European Network and Information Security Agency
Science and Technology Park of Crete (ITE)
PO Box 1309
71001 Heraklion, Greece
www.enisa.eu.int
Tel: +30 2810 391280
Fax: +30 2810 391410

ENISA *ad hoc* Working Group on CERT cooperation and support

Heraklion, 06 February 2006

Purpose of this document
This is the final report and is intended to give an overview of the activities of the ad-hoc working-group CERT cooperation and support in 2005, the delivered documents, recommended follow-up activities/documents for ENISA. The report also gives a proposal for a possible continuation of the activities for this group.

Terms of Reference
The Terms of Reference of this WG designate the following tasks:

Task 1:	Validate the data stock for ENISAs *Inventory of CERT activities in Europe*[1]
Task 2:	Perform a gap analysis of geographical and business areas that are not covered by CERTs or similar organisations
Task 3:	Recommendations for enhancing co-operation between CERTs
Task 4:	Compile a checklist or list of guidelines on how to establish a CERT, of recommended training and needed skills for the staff

The resulting documents (except for TASK 1) were to be compiled into a complete report as input for the management board on the status of the work of the group and the deliverables.

Activities of the WG
In June 2005 this WG was appointed to support the Agency in addressing particular matters in the field of CERT cooperation and support. The deliverables have been identified in a “Terms of reference” document. In total three meetings have been organised by the secretariat to carry out the necessary tasks and activities which have been foreseen to complete the deliverables. The secretariat was run by ENISA.

The following deliverables have been submitted:

- Document **Task 2: Gap analysis of areas not covered**
- Document **Task 3: Recommendations for ENISA**
- Document **Task 4: Guidelines on establishing and training of CERTs**

The single documents are compiled into a final report by the secretariat.

Follow up for ENISA
The final report has to further be processed to provide ENISA with clear perspectives for the future work in the field of CERT. This will be done by ENISAs own experts.

[1] http://www.enisa.eu.int/deliverables/

Conclusion

Alone to be able to track the developments in the European CERT community it is necessary for ENISA to proceed with the ad-hoc working-group in that field. For a new working-group in 2006 a re-allocation of members, including a more precise “call for interest” with a more precise focus of the work of the group should be discussed. Possible tasks for a new CERT working-group are:

- Look into quality measures for assuring a successful operation of CERTs and similar bodies
- Is ENISAs focus on CERTs contemporary? How can it be broadened? And therefore:
- Look into the question “Which (groups of) users to need which security services and what is the appropriate facility to provide them?”

Annex: Results of the work

Introduction

Computer emergency response teams (CERTs[2]) play a key role in the field of network and information security. Their work is essential in preventing security breaches, limiting the damage resulting from a breach as well as in recovering from a breach as quickly as possible. In addition they provide assistance to victims of attacks, vulnerability assessments, awareness raising and promotion of best practises. Today, there are already a significant number of CERTs in Europe. However, their coverage is far from sufficient to serve all Internet users that could benefit from such services. Therefore, incident management within organisations should be encouraged, including but not limited to the establishment of new CERTs, the expansion of CERT communities and improvement of information sharing capabilities.

The setting-up of and cooperation between CERTs currently is facilitated by several organisations and initiatives, e.g. TERENA's Task Force CSIRT (TF-CSIRT), FIRST and the European Government CERT group (EGC). As ENISA does not want to duplicate tasks it should be made clear where further action is needed in the area of CERT cooperation and support and what role ENISA should play e.g. in facilitating the setting up of new CERTs and to facilitate cooperation between existing CERT in Europe.

The special ad-hoc working-group CERT cooperation and support was set up in 2005 to support ENISA in this task. In their "Terms of reference" document the group identified the following tasks:

Task 1: Validate the data stock for ENISAs Inventory of CERT activities in Europe

Task 2: Perform a gap analysis of geographical and business areas that are not covered by CERTs or similar organisations

Task 3: Recommendations for enhancing co-operation between CERTs

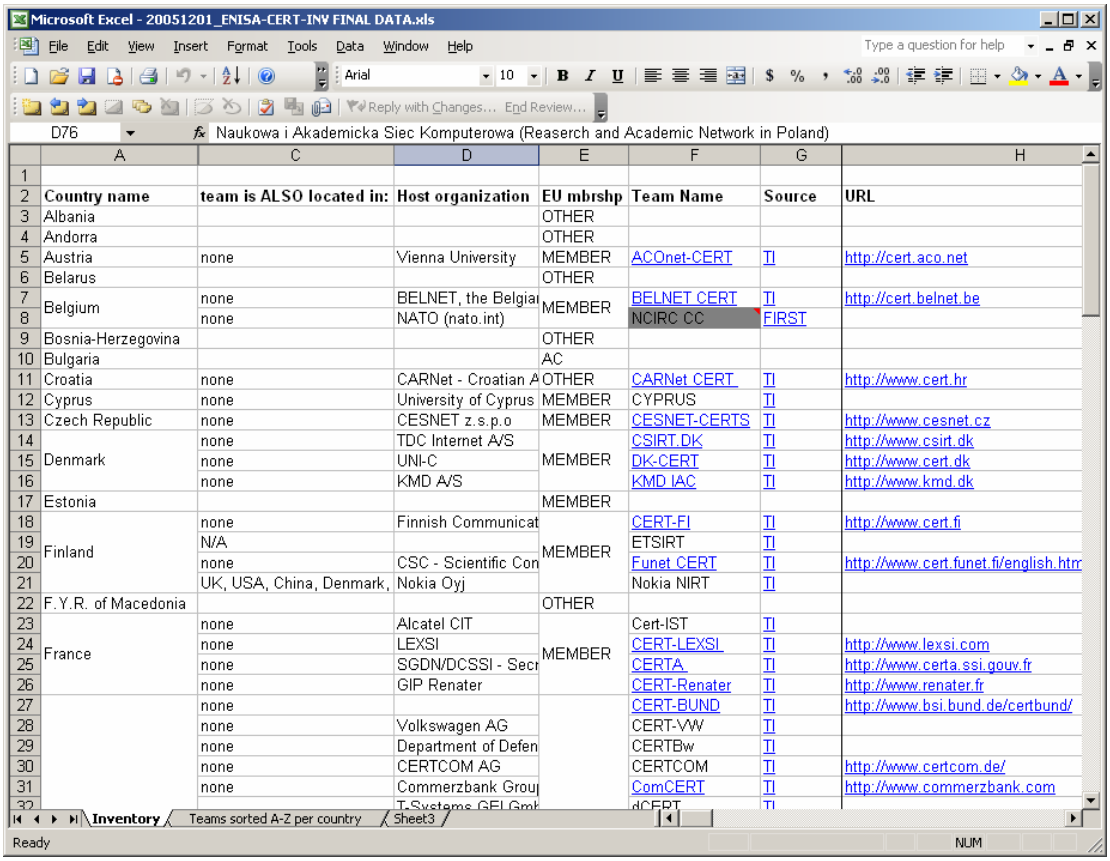
Task 4: Compile a checklist or list of guidelines on how to establish a CERT, of recommended training and needed skills for the staff

The report at hand compiles the result of the work.

[2] Nowadays the term CSIRT (Computer Security and Response Team) is more appropriate, because CERTs offer much more services than incident response. Nevertheless the widely established term CERT is used in this document to address all forms of facilities that provide security services.

Task 1: Validated Inventory on CERTs in Europe

The working-group checked and verified the data-stock which was provided by ENISA. The validated data stock was compiled into ENISAs Inventory of CERT activities in Europe and can be downloaded from ENISAs website[3].



