Agreement to join CEISNE
CEISNE model and processes

Identifier: **EISPP-D3-004-TR**

Version 1.0

Date 2003/12/17

Table of Content

GLOSSARY **3**

RELATED DOCUMENTS **4**

Applicable Documents **4**

Reference Documents **4**

1. EXECUTIVE SUMMARY **5**

2. INTRODUCTION **6**

3. THE ADVISORY CREATION PROCESS **8**

3.1. Overall workflow **8**

3.2. Detailed description of the tasks **9**

3.2.1. Watch for new vulnerabilities 9

3.2.2. Vulnerability analysis 9

3.2.3. Vulnerability Response Coordination 10

3.2.4. Create or update security advisories 10

3.2.5. Publish/disseminate security advisories 11

4. EISPP EXPERIENCES WITH CO-OPERATION **12**

4.1. Quality control and quality improvement **12**

4.2. Information exchange **14**

4.3. Re-use of advisory data **14**

4.3.1. Uncoordinated re-use of advisory data 14

4.3.2. Coordinated re-use of advisory data 16

4.4. Co-operation in monitoring new vulnerabilities **16**

5. A POSSIBLE STRUCTURE FOR CEISNE **18**

5.1. Analysis of EISPP experiences **18**

5.2. Rules and regulations for CEISNE **19**

5.3. CEISNE services roadmap **20**

5.3.1. Step 1 : Information sharing tools 20

5.3.2. Step 2 : Central advisory repository 22

5.3.3. Step 3 : Additional services 23

6. CONCLUSIONS **25**

Glossary

CSIRT	Computer Security Incident Response Team (1)
CERT	Computer Emergency Response Team (2)
EISPP	European Information Security Promotion Program
EISPP CERT	A CERT that is a member of the EISPP project .
EU	European Union
HTTP / HTTPS	Hyper Text Transport Protocol. HTTP is the default transport protocol for the Web. HTTPS is a secured version of HTTP.
IT	Information Technologies
SLA	Service Level Agreement
SME	Small and Medium Enterprise
SMTP	Simple Mail Transport Protocol. The standard protocol used to transport e-mails over Internet.
TERENA	Trans-European Research and Education Networking Association
TF-CSIRT	Task Force of CSIRTs (one of the Task-forces hosted by TERENA)
TI	Trusted Introducer : An initiative sponsored by the TF-CSIRT. (See http://www.ti.terena.nl/)
WP3	Work Package 3
XML	eXtended Markup Language

(1), (2) : In the present document, CSIRT and CERT are considered synonymous terms.

Related documents

Applicable Documents

Ref.	*Title*	*Version*	*Date*
AD01	CONTRACT No IST-2001-35200 and Annexes		
AD02	Project Consortium Agreement		
AD03	Annex 1 - Description of Work	6.0	2003/03/20

Reference Documents

Ref.	*Title*	*Version*	*Date*
RD01	EISPP Common Advisory Format Description - EISPP-D3-001-TR	1.2	

1. EXECUTIVE SUMMARY

The European Information Security Promotion Programme (**EISPP**) strives to set up a network of expertise with the aim of providing European SMEs with those IT Security services that give them the necessary trust in e-commerce to develop their businesses in that direction. EISPP is a project funded by the EU through the fifth European Framework Program within the thematic program Information Society Technologies (IST). Further information about EISPP can be found at its website, http://www.eispp.org/.

An important security service that **IT users such as SMEs have to be provided with** is **an advisory service**: security advisories supply system administrators with precise and timely information about new vulnerabilities and possible countermeasures. Such information is absolutely essential for IT security, because new vulnerabilities are discovered on a daily basis: IT systems can only be kept secure, if they are regularly upgraded or patched such that the latest security holes are closed again.

