Report on 4th ENISA CERT Workshop

The role of CERT Teams in National Incident Response Plans

Marco Thorbruegge

Executive Summary

The annual ENISA Workshop CERTs in Europe took place on 29th of May 2008 in Athens. After having covered international cooperation among CERTs and other players in order to mitigate massive cyber attacks (like those against Estonia in 2007), this year's workshop focussed on cooperation among key players in NIS on a national, Member State level and the role national and/or governmental CERTs play in the national incident response plans.

The workshop had three main goals:

- Inform the Member States representatives about the plans and projects of the European Commission, ENISA and others in the field of resilience of public communication networks
- Support these programs by discussing them with the representatives from the Member States and retrieve valuable feedback
- Prepare a good practice guide on this topic for ENISA's work program 2009

Concerning the first two goals the workshop was quite successful, as fruitful discussions took place on both the programs run by ENISA and the European Commission.

The diversity of solutions chosen by the various EU Member States who presented their approaches during the workshop showed, though, that a generic good practice guide that contains good practice on cooperation on national level and national incident response plans suitable for all EU Member States is difficult if not impossible to achieve. A possible solution is to break down the topic into smaller parts and provide good practice for specific tasks. The suggestions made by DG INFSO concerning WPK2.2 in ENISAs Work Programme for 2009 outline a feasible approach to a good practice collection and will be further taken into account while formulating that work package.

Motivation

Since 2005 ENISA collected and shared good practice from various fields of CERT activities in the EU Member States and beyond. Especially the two good practice guides "A step-by-step approach for setting-up a CSIRT" and the report on "CERT cooperation and its further facilitation by relevant stakeholders" were successfully applied in Member States for the setting-up of their national/governmental CERT and its integration into the international CERT community. A "Basic collection of good practice on how to run a CSIRT" from 2007 helped the new teams to establish and improve their services after a successful establishment; this will be supplemented by a good practice guide on "CERT exercises" in 2008.

As much as the integration of new CERTs into the international CERT community is understood and successfully applied in practice, the field of cooperation on national level especially during the response to incidents is not widely explored and raises problems for some Member States. There already are very far developed Member States with a very well developed national cooperation structure, and so ENISA decided to invite them to this workshop, let them present their national solutions, share this information with the other Member States and, by doing this, examine the feasibility of compiling a good practice on this topic for 2009. In addition two speakers from Japan and the US were invited to complement the views of the presenting EU Member States.

Agenda

Session 1. Resilience of networks, broader view

- Security and resilience in the Information Society: the role of CERTs/ CSIRTs in the context of the EU CIIP policy (Andrea Glorioso, **EC**)
- Improving Resilience in European e-Communication networks (Evangelos Ouzounis, **ENISA**)
- Open Discussion, Q&A

Session 2. EU Member State National response plans

- UK Networks & Security: An overview (Andrew Powell, CPNI, **UK**)
- National response plans: IT-Crisis Response in Germany (Andre Vorbach, BSI , **Germany**)
- CERT role in Finnish Response Plan & The Finnish CI Protection; State Crisis Management Model and Situation Awareness (Erka Koivunen, CERT-FI & Timo Härkönen, Director of Government Security, **Finland**)
- Polish experiences in running a national level CSIRT Miroslaw Maj, NASK, **Poland**)
- Introduction of the Hungarian financial information sharing and analysis model (Ferenc Suba, CERT-Hungary, **Hungary**)
- CNPIC as coordination centre in Spain & The Spanish case (Miguel Ángel Abad, CNPIC & Joaquín Castillejo Blanco, TB-Security on behalf of CCN-CERT, **Spain**)
- Open Discussion, Q&A

Session 3. Experiences outside of Europe

- CSIRT Contributions to National Cyber Incident Response: An Architectural Perspective with U.S. Examples (Bradford Willke, CERT/CC, **USA**)
- Public and Private National Cyber Incident Response Plan in Japan (Yurie Ito, JPCERT/CC, **Japan**)
- Open Discussion, Q&A

Presentation from ENISA and the European Commission

The first session of the workshop was dedicated to the sharing of information from the European Commission and ENISA about projects in the field related to the topic of the workshop.

Presentation of the EC

The presentation from the European Commission, DG INFSO A3, outlined the CLWP 2008 Policy Initiative on CIIP. The overall approach towards a secure Information Society builds on three pillars: dialogue, partnership and empowerment, driven by an open and inclusive multi-stakeholder debate. The objective of the initiative is an enhancement of the level of CIIP preparedness in the Member States, building on national initiatives and engaging all relevant public stakeholders. The presenter gave a summary of activities carried out so far, and by giving an outlook to future activities emphasised the position of the European Commission, that CERTs/CSIRTs play a significant role in national and international cooperation and, by this, in the preparedness of their respective country to respond to cyber threats. The EC invited the audience to reflect and provide views/feedbacks on what roles CERTs - especially national/governmental ones - could play in strengthening the incident response capabilities of each Member State and of the European Union as a whole.
Additional information can be found in the proceedings.