Microsoft Excel - 20051201_ENISA-CERT-INV FINAL DATA.xls

File Edit View Insert Format Tools Data Window Help

D76: Naukowa i Akademicka Siec Komputerowa (Reaserch and Academic Network in Poland)

	A	C	D	E	F	G	H
1							
2	**Country name**	**team is ALSO located in:**	**Host organization**	**EU mbrshp**	**Team Name**	**Source**	**URL**
3	Albania			OTHER			
4	Andorra			OTHER			
5	Austria	none	Vienna University	MEMBER	ACOnet-CERT	TI	http://cert.aco.net
6	Belarus			OTHER			
7	Belgium	none	BELNET, the Belgiar	MEMBER	BELNET CERT	TI	http://cert.belnet.be
8		none	NATO (nato.int)		NCIRC CC	FIRST	
9	Bosnia-Herzegovina			OTHER			
10	Bulgaria			AC			
11	Croatia	none	CARNet - Croatian A	OTHER	CARNet CERT	TI	http://www.cert.hr
12	Cyprus	none	University of Cyprus	MEMBER	CYPRUS	TI	
13	Czech Republic	none	CESNET z.s.p.o	MEMBER	CESNET-CERTS	TI	http://www.cesnet.cz
14	Denmark	none	TDC Internet A/S	MEMBER	CSIRT.DK	TI	http://www.csirt.dk
15		none	UNI-C		DK-CERT	TI	http://www.cert.dk
16		none	KMD A/S		KMD IAC	TI	http://www.kmd.dk
17	Estonia			MEMBER			
18	Finland	none	Finnish Communicat	MEMBER	CERT-FI	TI	http://www.cert.fi
19		N/A			ETSIRT	TI	
20		none	CSC - Scientific Con		Funet CERT	TI	http://www.cert.funet.fi/english.htm
21		UK, USA, China, Denmark,	Nokia Oyj		Nokia NIRT	TI	
22	F.Y.R. of Macedonia			OTHER			
23	France	none	Alcatel CIT	MEMBER	Cert-IST	TI	
24		none	LEXSI		CERT-LEXSI	TI	http://www.lexsi.com
25		none	SGDN/DCSSI - Secr		CERTA	TI	http://www.certa.ssi.gouv.fr
26		none	GIP Renater		CERT-Renater	TI	http://www.renater.fr
27		none			CERT-BUND	TI	http://www.bsi.bund.de/certbund/
28		none	Volkswagen AG		CERT-VW	TI	
29		none	Department of Defen		CERTBw	TI	
30		none	CERTCOM AG		CERTCOM	TI	http://www.certcom.de/
31		none	Commerzbank Grou		ComCERT	TI	http://www.commerzbank.com
32			T-Systems GEI Gmb		dCERT	TI	

Inventory | Teams sorted A-Z per country | Sheet3

Ready NUM

[3] http://www.enisa.eu.int/deliverables/

TASK 2: Gap analysis of areas not covered

Introduction

The ad-hoc working group was asked to deliver a gap-analysis, which should reveal areas not covered by CERT services. As an input we used the CERT inventory provided by ENISA as a starting point. Our approach to the task of completing a good and valuable gap analysis was to set up a list of questions that the analysis should answer for its reader ("If you know the questions it is easier to look for the answers").

During the work we have identified some areas of concern that impact both the gap analysis and its results. For example: we have looked at the available information about teams and found out that there are many teams that only provide their services for their hosting organisation and that don't publicly promote their activities. A lot of these teams play a very active role in handling threats and incidents, but they only work inside their organisation and avoid to be known as CSIRT outside this boundary. Another concern: due to a lack of time and resources it was not possible for us to interview each team individually, and the publicly available information might not necessarily allow an accurate interpretation of the team's charter and mission.

Therefore, the goal of this gap analysis can not be to provide a fine detailed map of coverage with CERT services in Europe. We rather see our main task in the analysis of the major areas of CERT related activities and the gaps within these activities.

We used a two-step approach: first we used the CERT inventory provided by ENISA to produce a matrix that describes the coverage of sectors in each country. This first step provides an overview of the available facilities and their services in Europe. Due to the above-mentioned lack of detailed information about CSIRTs and their services, this matrix can only be viewed as a very high level approach to a gap analysis.

Based on this matrix, our second step was to formulate and answer the questions a specific constituency might want to be answered by our gap analysis.

Depending on the specific role of a person, his or her questions might be different. It turned out that we have identified three main target groups that might want to review the gap analysis and find answers to their specific questions inside. Therefore, we have structured our analysis accordingly.

Coverage of Sectors and Constituencies

The inventory of CERT activities in Europe compiled by ENISA provides insight to the distribution and coverage of CERTs in Europe. The existence of at least one CERT in a country obviously serves as a major indicator on international level to understand whether there is any CERT capability at all. But the majority of countries today host more than one team. Therefore it is interesting to take a look at the main categories of sectors and constituencies that should be covered from a national perspective.

To manage the task it was decided to concentrate on the four sectors:

- **Citizen** – the individuals living in the country
- **Research / Education** – including academia and research networks
- **Government / Public Administration** – all entities and organisations on federal and state level (including the military)
- **Commercial** – entities like companies that are not already covered. To allow a more

distinctive discussion, we put commercial entities that are usually named as Small and Medium Entities (SMEs) in a separate category.

Certainly there could have been more elaborate schemes adopted for this report, but it is felt that the scheme is pragmatic and provides the most important insights. See Appendix A for the table of the coverage sectors/countries.

Some words about Critical National Infrastructure (CNI) Protection

The working group had a long and controversy discussion about the role of the components usually referred to as Critical National Infrastructure (CNI). While it is true that there are teams explicitly established for helping the companies and organisations involved in securing the CNI, it is also true that there is no practical way to separate ordinary companies from the ones that are involved in this CNI-related activity. At the end we had a vote whether to include CNI as a separate sector in the table or not. In the end only by one vote the working group decided to keep the table as it is right now.

Instead we decided to add a separate statement on CNI to the report. In most European countries CNI discussion are already initiated by the Government, and within Europe member states governments are looking for cooperation on CNI-issues. An example is the EGC-group, which consists of governmental CSIRTs with a focus on protecting CNI.

The problem with having CNI as a separate sector in this gap analysis is, that there is no clear and commonly agreed definition of CNI and how this topic should be approached. Some countries talk about CIIP (Critical Information Infrastructure Protection), others use the broader definition CIP. The CIIP handbook 2004[4] made an inventory and analysis of protection policies in fourteen countries that could be helpful in this matter. Most countries approach it by defining their critical business sectors and develop cooperation between the governments and those sectors. Furthermore, CNI protection is covered by more than one sector we defined in our gap analysis, so adding it as an additional sector was not considered appropriate by the majority of the group.

Gap Analysis from various points of view

As we already noted above, it is obvious that, depending on the specific role of a person or organisation, relevant questions and attitude towards CERTs and their services might differ. Within our working group we identified three points of view. The associated user-group is either considered as a direct target group of this report, or as an indirect target audience which just might be interested in reading this report.

We selected:

- **A citizen's point of view** – an individual end-user using a system that is connected to a network (mainly private users).
- **An organisation's point of view** – any organisational entity using CERT services
- **A government's point of view** – the view of a government of an EU member state

To address each target group we tried to formulate questions concerning security, this specific group might have and, in a second step, tried to answer these questions. The following text is

[4] CIIP handbook 2004, http://www.isn.ethz.ch/crn/publications/publications_crn.cfm?pubid=224

structured accordingly.