Many European CERTs produce advisories for their constituencies. Because of the ever rising number of vulnerabilities that are discovered, more and more resources have to be spent on producing advisories. In effect, similar tasks that lead to the creation of a security advisory for a given vulnerability are carried out in parallel at many CERTs. **In order to improve advisory quality and save resources** by avoiding redundant work through co-operation between CERTs, **EISPP envisions a *Co-operative European Information Security Network of Expertise*** *(CEISNE).*

EISPP has taken the following steps towards creating a basis for CERT co-operation that can be extended into CEISNE:

- Development of a standardized exchange format for advisory data,
- Creation of an infrastructure for exchanging advisory data and co-operating on advisories,
- Implementation of a half-year experimentation phase regarding co-operation between the EISPP partners on advisories.

The standardized exchange format for advisory data is defined in the public document *EISPP Common Advisory Format* [RD01].

The present document defines a road map for establishing CEISNE within the European CERT community. It draws on experiences collected in the experimentation phase, regarding both infrastructure and processes for co-operation. The road map is most likely to succeed if it can be implemented under the auspices of an already well-established association of CERTs such as TERENA TF-CSIRT.

2. INTRODUCTION

Adequate IT security is probably the most important aspect of creating a European environment in which an information society can flourish: Deficits in IT security bring risks to an otherwise desirable expansion of Internet-use by businesses and governments, deter potential home users, and generally endanger what already has become the nerve system of our critical infrastructures. The European Commission therefore has increased the importance of IT security within its new action plan eEurope 2005.

One of the most central threats to IT security is the high number of new vulnerabilities that are discovered. IT systems can only be kept secure, if they are regularly upgraded or patched such that the latest security holes are closed as soon as possible. System administrators therefore need precise and timely information about new vulnerabilities and possible countermeasures. Such information is usually provided in form of "security advisories", issued by vendors for their own products and CERTs for the products that are of interest to each CERT's constituency. Often, the information provided by vendors is the basis for security advisories issued by CERTs, which adjust the information to the specific needs of their constituency, but also other sources of information such as relevant mailing lists have to be monitored.

A troubling aspect in this context is the ever rising number of newly discovered vulnerabilities. CERT/CC, the CERT Coordination Center at Carnegie Mellon University (which takes an active role in coordinating vulnerability response), regularly issues statistics about the number of messages about potential vulnerabilities it received. In 1998, on the average CERT/CC received one announcement of a potential vulnerability per working day; in 2002, the average number had risen to 16. After analysis, communication with the vendors of affected products and processing of the gained information, over 400 warnings were published in 2002 by CERT/CC (compared to 20 warnings in 1998). Other CERTs that publish their advisories freely over the Internet (such as CIAC, a CERT within the US Department of Energy, or SecurityFocus, a commercial advisory service that makes selected information publicly available) reported additional vulnerabilities not covered by CERT/CC. All in all, the average CERT can be expected to at least struggle with the load of tracking all relevant vulnerabilities, gathering the required information, and writing security advisories for its constituency.

In June 2002, EISPP (*European Information Security Promotion Programme),* a project funded by the EU through the fifth European Framework Program within the thematic program Information Society Technologies (IST), was established. The aim of EISPP is to set up a network of expertise with the aim of providing European SMEs with those IT Security services that gives them the necessary trust in e-commerce. Because an advisory service that provides SMEs with relevant security information was identified as fundamental to all additional security services SMEs might be interested into, one work package (WP 3) within EISPP was tasked to work towards a *Co-operative European Information Security Network of Expertise (CEISNE).* This network should enable participating CERTs to co-operate on security advisories. The basic assumption is, that in the long run, CERTs will only be able to keep up with the rising number of vulnerabilities by sharing the work load in producing security advisories through effective co-operation.

EISPP has taken the following steps to establish a basis on which CEISNE can be built:

- **Development of a standardized exchange format for advisory data**

  A common format for exchanging security advisories has been defined by EISPP (see [RD1]), based on compiled best practice information of EISPP CERTs and otherwise available best practice information. The EISPP advisory format was adopted by all EISPP CERTs and has been in productive use since March 2003.