Presentation from ENISA

The presentation from ENISA explained the Multi Annual Thematic Programme (MTP) about "Improving Resilience in European e-Communication Networks". The presenter outlined the overall approach and the three Work Packages related to this MTP. A stock-taking exercise about regulatory, marketing and technological measures in the EU Member States in 2008 will be followed up in 2009 by an analysis and the generation of good practice guidelines in resilience that finally will be promoted and put into pilot actions in 2010. Some of the challenges on the way mentioned in the presentation are for example the complexity of regulations and measures in the Member States, the diversity of requirements from different sectors and the variety of expectations from these sectors towards ENISA. To mitigate these challenges ENISA invites all interested stakeholders by a "Call for expression of interest" to be involved in the execution of the programme and, in a first step, to identify national authorities responsible for network resilience in the EU Member States.
Additional information can be found in the proceedings.

Examples from EU Member States

The speakers were asked to structure their presentation along the following topics:

- the structure of the public communication networks in the MS
- the threat landscape these networks face
- the key players in NIS that have been identified as crucial for the national response plan
- cooperation initiatives with these key players and how to get them involved
- the layout of the response plan(s) in preparation for cyber attacks and threats
- if possible a use-case where these plans were put to a test

Presentation from United Kingdom

The presentation from UK started by giving a market and a technological view on the communication networks that, besides regional distinctions, are also valid for other Member States: e-communication is a highly competitive market with a constant growing need to modernise technology. New technologies have to be introduced and existing NIS schemata must be adjusted accordingly. Among the threats the UK communication networks face terrorist attacks and crimes committed via or against the networks were mentioned. UK organises its national response capability by separating security from resilience. Two governmental/national CSIRTs are in place: GovCERTUK serves the government's own networks, while CSIRTUK coordinates incident managing affecting private sector networks. In addition there are incident response capabilities from various individual operators that are included in a regular national dialogue under auspices of CPNI. The cooperation is based on a voluntary model. UK teams are also very well established and active in the international CERT communities.
Additional information can be found in the proceedings.

Presentation from Germany

The presentation from Germany outlined the German national plan for infrastructure protection (NPSI), the role of the national/governmental "CERT Bund" and the very well established dialogue on national level with various other incident response capabilities within the national "CERT Verbund" (CERT alliance), that regularly brings together players from public administration, critical infrastructures, economy and research. The cooperation in that field follows a similar, voluntary model as in the UK. The national plan foresees three areas: prevention, preparedness and sustainability, with CERT Bund as the key player for public administration and as national point of contact. The action plan to put in place NPSI for CIIP is facilitated by four working groups dealing with crisis exercises, crisis response and management, maintenance of critical services and national and international cooperation. CERT Bund is also responsible for the operation of an NIS information sharing and alerting service for the citizens called "Buerger CERT".
Additional information can be found in the proceedings.

Presentations from Finland

The presentation from Finland was split into two parts with separate speakers. The first part described the Finnish national CERT, CERT-FI, while in the second part the Finnish critical infrastructure protection plan was outlined. CERT-FI acts as national point of contact for incident reports and provides 24/7/365 incident handling services for the whole country of Finland, with emphasis on telecommunications network operators, service providers and critical infrastructure. By this, Ficora and CERT-FI is a vital part in the national response planning. Among the tasks of the authority are the collection of

information on violations of and threats to information security in Finland and public awareness building in NIS matters. Communication to all NIS key players is established, and in some cases ISPs (and other operators) are obliged to report incidents by legislation. At the present moment the governmental IT functions largely rely on commercial network providers, that not all have their main seat in Finland.
Additional information can be found in the proceedings.

Presentation from Poland

The presentation from Poland was mainly focused on NASK and CERT Polska, the (at the moment) de-facto polish national CERT. NASK is the main network- and also NIS provider in Poland and has strong academic roots. CERT Polska, a sub-section of NASK, provides various kinds of security services (among others incident handling and a hotline to report illegal content) for the whole country of Poland, is very well connected with and integrated in the international CERT communities and active in a couple of European and international NIS projects. CERT Polska also organises the dialogue with other CERTs and operators in Poland, the cooperation here is again operating on a voluntary basis. Recently a dedicated polish governmental CERT was established, that is supported and trained by CERT Polska. CERT Polska also cooperates with law enforcement agencies in Poland. So Poland provides an example case (that is not so unusual in Europe) where the de-facto national CERT has academic roots and is well established since a couple of years at the time the government decides to set up a dedicated government CERT. The very cooperative kind of the relationship, where the established (academic) CERT supports the new and the new governmental CERT learns from the established should be emphasised.
Additional information can be found in the proceedings.