We found out that there is one common question to all three groups: How can “my” gaps be filled? It is obvious, that for every group gaps in the supply with CERT services exist, some more critical than others, and therefore a structured approach to address the most critical ones is necessary. But given the limited resources of the working group and the terms of reference, we are unable to provide a final, comprehensive answer in this document. However, other results from the working group, most namely the recommendations, are pointing towards the right direction and will help government officials and representatives of other organisations to explore further opportunities of how they can at least narrow down the most critical gaps.

Gap Analysis from the Citizen point of view

We consider a citizen in the context of this analysis mainly as a private end-user. The questions private end-users might have can be separated into two categories: questions about reactive security (in the case a security incident already happened) and questions about proactive security. Both areas lead to an underlying question that needs to be addressed first: whom can a private end-user trust?

Reactive Security

Q: *What happens with if I become a victim of an attack? Should I care? Will I be contacted?*

A: Unless a victim is served by a service provider, most likely an ISP or a bank, there is simply no chance that a private end-user is contacted in case of a security incident. As of today there are no CSIRTs that are prepared to support private persons as there is no supporting infrastructure for contacting them. Only if an already established relationship exists, as in the previously mentioned service provider scenario, someone will care – depending on the business attitude.

Basically, all end-users should care about attacks, especially about successful ones. Numerous examples have shown that despite antivirus tools and other efforts to keep a system secure, end-users do not make backups regularly and do not really understand the impact a compromised system can have – until it is too late.

In high profile incidents, law enforcement will be interested to talk to end-users as well. In most cases they are only of interest if their computer attracted attention in some other investigation – for example copyright infringement or other, worse cases. But due to the lack of resources and mandate, law enforcement forces are also not suitable to help end-users to recover from an incident.

But for the last two years governments started to recognize the situation that end-users, especially private persons, are rather helpless in case of attacks. Therefore, some governments like the Netherlands and Germany have started activities to alert and inform this user-group about security issues. However, in most concepts there is no room for providing a full-fledged helpdesk for all kinds of requests of (private) end-users. In case of a high profile attack, for example a new worm that invades millions of systems at the same time, probably no governmental institution has enough resources to protect all of the private end-users to 100%, regardless how much effort has been made before.

At least private end-users that are more technical interested and educated might be able to gain support and help from other available resources. Although CSIRTs usually are responsible for closed communities, much of their technical information like security advisories is publicly available, free of charge. And most existing CSIRTs belonging to national research networks will not refuse to give at least limited support, in case a victim calls its hotline.

Q: *What kind of response can I expect? Will someone help me solve my problem? To whom do I report incidents?*

A: As noted above, the expectations of (private) end-users should be rather low. In general, nobody is directly responsible to solve their problems nor has a mandate to accept incident reports from them.

In the recent past, some activities have been founded that allow private end-users to report incidents, but these activities do not provide other reactive or proactive services and henceforth no further support will be provided directly in return.

Proactive Security

Q: *Do I have access to the information on how to make my system secure? Does this include vulnerability information from all vendors that are of interest for me? How do I know the vendors of interest for me? Do I understand the information as provided? Where do I find relevant information?*

A: Besides the efforts mentioned above, the necessary information to secure a system is not specifically tailored for the private end-user. A good start for this group of user is to use operating systems that provide an authenticated, secure and automatic update mechanism. Even if, due to technical or practical reasons, automatic update does not always works the way intended, the benefits of this approach proved successful in the field.

Most of the publicly available security advisories provide too much technical detail to be useful for most of the private end-users. If these do not include simple messages like “Patch your system! For this do X, Y and the do Z” the provided advisory is of little or no use for most end-users. Alas, this also raises the question “Which source can I trust?” (See below).

Sensitised by the media, a growing number of private end-users start to care about security of networks and computers. In search for help, and due to a lack of clearly communicated security contacts, a lot of persons rely on personal networks, friends, relatives who appear to have a decent level of knowledge, but often do not and by this make the situation even worse. Customers of specific service providers, most namely online banking services, nowadays receive tailored information addressing the security of this special service (phishing information, answers to questions about authentication, etc.). But beside these promising initiatives not much appropriate security information is readily available for private end-users, and at the moment of this analysis it is not clear if and how this will change in the future.

Q: *Whom do I trust?*

A: There is no generic answer to this question, because trust relies mainly on personal experiences and expectations. As trust is usually established over time and based on personal relationships, it is very difficult to assess if there are overall trusted relations for this group at all. It can be expected though, that private end-user that for example visited an university or who themselves have a technical background are likely to have heard about existing CSIRTs and might trust them due to some background checking and feedback received from others. Also it must be mentioned that governments already receive a lot of trust per se by most private end-users, so they can successfully act as a trusted source of security information (and have often already realised this) for this group of users.

Gap analysis from an organisational point of view

Within a lot of organisations CSIRTs have been established as separate entities which main task it is to dynamically respond to actual trends and threats that have not been properly addressed by the traditional risk management. However, nowadays more and more

organisations realise that a more integrated approach to organisational security is needed, combining traditional risk management with more adaptive and flexible approaches to react to actual trends on the spot. In this regard the main question for every organisation is how it will handle security events as part of their overall security management. More specifically it will need to answer the following questions:

- Are we prepared to handle attacks, system compromises and other security incidents effectively? Do we provide a single security POC (Point of contact) into our organisation?
- Does our organisation need to be represented in national and European CERT communities? If yes, by whom?
- Would standardisation and adoption of best practices improve our ability to respond?

There is some overlap with the questions from a citizen point of view, but they in most cases imply a much more critical impact, that also, to some degree, depends on the nature of the organisation and its business.

- What happens if we become victim of an attack? Will we be contacted? To whom do we report incidents?
- Do we have access to information how to make our systems secure? Does this include vulnerability information from all vendors that are of interest for us?

And again the overall question: whom can we trust?

Reactive Security

Q: *Is my organisation prepared to handle attacks, compromised systems and other incidents effectively?*

A: As 100% effective security does not exist, the simple answer to this question is: partly. The level of preparedness usually depends on the size of an organisation and its business culture. In case of a big company with risk management (RM) and risk analysis (RA) processes implemented into the overall business process, and probably with a own response team a usually high level of preparedness to handle network attacks on their infrastructure and resources can be expected. This is also the case in organisations related to research and academic, as they historically and from their profession have a high affinity to computer and network security.

The situation within the group of smaller organisations such as small and medium enterprises or freelancers is much more somber. The preparedness to react adequately to security incidents is usually much lower here, even though most of these organisations are aware of the threats posed to IT systems that are attached to the internet. This is mainly due to a lack of resources, so the provision of this group (SMEs) with payable security services have recently been discovered as a promising business field for some security service providers, and also some governments started similar initiatives, but the situation in this field is still far from being sufficient.

Q: *What happens if my organisation becomes victim of an attack?*

A: In the case that an organisation, independent from its size, has a dedicated incident detecting system (like intrusion detection systems -IDS) in place inside its network, then chances are good that an organisation will react to detected attacks. This reaction may differ – for example ranging from monthly summary statistics reports of unsuccessful attacks to real time reports and an execution of appropriate response procedures.

If an organisation has no detecting capability at all and it does not experience any change in its

infrastructure (like system behaviour) or in a business process, there is a quite likely that there will be no reaction within an organisation.