- **Creation of an infrastructure for advisory exchange and co-operation**

  Using the EISPP advisory formats, the EISPP CERTs exchange all issued advisories. In effect, a distributed repository, where each CERT maintains a local advisory database both of its own advisories and the advisories of the other EISPP CERTs was established. This decentralized model was adopted first to avoid the "single point of failure" associated with any centralized site containing all the advisories from all the CERTs. While that decentralized model did work perfectly to circulate and store the advisories, it also reached its limits with respect to implementing essential support for CERT co-operation. As will be shown below, a more centralized infrastructure needs to be implemented for CEISNE.

- **Implementation of a half-year experimentation phase regarding co-operation**

  During the experimentation phase, various co-operation models where defined and experimented with. The experimentation focused on quality control and quality improvement for advisories, information exchange about vulnerabilities, re-use of advisory data, and co-operation in monitoring new vulnerabilities At the same time, feedback from European CERTs about their ideas and expectations regarding CERT co-operation was collected.

This document presents a road map for establishing CEISNE within the European CERT community. After a brief introduction to the advisory creation process in Section 3, the experiences regarding both the supporting infrastructure and possible models for CERT co-operation are summed up in Section 4. These experiences form the basis for recommendations regarding the establishment of CEISNE as presented in Section 5.

The two central results of the experimentation phase that shape the roadmap are:

1. Co-operation between CERTs on advisories that actually saves resources by sharing the workload cannot be reached in one step by interfacing a small number of CERTs (see Section 4.3.2). Such co-operation must rather grow step by step, starting with the establishment of information sharing about vulnerabilities and advisory data between a significant number of CERTs.
2. Co-operation between CERTs on advisories must be supported by adequate tools, which only can be supplied and maintained centrally.

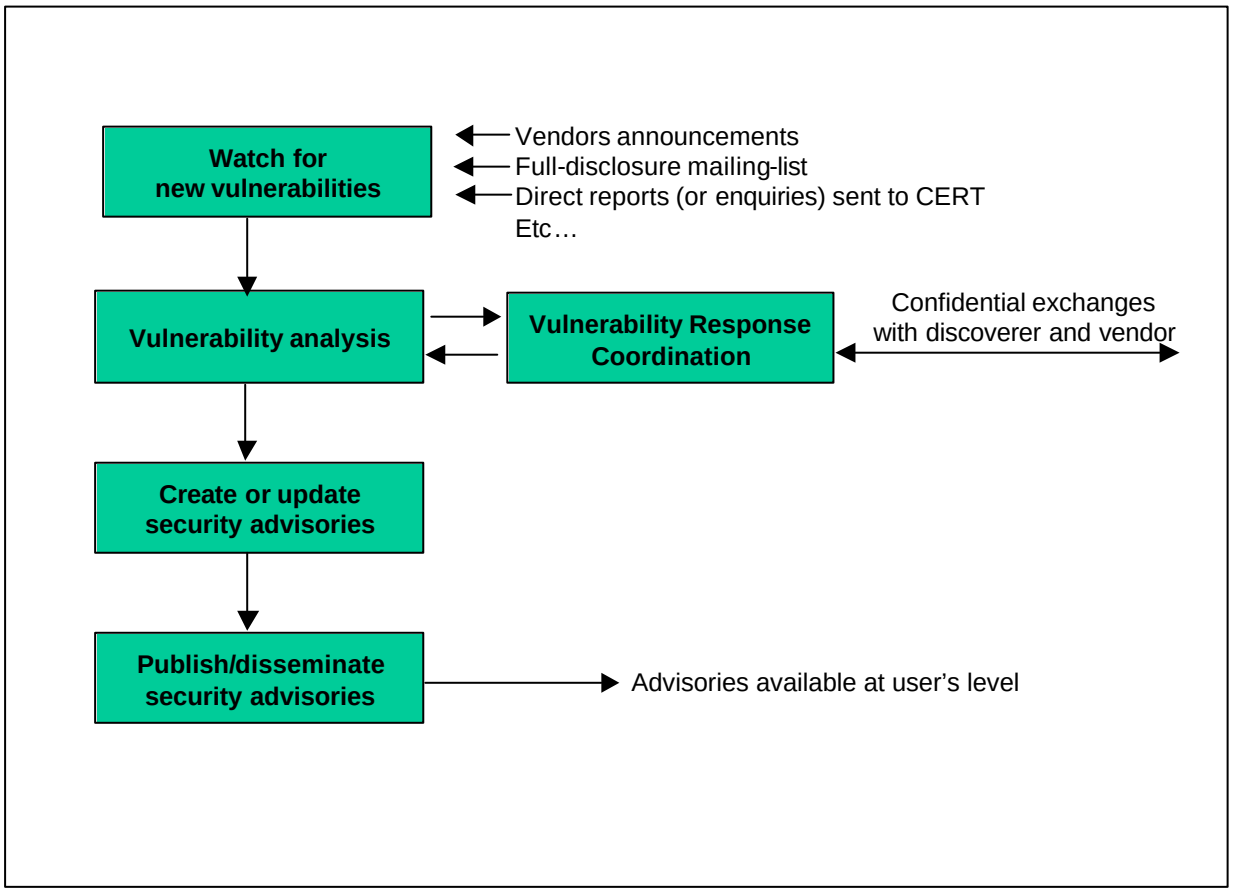
As a consequence, CEISNE must be created under the auspices of an already well-established association of CERTs such as TERENA TF-CSIRT, through which both a significant number of CERTs can be reached and central tools and services can be provided.

