs should be established, and especially for these CSIRTs it would be beneficial if a baseline is developed and a toolbox for CSIRTs in the starting phase.

CSIRT Measurement

By Serge Droz, Senior Security Adviser, SWITCH.

It is important to have a more objective approach towards maturity, also allowing comparisons and benchmarking in due course. During this session Serge Droz discussed the Security Incident Management Maturity Model with the participants. This model identifies 40+ parameters that measure categories of maturity: Organization, Human, Tools, Processes and Foundation.

Serge argues that SIM3 is an excellent measurement of CSIRT maturity, and is very useful for teams as it was for his team, twice. However, the question is how it could also cover things as agility, performance and efficiency. There seems to be agreement in the meeting that these topics are important, but very hard to quantify and measure.

Closing and next steps

By Petra Nijenhuis-Timmers, Coordinating Policy Advisor, Ministry of Foreign Affairs of the Netherlands.

The GFCE will serve as a facilitation platform for continuing the dialogue regarding the implementation of the best practices discussed and related capacity building efforts. Nation states are encouraged to submit offers of assistance and requests for assistance to the GFCE Secretariat. The initiators will, in cooperation with the GFCE Secretariat, share requests for and offers of assistance to the GFCE members on a timely and regular basis.