Without detection systems enterprises can only defend themselves by preventive actions. Consequently most small and medium enterprises rely heavily on pro-active measures but maintain no response capabilities at all. This also means that, as there is no 100% effective prevention that they are subject to attacks to a much larger scale. If at all, successful attacks are only detected by misbehaving systems (performance decreases, complaints about unsolicited mail from a specific system, etc.). As they usually do not have a formalised method of reaction, users and administrators inside this organisation are left alone, and often panic reactions only makes things worse. This situation can be improved by raising the security awareness level of users and administrators alike, and spreading wider knowledge of external organisations capable of help.

Q: *Will my organisation be contacted in case of an attack?*

A: As written above, the possibility and willingness of an organisation to react to security incident highly depends on its detection capabilities. In case of lacking these abilities the only chance to bring security incidents to the attention of these organisations is by a "signal from the outside". There are a lot of external warning and alerting facility which provide their service for the internet community as a whole, like SPAMCOP, AUS-CERT Probe Reporter, SecurityMap.Net, Brazilian CAIS-BR system etc. These are usually free of charge and by that a good source of incident detection information for organisations without their own capabilities. A second possibility, which is widely used in practice, is the notification about security incidents affecting an organisation by an operating CSIRT or other response team, during their incident handling processes. One most useful source of contact information for a CSIRT is the data in the RIPE database[5]. So for the correct functioning of this alert method it is essential to populate the RIPE database with as much useful information as possible, mainly by maintaining dedicated data-fields like the RIPE database IRT object, which contains information about a responsible CSIRT for a specific IP address, or a similar field for information about appropriate abuse teams.

But operational response teams use other sources of information besides the RIPE database. Often an incident reporter searches for an appropriate contact data directly at victim assets (e.g. a company website). So it is important also for small organisations to make this data available and visible.

If a victim of an attack is untrained in security questions, he possibly cannot properly and responsibly interpret warnings from third parties, so he (in most cases) ignores them. This could probably be circumvented by alerting the appropriate ISP of the organisation instead, which then can locate the victim by their own customer database, and also help them to recover from the attack.

Q: *To whom does my organisation report incidents?*

This question applies to two different subgroups inside this group of users, and so there will be two different answers. First there is the sub-group of members of an organisation, which means end-users belonging to a specific company, enterprise, etc. Second, the question applies to an organisations internal security point of contact (POC), if such facility exists. In this case the first subgroup usually report detected incidents or anomalies to their POC. If no POC exists, the previous given answer to the citizens group applies: There are few, if any, contact points to report incidents to, mainly set up by the government of a specific country. POC on the other

[5] http://www.ripe.net

hand when it comes to incident reporting can act like a “full grown” CSIRT: report incidents and attacks to the POC of the attacker, the appropriate CSIRT, abuse team, ISP or other facility. But in most cases this is not done due to lack of resources (a lot of POCs also fulfil other roles in an organisation), so outsourcing this problem could be a solution for these organisations.

Proactive Security

Q: *Does my organisation provide a security POC (Point of Contact) into internal constituency?*

A: The answer to this question is very much related to the fact of existence (or not) of an incident response team (IRT) within an organisation. If it does exist it usually provides its community with a visible POC. If an organisation does not entertain its own response team, they usually do not have a visible POC.

Some organisations with a decent level of security awareness just outsource its incident response services, keeping within an organisation only an internal POC which is usually not visible to the outside. Such organisation is represented to the outside by this service provider and it must take care that this information (through website, etc.) is made available to the public.

But the somber answer for most SMEs is: there is no POC for their organisation. There might be an employee, who acts as a part-time security officer, but his tasks are most often not formalized and the provision of this service is subject to personal connections in many cases.

Q: *Does my organisation need to be represented in national and European CERT communities?*

A: Most of the organisations will recognize that "gaining access to information is important". This is especially true for information on IT and network security that is provided by CSIRTs and related organisations. Those share this information in for a like TF-CSIRT, EGC or E-COAT, but that does not necessarily mean that an organisation must be a member of these European CERT communities (and, if existing, national communities too) to participate in security information relevant for them, because a lot of teams and also the communities share information with the public (through websites, mailing-lists, etc.).

Alas, organisations that run internet dependant critical business are good advised to at least keep close touch to the communities of response teams, as for them a more detailed grade of information which has to come in more timely and frequently vitally important. Specific incident related information like compromised systems, attacking hosts or log-files are considered sensitive data by CSIRTs that potentially can compromise parts of their constituency. To get access to this information it is necessary to participate in the appropriate European CSIRT community (see “ENISA inventory of CERT activity in Europe”) for both trust-building (which works best on personal, bilateral level) and to communicate the existence of a POC to the other teams.

Q: *Who should represent my organisation in national and European CERT communities?*

A: This question can easily be answered for organisations that already have their own IRT: they will be represented by their team. As for the ones that can't afford this type of contact, they should be represented by either a coordinating CSIRT or by the service provider/ISP as part of its mission.

In the case of SMEs it is possible for them to be represented by their professional organisation (like for example their respective chamber of commerce), or by other enterprises (outsourcing).

Q: *Would standardisation and adoption of best practices improve my organisations ability to respond to security incidents?*

A: Incident Response is essentially based on the exchange of information, so both

standardisation and the adoption best common practice (BCP) are key factors, and those two domains have been of concern to the CSIRT community for quite some time. Nevertheless, the level of standardisation is far from being sufficient, and this also results in a lack of appropriate tools for information sharing and of widely accepted BCP. By helping to stabilise emerging standards and by collecting and distributing of BCP between similar (in size, sector, or maturity) organisations would contribute to improving the current situation.

For those – mainly small – enterprises which do not have their own RM/RA groups and response team standardisation will not provide many advantages. In this case, the current situation can be enhanced by providing free, publicly available information which describe these problems in a way that is understandable for the end users. Raising awareness by for example teaching these organisations appropriate reactions to attacks would literally establish a culture of security in this field.

Q: *Does my organisation have access to information how to make our systems secure?*

A: Information about hardening it systems is publicly available on the internet in a sufficient number and technical depth publicly, supported by many articles in computer magazines which deal with this topic. A problem could be raised by the widespread and differing level of quality of this information, as an organisation (especially SMEs) could lack the expertise to find, evaluate and implement the information. As long as these organisations is willing to spend money, for example for subscription to security services, or for external to compile the information, or time and resources to do this by themselves, organisations do have access to the sufficient information on how to make their systems secure.

Alas, in all cases the following questions have to be addressed: does the available information come from trustable sources and do I really have access to all needed security information, without limitations due to business models of the vendors?

Trustful information usually can only be provided in case of larger enterprises, when the source and user of the information are in contractual relation, so there is a predefined informational tunnel between the parties, often enhanced by personal connections.

Q: *Does this include timely vulnerability information from all vendors that are of interest for us?*

A: This question contains two sub-questions, asking for “timeliness” and “completeness”. But for both sub-questions there is one unique answer: both the timeliness of the provision of vulnerability information and the question, if a vendor provides this at all depend highly on the vendor and his business model. Not all vendors provide security information about their products and some do this only if they are paid for. But in the recent years a growing number of vendors do provide timely security information for their products as this is more and more seen as a performance indicator for the overall quality the company provides. Nevertheless the provision of security information by a vendor should, if possible, be regarded before the purchase of a product.

Whom does my organisation trust?