3. THE ADVISORY CREATION PROCESS

An advisory released by a CERT is the output of a process that starts with identifying a new vulnerability and culminates with distributing the advisory to the end users. As further information becomes available, updates of an advisory may be required. Modeling the advisory creation process is a good starting point for identifying activities that could benefit from co-operation between CERTs. This is the purpose of the present chapter.

3.1. Overall workflow

The following diagram shows the major tasks and dependencies between these tasks. Details are provided in the next chapter.



3.2. Detailed description of the tasks

3.2.1. Watch for new vulnerabilities

Task objectives

New information regarding vulnerabilities is made public day after day. It is therefore imperative for a CERT to

- become aware of new vulnerabilities that may be of concern to its constituency in a timely fashion.
- monitor the development of vulnerabilities for which the CERT already has published an advisory in case an update of the advisory in question becomes necessary.

Task description

Activities in this task can be split into two main categories: (1) information gathering and (2) information analysis. For information gathering, various sources of information have to be monitored. Typical sources include:

- Vendors' security announcements
- Security advisories released by other bodies (e.g., other CERTs)
- Open mailing lists or forums (e.g., full disclosure mailing lists)
- Closed mailing lists (e.g., mailing lists restricted to members of some CERT forum)

Depending on the role of the CERT, information directly addressed to the organization, such as a user report about a possible flaw within some product, may also play an important role.

Information gathering must be combined with information analysis, so as to

- discard the information that is not relevant (e.g. a vulnerability impacting a product the CERTs constituency does not use),
- maintain a list of pieces of information that needs to be completed before a decision can be taken (e.g., wait for corroboration of information that comes from an unknown or possible untrustworthy source)
- maintain a list of reports that require an action on part of the CERT, e.g., an analysis of a reported vulnerability or updating an already published advisory.

3.2.2. Vulnerability analysis

Task objectives

In order to react properly to a new vulnerability or new information about an older vulnerability, a CERT must

- understand the vulnerability.
- assess the risk associated with the vulnerability
- if possible, identify solutions or workarounds

Task description

This task is the core activity for an advisory service, although the depth of the analysis that is performed depends much on the service level the CERT has to provide to its constituency. In the simplest case, information is basically only forwarded, in which case the CERT may do nothing more than perform a very rough risk assessment on a uniform scale, express information about the

affected systems in a uniform schema, etc. For providing a high service level, on the other hand, a detailed analysis of the vulnerability, extensive tests of patches, etc., may be necessary. Especially for high service levels, a prioritization usually will be necessary so that high-risk vulnerabilities are treated first; risk assessment therefore usually is the very first sub task to be performed during vulnerability analysis.

