



CERT-FI

**National and Governmental
CSIRTs in Europe**

Study Conducted by CERT-FI

22 October 2009

Index

Executive Summary
More Detailed Findings
Discussion
About the Study

Executive Summary

In 2008, CERT-FI conducted a survey among selected group¹ of European national and governmental computer security incident response teams (CSIRT). The purpose of the study was to identify good practices in various aspects of the CSIRT functions and to help CERT-FI learn from them. The survey was first of its kind in Europe.

The main findings of the study were as follows:

Each CSIRT is unique

Each CSIRT has established its operations, organisation and legal mandate to meet the needs of the host organisation, home state and constituency. Despite the differences every national and governmental CSIRT has the same goal on its mind – to help keep its country's critical networks secure and clean.

A set of recommended capabilities for national and governmental CSIRTs were identified

There exist a set of functions and capabilities that every national and governmental CSIRT should meet in order for the country to fulfil its international and domestic responsibilities in the modern network-dependent society.

First, effective incident handling functions in the field of incident analysis and incident response coordination are absolutely essential for the success of any CSIRT. The CSIRT needs to have a clearly defined point of contact that interfaces the team with the outside world.

Second, the CSIRT should have an extensive contact network both nationally and internationally. Belonging to international CSIRT organisations (like the FIRST) helps facilitate the creation and maintenance of international CSIRT networks. Wide national contact network is essential in incident coordination especially for national CSIRTs.

Third, in addition to incident handling, other typical functions offered by the CSIRTs include information security situation monitoring services and awareness building efforts.

Governmental CSIRTs are funded by state

All governmental CSIRTs receive the majority of their funding from the state budget. Additional funding, if present, may come from sources such as service agreements, projects and various fees.

CERTs (Computer Emergency Response Teams) are responsible for collecting information about and coordinating the response to computer security incidents in a certain domain. In general settings the term CSIRT (Computer Security Incident Response Team) is preferred as CERT is a registered trademark of Carnegie Mellon University.

¹ Following teams took part in the survey: CERTA (France), CERT-Bund (Germany), CERT Estonia (Estonia), CERT-Hungary (Hungary), CERT-FI (Finland), CPNI/CSIRT-UK (UK), DK-CERT (Denmark), GovCERT.NL (The Netherlands), NorCERT (Norway), SITIC (Sweden) and SWITCH-CERT (Switzerland).

More Detailed Findings

Host organisation

Typically, national and governmental CSIRTs are governmental authorities embedded in varying agencies. Placement depends on the structure of public administration and government, history and political decisions.

Sometimes the host organisation has further responsibilities regarding network and information security. These responsibilities include, for example, production and administration of cryptographic services, evaluation of ICT systems, deploying information security policies for government and raising awareness among citizens and SMEs.

Legal basis and responsibilities

It is strongly recommended that CSIRT's tasks, duties and responsibilities have legal foundation such as an act, decree or government decision. This clarifies the mandate and gives boundaries for operations. Clear mandate also reduces competition among government branches.

Usually the responsibilities defined in the law include various duties on information security and CSIRT operations such as incident handling, analysis of threats and disseminating security-related information. The responsibilities may also include other tasks like participating in international cooperation, acting as a national point of contact or maintaining a situational picture on information security.

Customers

CSIRTs have a wide range of beneficiaries, but all teams covered in the study share one thing in common – they act as an information security incident reporting point of contact for their country. This means that they receive network and information security incidents and coordinate their handling between different organisations in their own countries.

The CSIRTs' customers are often divided into primary and secondary customers. Primary customers are the ones who receive extended services and usually fund the operations. For most of the teams, the main primary clientele

is the public administration. Other primary customers are operators of critical national infrastructure (CNI) and public sector-oriented companies.

Secondary customers either pay for the services per subscription or the services are provided free-of-charge, but in a best effort manner within the resources and time allowing. Citizens, municipalities and local governments are typically regarded as secondary customers.

International cooperation

International cooperation is a vital part of CSIRT activities. Information security incidents affect several actors in many countries, so it is extremely important that CSIRTs have contacts in foreign organisations either directly or via other international teams and forums.

Countries without a national CSIRT point of contact pose a major challenge to international cooperation. Even in Europe, there are countries that are considered to be difficult to contact due to their lack of a properly functioning CSIRT. This underlines the importance for a CSIRT to create a wide international contact network.

Funding

CSIRTs are funded either wholly from the state budget or state funding is combined with other funding sources like agreements and separate project funding. CSIRTs (or their host organisations) may also collect fees such as service and information security fees, which in some cases can be considered as tax-equivalent by nature.

Discussion

The study suggests that teams originally set up as governmental CSIRTs eventually end up adopting tasks that would normally be categorised to belong in a national CSIRTs' domain. What was remarkable is that the converse holds for teams originally established as national CSIRTs. This development is seen as part of a natural maturation process. In case the national and governmental CSIRTs operate as separate entities, their seamless cooperation is seen crucial. Unhealthy competition between the two CSIRTs (or more) leads to inefficiency and confusion in mandate and authority.

A national CSIRT is a trusted point of contact for a given country that its international counterparts and network managers can use to report incidents affecting or originating from the country. It needs to be a neutral and independent entity whose task is to operate in the benefit of its own country's citizens, industry and public administration in information security and critical network infrastructure matters. A national CSIRT acts as a representative for the above-mentioned parties and seldom assumes the ownership of the security incident it coordinates. National CSIRTs in general are more approachable by the private citizens and SMEs which makes them well suited for awareness building campaigns.

A governmental CSIRT, on the other hand, focuses on serving the public sector, often the central government and governmental institutions. The governmental CSIRT usually represents the owner of government ICT assets but generally has no authority over private sector organisations such as telecommunications operators or financial institutions.

As CSIRT authorities mature and the need for various approaches becomes evident, the focus of the existing CSIRT either expands or new CSIRTs are being established to fill the gap. This has been seen among the CSIRTs that took part in the study.

About the Study

The survey was carried out in form of personal interviews during the first half of 2008 and was finalised during the latter half of the year. The survey consisted of four topics: 1) organisation, 2) operations, 3) cooperation and 4) communications. The topics were further divided into twenty sub-topics.

The study was conducted by Mr. Harri Bryk who worked as a research consultant with Finnish Communications Regulatory Authority (FICORA). Mr. Bryk was embedded in CERT-FI over the duration of the project. He also produced a related report for the Helsinki University of Technology as part of his Master's Thesis.

Should you have any questions regarding this study, please send them to CERT (at) ficora.fi.