Given the lack of a worldwide established and accepted certification scheme for incident response facilities and providers of security information, an organisation will mainly trust those entities with which they developed a sufficient level of trust, mainly on a personal basis. That also includes trust-relation to the own response capabilities, which is (surprisingly enough) not always given per se.

Question from a governments point of view

Usually a government sees NIS integrated into more global concepts to protect critical national

infrastructure. Also has a government to take into account the variety of target groups to be covered by security services. Our working group identified three main aspects and tried to formulate the appropriate questions.

- Is there a dedicated security point of contact (POC) into my country? Is there an entity that is responsible for incident response (coordination) on a national level? What kind of model is used to handle incident response on a national level – federal or centralized?
- Are all my domestic constituencies covered? Are enough resources made available to provide the right set of security services?
- Is my country represented in the European and international CERT communities? By whom? Is there some EU integration?

And, like before, the final question is: How can the detected gaps be filled? It proofed that these questions were the most difficult to answer for our working group. Alas, the question about trust, which seemed difficult to answer for the other two user-groups dealt with in this document, is less problematic for a government. For a long time governments have build up a framework for negotiations and settlement of disputes that is already explored for addressing some of the underlying issues we have touched in our analysis.

Reactive security

Q: *Do we provide a single security point of contact (POC) into our country? Is there an entity providing incident response (coordination) service on a national level?*

A: Traditionally in most countries the first CSIRT built up acts as an initial point of contact for reporting incidents. In most cases these are CSIRTs in the research and academic sector whose task it is to protect the national research network. In the recent years more and more European governments have started to build up governmental incident response capabilities that take over the responsibilities for the governmental institutions. In some cases this (new) CSIRT evolves into the national POC, at least for incident handling. In other cases, especially in countries with an already very well established CSIRT community, this is not the case, and the teams inside this country act as contact points for their respective constituencies. But in all cases known to us the governmental CSIRT, even if it faces an established community in its country, is accepted as an equal partner on national level.

Some European countries have chosen to assign specific responsibilities for tasks on a national level to their governmental CSIRTs, including services to protect critical national infrastructure (CNI) or to support the citizen in regard to NIS. In some cases this might include the role of a national security POC.

Overall, the need for co-ordination on a national level, and also the benefits of a single POC for reachability of a nation, is a widely accepted matter of fact. But as for now not all of the European countries have established a dedicated security POC.

Q: *What kind of model is used to handle incident response on a national level – federal or centralized? Are all my domestic constituencies covered?*

A: As this first, very high-level gap analysis already has shown, there are many constituencies left without coverage of CERT services. Also the existence of a national security POC is not always guaranteed. But we see more and more countries in which the existing CERT community tries its best to resolve and respond to incidents, inside and outside their own organisations / constituencies. Co-ordination on national level is in some cases a really community-driven effort, which in many cases works very well. In a case of emergency like a new worm some CSIRTs are volunteering to serve as coordination centre and help especially

peers in other countries by identifying the right point of contact for given sites and organisations, sometimes on a ad-hoc basis.

In some countries established CSIRTs have set up national co-operation activities without coordination by their governments, and they gave themselves their own policies and procedures. Dealing with national incidents is usually on their agenda and while no formal contracts were signed it can be expected that these countries will more likely be able to pull together existing resources and respond faster and better to any incident they might face. It needs to be recognized that most national communities have been established by peers, the government CSIRTs only one part of them. This is especially true, as said before, if the country already has a history of CSIRT activities when the governmental CSIRTs finally have been set up. In most countries research networks were pioneers in the field of CSIRT activities, spreading the word as well as helping other teams to evolve. But it is important to note that the development today looks quiet different in countries without established CSIRTs. In such countries it is the government that, pushed by the increased security awareness in other countries, kick-start such activities.

It is assumed by many parties that a centralised model for CSIRT co-ordination would improve efficiency. But so far the experience has shown that the mutual interests between CSIRTs acting for various constituencies could be better leveraged within a peer-to-peer structure. While a lack of centralised authority prevents any way of steering this structure, the established network of trust is very strong and growing as it needs to. But with more and more overlapping interests - most namely from the viewpoint of a nation most certainly subsuming all "national" constituencies - there must a better understanding of alternative co-ordinating structures be achieved. It is the opinion of this working group that the discussion of this topic needs much more research and analysis, before any common, concluding understanding can be found and improved framework can be established.

This again touches the issue of coordination on national level. In the past some coordination projects were started in some countries, but they all failed to add value to services the existing CSIRTs already provided. In our opinion this is due to an immature understanding of coordination issues and a lack of resources invested in research in this field. Some experts have expressed concerns about this lack of progress, but as CSIRTs are tasked to handle incidents usually by their management, including the governments as a special form of management, they are not willing to assign resources to such tasks, as they not provide an immediate benefit.

Proactive security

Q: *Are enough resources made available to enhance the coverage with security services in our country?*

A: While usually the availability of resources is not considered sufficient by the involved players, some countries started important initiatives over the past few years to address at least some gaps in their country’s CSIRT landscape, namely citizens and SMEs. As both groups by itself lack an established community, one clear task for a government is to support their citizens. In addition SMEs, as they are often received as citizens running their own business with IT and networks, are targeted by the government, as nobody else can provide help within the budget constraints SMEs usually face. And, as already mentioned before, a growing and well understood trend to address the protection of critical national infrastructure can be observed in the European countries.

As a governments usually do not have enough resources available to fulfil these tasks alone, co-operation with the private sector, most namely public – private – partnerships, are more and more considered as a useful alternative.

Q: *Is my country represented in the European and international CERT communities?*

A: Within the recently published ENISA inventory and the country pages of the Trusted Introducer service all governments can easily identify non-governmental CSIRT activities and their representation within for example EGC, TF-CSIRT or FIRST.

It is clear, that representation is needed on various levels, not only to ensure that critical information is accessible but also to influence the further development in the field of NIS. Each country will need to access their current representation and decide on its further course. This again points back to the discussion about established CSIRT communities in which cases a co-operative approach needs to be developed to avoid the perception that the "government is taking over".

Governments right now are highly dependent on the co-operation with other CSIRTs out of their direct control, to plug into international and European communities otherwise not accessible for them. It is of special importance to recognise that the introduction of a national security POC will potentially impact the flow of information to other CSIRTs. Other CSIRTs might change their procedures and report to the national security POC instead of the individual CSIRT inside a country. Several problems can be identified, most namely that this involvement is against the "need-to-know" principle in almost all cases of routine incidents and that the service of the national security POC must then include the further dissemination of information to other CSIRTs as a (free) service. The service level of the national security POC then has a negative impact on the ability of other CSIRTs to respond. While this should not be seen a as show stopper, careful analysis and discussion with all parties involved are mandatory to succeed in enhance the status quo.

Outlook

After having worked together for several months the working group realizes, that this gap analysis is only showing a snapshot of the current situation. It will – as it was outlined earlier – be incomplete and outdated very soon, perhaps already at the time of publishing.

Therefore it is recommended to repeat this exercise from time to time, and also to look closer into specific areas. While global gap analysis like this does not necessarily need to be done on a yearly basis, it will provide interesting and valuable reference for all stake holders anyways.