Frequent sub tasks performed during the vulnerability analysis are:

- risk assessment
- collection of additional information about the vulnerability
- analysis of the vulnerability based on the collected information, i.e. without testing it
- test of the vulnerability
- analysis/test/design of a workaround/solution for the vulnerability
- test of patches for the vulnerability

3.2.3. Vulnerability Response Coordination

Task objectives

To coordinate the various steps necessary in responding a newly discovered vulnerability such as analyzing the vulnerability, finding solutions, notifying the public, etc.

Task description

If a CERT discovers a new vulnerability or is notified about a possible vulnerability that is not publicly known yet, it may chose to act as a coordinator of the vulnerability response. The first action that needs to be coordinated is when the vulnerability should be made public; this usually involves mediation between the discoverer of the vulnerability and the vendor of the affected product. If more than one vendor is affected by the vulnerability, additionally the actions of the vendors need to be coordinated.

Because the decisions that have to be taken when coordinating vulnerability response may have a significant impact – economical and otherwise – a well defined policy regulating the coordination process must exist. Such a policy should, for example, define a notification phase (in which the vendor is informed about the vulnerability) and a grace period (a delay given to the vendor to react and to propose a solution to the vulnerability).

Because vulnerability response coordination deals with highly sensitive information and is of a very political nature, co-operation between CERTs in this field was not perceived as the primary focus of the EISPP project.

3.2.4. Create or update security advisories

Task objectives

To create/update a security advisory that is tailored to the specific needs of the CERT's constituency.

Task description

Information about a vulnerability – acquired by information gathering and vulnerability analysis – that is relevant to the CERT's constituency must be presented in such a way that readers of the

advisory can respond to the new vulnerability both effectively and efficiently. Every security advisory therefore has to be authored with an eye to the intended audience. If relevant new information becomes available about a vulnerability for which an advisory already has been issued, that advisory needs to be updated in some way.

Several best-practice descriptions regarding the contents of security advisories are available; the process of how an advisory is created, which means of quality control are employed, etc., depends on the processes and tools within each CERT. Also, the advisory release policy usually varies from one CERT to the other; for example, some CERTs release advisories even if no reliable solution or workaround is available, while others only issue advisories once an effective counter measure has been found.

3.2.5. Publish/disseminate security advisories

Task objectives

For a security advisory to have an effect on information security, a CERT

- must insure that the advisories produced reach the constituency
- should, if necessary, provide further assistance to the constituency

Task description

This final task deals with making advisories available to the CERT's constituency. Usual means of dissemination are mailing lists and/or publication via a web server. Often, dissemination is based on the definition and maintenance of user profiles (usually based on lists of relevant products): thus, the number of security advisories can be decreased by filtering out advisories that clearly are of no interest to a given user.

Any additional service that aides the constituency to carry out the measures described in a security advisory (e.g., providing a local mirror of relevant patches or providing a help-desk service) could also be included in this task.

4. EISPP EXPERIENCES WITH CO-OPERATION

In this chapter we summarize the main experiences and conclusions drawn from an experimentation phase regarding CERT co-operation carried out during the EISPP project. Basis for the co-operation between the EISPP CERTs was the exchange of advisory data using the EISPP advisory format: whenever an EISPP CERT publishes an advisory, the XML data advisory data is sent to the other EISPP CERTs, which then integrate the advisory data into their advisory database. In effect, each EISPP CERT maintains a database of all advisories published within EISPP. This decentralized approach was preferred over the obvious alternative – a central database server on which all EISPP advisories are stored – for the following reasons:

- Using a central server creates a "single point of failure" – if the server is down, the EISPP co-operation comes to a halt.
- In order to avoid a single point of failure, EISPP CERTs must store all advisory data also locally, in effect making the central server redundant.

As the experimentation phase has shown, a central server would have been helpful not so much for providing access to advisory data, but for hosting tools supporting the co-operation; the importance of proper tool support for CERT co-operation that ties into the CERT-internal processes is one of the most important results of the experimentation phase.