Presentation from Hungary

The presentation from Hungary was focused on a cooperation activity of the national CERT in a specific sector (banking) that was also successfully established in at least one other Member State (The Netherlands). CERT Hungary, the Hungarian national CERT, operates a couple of cooperation activities with banks, banking associations and financial regulators that mainly have as aim information sharing (especially during and after incidents) and exercises to prepare the financial sector to mitigate and react to threats and incidents in an effective fashion. The Hungarian (as much as the Dutch) cooperation is an example for a national CERT that undertakes efforts to improve the resilience for a crucial sector in its country, and could act as an example for other Member States. This model of cooperation will be made widely known to other Member States and supported by ENISA via its NIS brokerage function.
Additional information can be found in the proceedings.

Presentations from Spain

The Spanish presentation was given in two parts with separate speakers. The first presenter outlined the Spanish national response strategy for infrastructure protection. Spain chose a holistic approach to security and a multi-sectoral discussion with police forces, government departments, operators, managers and owner of networks, and emphasis the importance of international cooperation. Spain operates a dedicated coordination centre for CERT activities (ES-CERT-CC, a service inside of the CNPIC (National Centre for the Protection of Critical Infrastructures) in order to provide a coordinated response to threads and/or attacks targeting the national critical infrastructures) and the responsible national centre for infrastructure protection (CNPIC)

also acts as Spanish point of contact for international cooperation. Besides this Spain runs a separate governmental CERT (CCN-CERT, established in 2007) and a CERT for SME and citizens (INTECO-CERT). Besides this also Spain has a very experienced, well established and known CERT in the academic sector, RedIRIS CERT. National cooperation among the CERTs and operators like ISPs are established on a more bilateral basis between two parties, but a plan for the establishment of a national Spanish CSIRT association involving all relevant stakeholders is in place.
Additional information can be found in the proceedings.

Examples from Non-EU countries

Participants from the US and Japan were invited to provide a beyond-Europe view on national response planning and the role of national CERTs. Additional information can be found in the proceedings.

Preliminary Results

The diversity of solutions chosen by the various EU Member States who presented their approaches during the workshop showed, that a generic good practice guide containing good practice on cooperation on national level and national incident response plans suitable for all EU Member States is difficult if not impossible to achieve. For example there are different approaches to motivate the cooperation among key players during incident response. While one Member State bases this cooperation on a voluntary model, another Member State chose to enforce cooperation via legislation. Another example is the variance in the definition of sectors, priorities and interdependencies.
A possible solution is to break down the topic into smaller parts and provide good practice for specific tasks. The suggestions made by DG INFSO concerning WPK2.2 in ENISAs Work Programme for 2009 outline a feasible approach to a good practice collection and will be further taken into account while formulating that work package. In addition ENISA will investigate which activities carried out by national/governmental CERTs exist in the EU Member States to assess or define a common set of services, structures or other means of national response planning that can support ENISAs goals.

Conclusions and next steps

ENISA will continue in two steps with its approach for 2009:

Implement the comments and proposals from DG INFSO

In the process of the development of ENISAs Work programme for 2009 the next version of the description of the "CERT Work Package" (WPK 2.2) will be written out implementing the comments and proposals DG INFSO made concerning the previous version of the description:

> *WKP 2.2: we recommend ENISA to work with Member States to identify best practice and formulate guidance regarding minimal (baseline) services and functions for national/governmental CERTs as a pillar for national incident response capability and as a basis for structured and effective European/International cooperation. To this end, tasks could be envisaged on: i) stock taking of existing*

approaches and initiatives in the EU and internationally; ii) analysis of existing practices; brainstorming with stakeholders on good practices, gaps and possible development as well as validation with national competent Authorities of perspective guidance.

In adapted form these recommendations seem to be a most suitable way to approach the complex topic of good practice compilation for national response planning and the role of national CERTs in the EU Member States.

Continue ad facilitate the dialogue with all relevant stakeholders

The process of discussion with stakeholders (like the EC, the Member States and others) needs to be continued in 2009 in order to prepare ENISA to give advice to the Member States and the European Commission concerning roles and services for their national CERTs (task ii. in the recommendations of DG INFSO).

Proceedings of the Workshop

All related material including the presentations is published on the ENISA website:
http://www.enisa.europa.eu/pages/04_01_4th_cert_ws_2008.htm