Appendix A: Gap analysis of areas not covered by CERT services

Country	Commercial		Government / Public Administration	Research / Education	Citizen
	SME	All other			
Albania	No known activity	No known activity	No known activity	No known activity	No known activity
Andorra	No known activity	No known activity	No known activity	No known activity	No known activity
Austria	Partly covered by CIRCA	Partly covered by CIRCA	Partly covered by CIRCA	Yes	No known activity
Belarus	No known activity	No known activity	No known activity	No known activity	No known activity
Belgium	Partly covered	Partly covered	Partly covered	Yes	No known activity
Bosnia-Herzegovina	No known activity	No known activity	No known activity	No known activity	No known activity
Bulgaria	No known activity	No known activity	No known activity	No known activity	No known activity
Croatia	Yes for .hr	Yes for .hr	Yes for .hr	Yes for .hr	Yes for .hr
Cyprus	No known activity	No known activity	No known activity	Yes	No known activity
Czech Republic	Yes for cesnet.cz, cesnet2.cz, ces.net, ten.cz and ipv6.cz	Yes for cesnet.cz, cesnet2.cz, ces.net, ten.cz and ipv6.cz	Yes for cesnet.cz, cesnet2.cz, ces.net, ten.cz and ipv6.cz	Yes for cesnet.cz, cesnet2.cz, ces.net, ten.cz and ipv6.cz	Yes for cesnet.cz, cesnet2.cz, ces.net, ten.cz and ipv6.cz
Denmark	Partly (KMD, TDC)	Partly (KMD, TDC)	Only local authorities	Yes	No known activity
Estonia	No known activity	No known activity	No known activity	No known activity	No known activity
Finland	Partly (Nokia, Ericsson)	Partly (Nokia, Ericsson)	Yes	Yes	Yes
F.Y.R. of Macedonia	No known activity	No known activity	No known activity	No known activity	No known activity
France	Partly	Partly	Yes	Yes	Yes
Germany	Tailored Advisory Service	Some global players, banking sector	Federal, some state	NREN, some universities	(announced)
Greece	No known activity	No known activity	No known activity	Yes (also some universities)	No known activity
Hungary	Partly	Partly	Yes	Yes	Partly
Iceland	No known activity	No known activity	No known activity	Yes (also some universities)	No known activity
Ireland	No known activity	No known activity	No known activity	Yes	No known activity
Italy	Partly	Partly	Yes	Yes	Planned for 2006

Country	Commercial		Government / Public Administration	Research / Education	Citizen
	SME	All other			
Latvia	No known activity	No known activity	No known activity	No known activity	No known activity
Liechtenstein	No known activity	No known activity	No known activity	No known activity	No known activity
Lithuania	Partly	Partly	No known activity	Yes	No known activity
Luxembourg	Subscribers to CSRRT-LU services	Subscribers to CSRRT-LU services	Subscribers to CSRRT-LU services	Subscribers to CSRRT-LU services	Subscribers to CSRRT-LU services
Malta	No known activity	No known activity	Yes	No known activity	No known activity
Moldova	No known activity	No known activity	No known activity	No known activity	No known activity
Monaco	No known activity	No known activity	No known activity	No known activity	No known activity
Norway	Partly	Partly	Yes	Yes	No known activity
Poland	Partly (for .pl)	Partly (for .pl)	Partly (for .pl)	PIONIER network / Partly (for rest .pl)	Partly (for .pl)
Portugal	No known activity	No known activity	No known activity	Yes	No known activity
Romania	No known activity	No known activity	No known activity	No known activity	No known activity
Russia	Partly (WebPlus Customers, General Services)	Partly (WebPlus Customers, General Services)	Partly (General Services)	Partly (WebPlus Customers, General Services)	Partly (WebPlus Customers, General Services)
San Marino	No known activity	No known activity	No known activity	No known activity	No known activity
Serbia & Montenegro	No known activity	No known activity	No known activity	No known activity	No known activity
Slovakia	No known activity	No known activity	No known activity	No known activity	No known activity
Slovenia	Partly for .si	Partly for .si	Partly for .si	Yes	Partly for .si
Spain	Partly for .es	Partly for .es	Partly for .es	Yes (also some universities)	Partly for .es

Country	Commercial		Government / Public Administration	Research / Education	Citizen
	SME	All other			
Sweden	Partly (Telia)	Partly (Telia)	Yes	Yes (also some universities)	No known activity
Switzerland	Partly (Cablecom, IP-Plus, SWITCH customers)	Partly (Cablecom, IP-Plus, SWITCH customers)	Partly	Yes (also CERN)	Partly
The Netherlands	Partly ("Top 500", KPN)	Partly ("Top 500", KPN)	Yes	Yes (also some universities)	Yes
Turkey	No known activity	No known activity	Yes	No known activity	No known activity
United Kingdom	Partly	Partly	Yes	Yes	Partly (through WARPs)
Ukraine	No known activity	No known activity	No known activity	No known activity	No known activity
Vatican City	No known activity	No known activity	No known activity	No known activity	No known activity

Task 3: Recommendations for ENISA

The working group was asked to provide recommendations to ENISA how to facilitate the cooperation between CERTs. While discussing this matter the group came to the conclusion that it should compile a list with global recommendations on how to facilitate CERTs in Europe in a wider sense, including recommendations for enhancing cooperation.

We discovered the following fields of potential ENISA involvement, which will be further discussed in this document:

- Building Trust
- Early Warning System Cooperation
- Information Sharing
- Other issues

Building Trust

One of the areas the working group was asked to analyse were methods for building trust for facilities in order to be able to participate in existing CSIRT networks. This mainly addresses new teams but is also of concern for existing CSIRTs that are, for different reasons, not yet well integrated. Some CSIRTs don't feel comfortable to join communities early on as they consider themselves not to be “on the same (technical) level”. Others are inhibited by not knowing how to approach existing communities and what is the process needed to become a member.

Recommendation 1: Promote existing communities

The first conclusion of the working group was that the existing communities and activities (see ENISAs CERT Inventory) are facilitating a lot of interaction and provide a good set of services and networking opportunities. Some teams have found it difficult to join, but this is already addressed by the communities themselves. Therefore there is no need for any other new organization at the moment.

Recommendation 2: Observe community development

The need for new communities might change in the future as the teams as well as the organizations are becoming more mature. Therefore our second recommendation is to observe the development in that field and analyze the potential for cooperation with the existing organizations in order to take the next step of their development. There might be opportunities for ENISA to facilitate these steps but this will depend on factors not know today.

Recommendation 3: Facilitate participation

Our third recommendation: ENISA should facilitate the broad participation of interested parties in the meetings of existing organizations, as these meetings are especially important to build personal networks. Starting with such personal networks the teams will be able to grow the networks beyond the involvement of single persons towards a participation of the team as a whole. Ways to succeed would be to direct interested parties to planned meetings and disseminate information about upcoming meetings.

Recommendation 4: Facilitate CSIRT mentoring

The working group especially wants to point at the work of TF-CSIRT on some kind of mentoring scheme. The mentoring of new teams by a “mature” team will greatly enhance the integration of new teams as the responsibility for overseeing this integration is explicitly assigned to a specific

team. This assignment not only expresses clear expectations but also communicates the commitment to all parties involved. Therefore the fourth recommendation to ENISA is to facilitate the further development of a mentoring scheme especially by working with TF-CSIRT and EGC to ensure that information about the related practices (checklist for mentors, selection of mentors) and processes (how to identify a mentor) are easily accessible by interested parties.