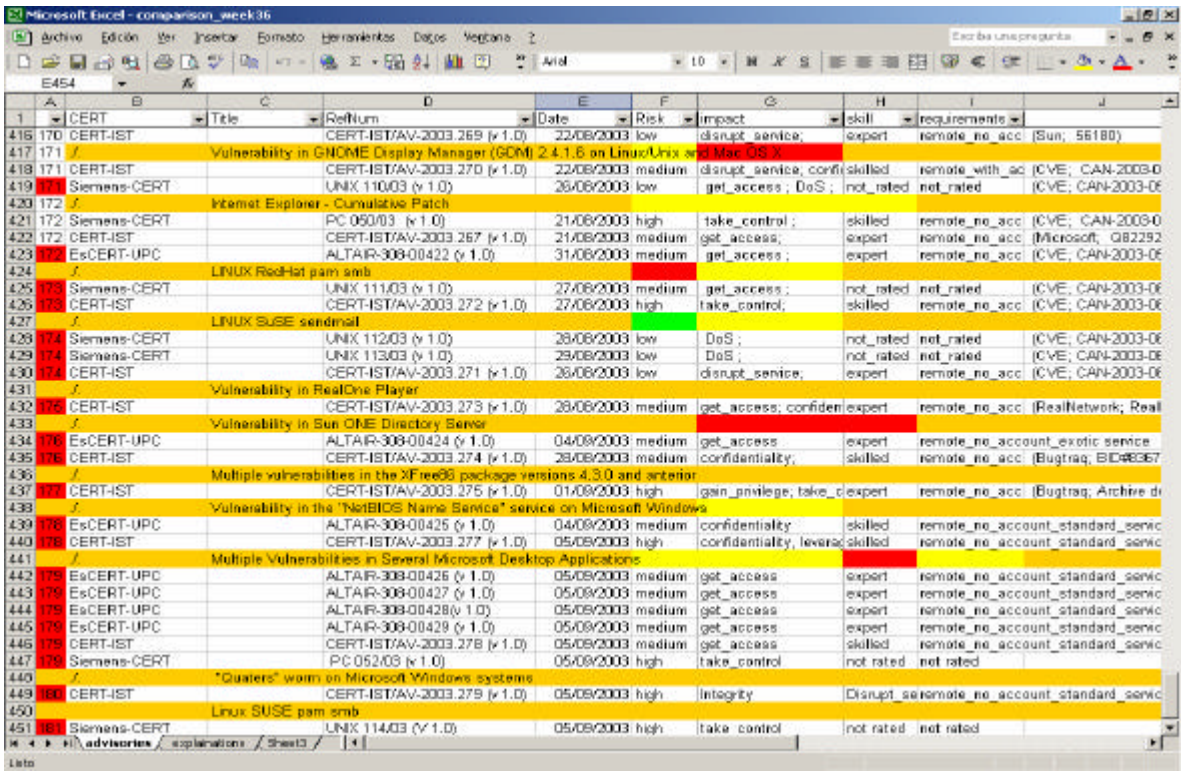
4.1. Quality control and quality improvement

The first use of the exchanged advisory data was for quality control and quality improvement regarding each CERT's own advisories. In concrete:

- Advisories published about the same vulnerability by other CERTs can be used to check the contents of one's own advisory.
- Especially helpful in this context is the use of a common schema for assessing vulnerabilities as defined by the EISPP advisory format: Ideally, all CERTs should arrive at a similar rating, since the same process is used. Significant differences in the rating of the same vulnerability therefore point to different perceptions that are worth investigating. This investigation, usually in form of a discussion between the EISPP CERTs, is supported by the common rating schema, as it provides a common language for talking about vulnerabilities.
- Apart from examining the contents of an advisory, already the mere fact that an advisory regarding a certain vulnerability is published by one or more of the other EISPP CERTs provides useful information: a CERT may be pointed to an important vulnerability that it missed for some reason.
- Similarly, the absence of new advisories tells a CERT at least for those systems supported by several of the EISPP CERTs, that no relevant issue has been missed

The main finding in using the exchanged advisory data for quality control and quality improvement was that **a tool that provides an overview of the exchanged advisories is absolutely essential**. Without such a tool, already the advisory data of only four CERTs can become too much to handle: advisories *must* be grouped according to the vulnerabilities that are covered. With the EISPP advisory format, at least semi-automated grouping becomes possible, because references to standard vulnerability identifiers and relevant sources such as vendor advisories are given in a standardized form. Within a group of advisories, differences regarding the vulnerability rating can be highlighted so as to focus the attention of the reader on possible trouble spots.