Recommendation 5: Multilateral agreements and accreditation

Its long and well known within the communities that bilateral agreements (like for example a “Memorandum of Understanding” MoU) are an important and successful tool for cooperation that specifies the “rules of engagement” of the involved teams. Similar to a contract, such agreements lay out the rights and dues as well what sanctions in case of disregard for both parties. While bilateral agreements do not scale in larger communities, they nevertheless solve well understood problems. As these problems usually concern more than two teams inside the various communities, the challenge is to identify the requirements for multilateral agreements and to facilitate the development together with the communities. The most advanced approach so far has been established by the Trusted Introducer (TI) service by TF-CSIRT. The accreditation scheme itself involves an agreement to accept the rules and provide needed information about the participants as well as work inline with the TI processes. In addition to the specific rules and processes the TI accredited teams have accepted a common Code of Conduct (CoC) after long and fruitful, though sometimes difficult discussions. So the fifth recommendation for ENISA is to recognize the scalable accreditation scheme under supervision of the elected TI review board and the TF-CSIRT as best practice and communicate the benefits of the Code of Conduct in support of a more trustworthy infrastructure.

Recommendation 6: Research in other areas of trust building

The sixth recommendation for ENISA is to support further research and activities that are addressing topics which are beyond the current state of the art. We have identified two concerns that are currently under discussion by the community, but lack progress at the moment:

- *Certification*: Most experts consider certification as a useful tool for ensuring specific levels of service quality, but the impact of certification on matters of trust is not well understood. With the growing success of the TI accreditation scheme the question arises how to extend this scheme towards certification, and this question could be explored with TF-CSIRT and the TI accredited teams, but needs resources committed for analyzing the benefits and potential approaches.

- Management of expectations: From the point of view of some security experts the term “trust model” only insufficiently describes the underlying intention. For quite some time those experts demand to replace this vague concept of trust by clearly defined sets of expectations towards cooperation partners, that can objectively be measured and for which it is easy to asses, how well the involved partners meet them . Certification can help to drive this way of thinking, but only if the teams are forced to define their level of services and ensure a specific level of resources. This aspect, therefore, needs research as well.

Early warning systems and Cooperation

The prevention of security incidents is one of the fields in which both CERTs and their constituencies are in constant demand. One key issue to achieve prevention is the efficiency of so called “Early Warning Systems (EWS)” that CERTs use or cooperate with. One of the tasks of our working group was to analyze the needs for early warning cooperation systems.

Overall the Working Group feels that the current lack of cooperation between the "actors” is the

major obstacle to the development of efficient EWS, on both technical and operational basis.

On the technical side one obstacle is the lack of standards to exchange information (data) within a EWS and between EWS. On the operational side the lack of reliability of operation and communication processes, and the difficulty to achieve scalability are the main areas which have to be improved. We foresee a growing use of EWS for closed communities in the near future (corresponding projects have already been started in a couple of EU member states like Germany, Poland and Austria). As it is unavoidable that those communities overlap, EWS will need to collaborate and exchange information among each other to achieve comprehensive coverage. EWS will provide different levels of information, generating various warnings, most commonly on the international level, the national level but will also serve larger user groups like national research networks. Especially those provide an added value to the regular CSIRT services focusing on particular communities. Key factors for CSIRTs who utilise EWS are timeliness and efficiency of response to new threats.

Recommendations for ENISA

The idea of EWS in NIS is not new, and research is being done in a non-coordinated way in various places. A lot of approaches have been tried out, for example automated systems or the usage of expert knowledge systems (e.g. AI). A review of research activities in the domain, and a proposal of cooperation would help create a synergy and improve the cooperation in that field.

In our opinion the development of technical standards and dissolving of technical problems of EWS operations is not enough. We see another important field the development of methods to bring feedback from the constituency back to the operators of a EWS, in order to improve the dissemination of early warnings, and to be able to assess their usefulness.

The working group has tried to address the problem of insufficient development and insufficient usage of EWS. It recommends ENISA to get engaged in strategic activities in EWS by:

- **Recommendation 7:** Promote EWS as the source of important and valuable information and as a lever for other security activities in order to achieve a better level of security level (e.g. a better patch management, better internet crime investigation, better incident response, e.g.)
- **Recommendation 8:** Facilitate the dialog between the various EWS to enhance the possibility for information sharing
- **Recommendation 9**: Encourage cooperation between the potential providers of EWS
- **Recommendation 10:** Assessment of any legal issues in respect of information being exchanged by the EWS

Information Sharing

One major activity of CERTs engaged in cooperation is without doubt the exchange of information. While incident response assumes a bilateral engagement on a “need to know” basis, other services provided by CERTs involve the need for other information and data, like upcoming threats, new vulnerabilities, how to identify specific attack tools, signatures of new viruses and worms, contact information of other CERTs, etc.

It is important to understand, that information sharing is a necessary prerequisite to everything a CERT does: cooperation is not possible without it, neither is coordination, although the level of sharing and the kind of information exchanged differ significantly. The need for coordination is only small compared to the need for cooperation and basic information sharing in the fields of research, tool development and standardization efforts. The need for cooperation can be seen

to be in the middle between coordination and sharing. Examples for cooperation efforts are the establishment of knowledge pools and databases, establishing of liaisons to other communities and the development of infrastructure components as well as communication channels.

It is the opinion of the working group that the improvement of the quality of information sharing (both concerning the content, the amount and the channels) is most important, even though some experts take the position that the only key factor to quality is to cut down the amount of data (to avoid “information overflow”).

Sometimes necessary information sharing just does not take place between CERTs. This situation can only be improved if the reasons for this are fully understood. The need for “information sharing” is agreed between the CERT community and other involved players, but the definition of the term “information sharing” remains very abstract in a lot of cases. When CERTs usually discuss information sharing issues, they very fast come to a point where questions like the following are presented:

- Legal impediments
- Lack of trust
- Lack of understanding of the benefits
- Competition among entities
- Lack of preparation or prerequisites (like PGP keys, standards)
- Differences in culture, language, policies, etc.

Usually this sooner or later leads to the adjournment of the discussion. It is true that these factors have to be discussed and some of the obstacles have to be overcome. But such top-down approach makes it very difficult to achieve practical results, which of course also can act as “success stories” to foster further information sharing. In our opinion (and this has been proved useful in practice for example among the teams in the EGC) the assessment of exchanging specific types of information (like contact data or national law enforcement procedures) is much more efficient than a call for more exchange in general. This will also ease the decision of single CERTs if they want to take part in the exchange of information of a specific type.

In any case it seems important to address the whole problem – lack of information exchange and therefore lack of cooperation – in a more efficient way.

Recommendations to ENISA

The working group identified that there is a rather simple – although demanding – strategy, applicable to all cases:

1. Provide a direct application of the exchange within the context of the targeted CERTs. This will allow them to understand the benefits and relate the exchange to services provided.
2. Managing expectations to allow a realistic assessment not biased by unrealistic wishes or extreme conditions not likely to represent the major needs and cases.

Recommendation 11: We recommend that ENISA, whenever possible, communicates this way of strategy in discussions about information sharing. While this sounds rather simple, it still demands a lot of work, not all of it straight forward as it requires a very detailed understanding and insights in the day-to-day work of CERTs. ENISA should go for enhancing this understanding, and – to avoid any “not developed here” mentality – the CERT community

should be involved in that process.

Beside the more concrete recommendations given above there are some other issues the working group felt important to be considered by ENISA.

Recommendation 12: Act as a multiplier

ENISA is already acting as a positive multiplier in regard to communicating the needs and benefits for improved incident response and collaboration among CERTs and CERT communities. This role will persist and should be carried out together with the established CERT communities to avoid that different messages are sent and that the individual efforts are working towards some common goals.

Recommendation 13: Close gaps in the communication with policy makers

While especially policy makers often try to approach a particular problem in a top – down strategy, CERTs have a long history to approach things from the bottom – up. This is also responsible for the weak communication towards policy makers and the lack of management support in many cases. But beside the negative impact the bottom – up strategy has, it is very much driven by the pragmatic, hands – on perspective. CERTs are routinely dealing with new trends that are not yet addressed by the established policies and procedures. While these trends are mostly related to technology CERTs must be very flexible even in organizational approaches. We hope that ENISA can help to communicate the need for bottom – up emerging approaches and help to develop working approaches.

Recommendation 14: Facilitate the funding of projects

In order to facilitate the development of a European culture of security ENISA should take into account efforts towards this goals already made by the CERTs and their communities. We especially recommend that ENISA looks into issues of funding, which in the past have been responsible for long delays or even abandonment of projects, which often are community-driven and base on voluntary work. As CERTs have always been dealing with incidents on a very practically level, almost all their funding is associated with internal projects and service contracts to their constituencies. Funding organizations usually refuse to fund projects which do not directly provide benefit to their own interests. What they do not see is that CERTs have to interact and cooperate with other entities, and they highly depend on their input and help to be successful. The “give and take” principle has a long time tradition, especially inside the communities. So CERTs need to put resources into projects and activities that do not serve their interests alone. ENISA can help here to communicate that fact to the relevant (funding) bodies. We want to explicitly note here that we consider support for follow-up measures after successfully finalizing EU funded projects like those in the IST framework more than insufficient. Good results have been produced, but the benefits were limited to the lifetime of the projects. Only driven by the idealism of some project partners projects like eCSIRT.net still provide benefit to the CERT community even though the project was finalized.

In our opinion, one time funding of projects is not enough. Depending on the characteristics of the activities seed funding can help to overcome the fact that CERTs have no funding at all for example for the development of a common terminology for incidents and attacks. For other services, which will not succeed in securing enough business proceeds or which cannot be achieved with a commercial business model, continuous support is mandatory. Example for such service would be the TRANSITS courses, as such courses are targeting at all CERTs, explicitly including non-commercial teams that lack funding for high-priced commercial offers.

Task 4: Guidelines on establishing and training of CERTs

Introduction

Our ad-hoc working-group was asked to compile a list of guidelines on how to establish CSIRTs and similar facilities and appropriate training for CSIRT staff. The European and worldwide CSIRT community is very active in that field and prepared, over the years, lots of useful documentation.

Taking into account the very limited resources we can spend on the working-groups deliverables (most of the activity had to be spent on task 2) we compiled a list with useful URLs dealing with different areas of CSIRT development. Future work could be put into extract information from these websites and to assemble a best practice document out of it.

About CSIRTs

> The first CSIRT was set up by the US Defence Advanced Research Projects Agency (DARPA) in November 1988 after the Internet was attacked by a worm written by Robert Morris, the son of a NASA scientist. The CERT Coordination Centre (CERT/CC) is located at the Software Engineering Institute (SEI), a US federally funded research and development centre at Carnegie Mellon University in Pittsburgh, Pennsylvania. As at August 2005, there are now in excess of one hundred and eighty CSIRTs from around the world with various backgrounds including central government, Defence, academia and the commercial world.

(Extract from the State of the Practice of Computer Security Incident Response Teams[6])

A CSIRT is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Its services are usually performed for a defined constituency that could be a parent entity such as a corporation, government, or educational organization; a region or country; a research network; or a paid client.

Part of a CSIRTs function can be compared in concept to a fire department. When a fire occurs, the fire department is called into action. They go to the scene, review the damage, analyze the fire pattern, and determine the course of action to take. They then contain the fire and extinguish it. This is similar to the reactive functions of a CSIRT. A CSIRT will receive requests for assistance and reports of threats, attack, scans, misuse of resources or unauthorized access to data and information assets. They will analyze the report and determine what they think is happening and the course of action to take to mitigate the situation and resolve the problem.

Just as a fire department can be proactive by providing fire-prevention training, instructing families in the best manner to safely exit a burning building, and promoting the installation of smoke alarms and the purchase of fire escape ladders, a CSIRT may also perform a proactive role. This may include providing security awareness training, security consulting, configuration maintenance, and producing technical documents and advisories.

This document provides new, or existing, CSIRTs with a series of website URLs where detailed information can be obtained on how to create and run an operational CSIRT.

[6] http://www.cert.org/archive/pdf/03tr001.pdf

Useful URLs

Starting Point

CSIRT Starter Kit - Useful information for beginners

http://www.terena.nl/tech/task-forces/tf-csirt/starter-kit.html

Creating a CSIRT

CSIRT FAQ

http://www.cert.org/csirts/csirt_faq.html

RFC2350: Expectations for Computer Security Incident Response

http://www.rfc-archive.org/getrfc.php?rfc=2350

CSIRT Handbook

http://www.cert.org/archive/pdf/csirt-handbook.pdf

Forming an Incident Response Team

http://www.auscert.org.au/render.html?it=2252

CERT in a Box

http://www.govcert.nl/render.html?it=69

Creating a national CSIRT

http://www.cert.org/archive/pdf/NationalCSIRTs.pdf

Staffing Your CSIRT – What Basic Skills Are Needed?

http://www.cert.org/csirts/csirt-staffing.html

Organizational Models for CSIRTS

http://www.cert.org/archive/pdf/03hb001.pdf

Defining Incident Management Processes for CSIRTs

http://www.cert.org/archive/pdf/04tr015.pdf

CSIRT Mentoring Project

http://www.terena.nl/tech/task-forces/tf-csirt/mentoring.html

CSIRT Operational Issues

CSIRT Services

http://www.cert.org/csirts/services.html

CSIRT Case Classification (Example for enterprise CSIRT)

http://www.first.org/resources/guides/csirt_case_classification.html

NISCC First Responders Guide

http://www.niscc.gov.uk/niscc/docs/re-20051004-00868.pdf?lang=en

http://www.niscc.gov.uk/niscc/docs/re-20051004-00869.pdf?lang=en

Legal Issues

Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries

http://europa.eu.int/information_society/eeurope/2005/doc/all_about/csirt_handbook_v1.pdf

Guidelines for Evidence Collection and Archiving (RFC 3227)

http://www.ietf.org/rfc/rfc3227.txt

Information Sharing

WARP: Warning, Advice and Reporting Point

http://www.niscc.gov.uk/warp/

General

State of the Practice of CSIRTs

http://www.cert.org/archive/pdf/03tr001.pdf

Resources for CSIRTs

http://www.cert.org/csirts/resources.html

CSIRT information sources

European Network & Information Security Agency

http://www.enisa.eu.int

Forum of Incident Response & Security Teams (FIRST)

http://www.first.org

Asia Pacific CERTs
http://www.apcert.org/

CSIRT Trusted Introducer Scheme
http://www.trusted-introducer.nl

RFCs

RFC 3013: Recommended Internet Service Provider Security Services and Procedures
http://www.faqs.org/rfcs/rfc3013.html

RFC 2196: Site Security Handbook
http://www.faqs.org/rfcs/rfc2196.html

RFC 2828: Internet Security Glossary
http://www.faqs.org/rfcs/rfc2828.html

RFC 1983: Internet Users Glossary
http://www.faqs.org/rfcs/rfc1983.html

Training

TRANSITS
http://www.ist-transits.org/

Presecure
http://www.pre-secure.com/ir/courses/index.html

CERT/CC
http://www.sei.cmu.edu/products/courses/cert/creating-csirt.html