Lacking a central server to host such a tool, the EISPP CERTs carried out experiments with a spreadsheet in which advisory groups and differences regarding the vulnerability rating were displayed. Using an XSLT stylesheet, the relevant data were imported from the advisory XML data into the spreadsheet (see figure); then, on a weekly basis, the entries were grouped and notable differences highlighted. The resulting sheet could then be used, for example, as a basis for discussion of vulnerability ratings.



Spreadsheet with overview of EISPP advisories (grouped by issue, differences w.r.t. the vulnerability rating highlighted)

Obviously, maintaining a spreadsheet by hand is not a feasible basis for CERT co-operation. While each CERT involved in the co-operation could implement such a tool locally for its own database, **providing such a tool via central server is the better approach**: it guarantees that all the participants use the same baseline when discuting on advisories and saves resources by maintaining only one common information base.

During the experimentation phase, when discussing different vulnerability ratings, the rating schema used in V1.2 of the EISPP format was found to be in need of improvement: both factual data regarding a vulnerability, on which all CERTs should agree, and constituency dependent data that may differ from CERT to CERT was used as a basis for rating vulnerabilities. At time of writing, the EISPP format is undergoing a revision; version 1.3 will feature a new, improved rating schema.

Especially, but not exclusively, for investigating different vulnerability assessments, communication in addition to the exchange of advisory data was necessary. Various means of information exchange that were employed within EISPP are treated in the following section.

4.2. Information exchange

When starting the co-operation, a mailing list was set up as a means for exchanging information during the experimentation phase. Any kind of information was to be exchanged via this list – in the beginning, the EISPP CERTs primarily expected

- discussions about current advisories, e.g., differences between the EISPP CERTs in rating a vulnerability (see Section 4.1)
- questions and answers, for example about newly discovered vulnerabilities
- information, for example about newly discovered vulnerabilities, provided *without* having been prompted by a preceding question on the mailing list

Should a single mailing list prove to be insufficient for information exchange, e.g., because of a lack of structure, other options were to be explored.

The mailing list has proved to be moderately useful in the sense that (1) discussions about different vulnerability ratings took place and (2) some of the questions asked by one CERT could indeed be answered by one of the other EISPP CERTs; information not requested in advance, however, was rarely posted.

Experimentation regarding information exchange between CERT members was hampered by the small number of CERTs participating within EISPP. With only four CERTs, the chance that a question asked by one of the CERTs can be answered by another CERT is relatively low. Similarly, there is little motivation for members of one CERT to post unrequested but possibly useful information on the mailing list, as the information will only reach a small readership. All in all, the experimentation phase showed that for information exchange, a certain critical mass has to be reached. For this reason, further experiments within the EISPP project, for example with different tools such as bulletin boards, Wiki systems, etc., did not make sense: the value of such tools can only be accessed once a certain volume of information is exchanged via these tools.

4.3. Re-use of advisory data

As mentioned above, the exchange of advisory data between the EISPP CERTs provided a basis for quality control and quality improvement of advisories. As a further step of co-operation, the EISPP partners envisioned to share the workload of writing advisories by re-using advisory data. The experiences made with respect to re-use can be divided into *uncoordinated* and *coordinated* re-use:

- *Re-use of advisory data* means that a CERT imports parts of advisories or complete advisories taken from the pool of exchanged advisory data and – probably after carrying out some modifications – issues its own advisory based on this data.
- *Coordinated* re-use means that processes and rules have been defined by which re-use is regulated such that regular re-use of advisory data can be practiced.
- *Uncoordinated* re-use takes place in the absence of such rules and thus can only be regarded as "good luck" for the CERT that manages to save some work because it happens to find re-usable material in the exchanged advisory data.

4.3.1. Uncoordinated re-use of advisory data

Uncoordinated re-use of advisory data was possible right from the start of the advisory exchange practiced within EISPP.

It must be noted that (1) the re-use was limited to advisory parts, and (2) re-use of advisory parts did not occur as frequently as had been expected when the project started. The following reasons were identified:

The re-use was limited to advisory parts mostly because, even though all EISPP CERTs used a standard advisory format, **there are still significant differences between the advisory styles of these CERTs**. For example, between the EISPP CERTs, the following differences were noted:

- *Concise vs. detailed* While Siemens CERT prefers very concise vulnerability descriptions, CERT IST tends to write very detailed descriptions; the level of detail in esCERT's advisories usually is somewhere between that of Siemens CERT and CERT IST.
  Consider the NFS vulnerability CAN-2003-0252 as an example. In the following, the information given by each CERT in the respective advisory is reproduced. Because the EISPP advisory format provides several description fields that distinguish between the description per se, background information, technical information, etc., the entries of all relevant fields are listed.
  - Siemens CERT writes in advisory *Siemens CERT/UNIX 103/03*:
    "There are vulnerabilities in rpc.mountd, which can be remotely exploited to perform an DoS attack." (in advisory field `description`)
  - esCERT writes in advisory *esCERT/ALTAIR-307-00399*:
    "The logging code in nfs-utils contains an off-by-one buffer overrun when adding a newline to the string being logged. This vulnerability may allow an attacker to execute arbitrary code or cause a denial of service condition by sending certain RPC requests." (in advisory field `description`)
  - CERT IST writes in advisory *CERT-IST/AV-2003.219*:
    "A vulnerability has been discovered in the "nfs-utils" package on Linux. It allows a remote attacker to crash the system, or possibly to execute malicious operations on the system." (in advisory field `description`)
    The "nfs-utils" package provides a daemon for the NFS (Network File System) server on Linux. The "rpc.mountd" RPC service implements the server side of the NFS protocol. (in advisory field `technical_context`)
    The vulnerability discovered is a buffer overflow in the logging function of the "rpc.mountd" RPC service of the "nfs-utils" package. It allows a remote attacker, by sending specific RPC requests to the "mountd" service, to cause a denial of service, or to execute arbitrary code on the system." (in advisory field `technical_description`)
- *Treatment of new information* While Siemens CERT treats essential new information regarding a vulnerability for which an advisory already exists by creating a new advisory (along with the information that it supersedes the older one), CERT IST and esCERT re-issue an updated version of the original advisory
- *Handling of patch information* While Siemens CERT mirrors all patches locally and provides an explicit link to each of them, CERT-IST and esCERT do not mirror patches and usually provide only a link to the web page on which the vendor publishes all relevant patches.

It is clear that differences in the advisory style limit the possibilities for re-use of larger parts of an advisory or even the whole advisory. One can observe, though, that the re-use of advisory parts is supported well by the EISPP advisory format; especially the division of the description field in the EISPP advisory format supports re-use by adding structure to the free text information within the advisory. Indeed, **reuse of partial advisories occurred several times during the experimentation phase**, mainly when a CERT already had received the advisory from another EISPP CERT before starting to write an advisory about the same issue. Because Cert-IST releases very detailed advisories, its advisories were the ones the most re-used by other CERTs. For example, esCERT reused the information within the field `description` from CERT-IST's advisories CERT-IST/AV-2003.365 and CERT-IST/AV-2003.375 in its advisories ALTAIR-312-00516 and ALTAIR-312-00524, respectively. The fields `technical context` and `technical description` that CERT-IST also had filled in, on the other hand, were not carried over.

That advisory parts were not re-used more frequently is due to the lack of proper tool support; when the experimentation phase started, none of the authoring tools was mature enough to import XML-advisories to easy manipulation. If re-use has to be managed with "copy" and "paste" out of the XML source, chances are that the advisory author will not even bother to check for re-usable material. **Had the tools been more mature from the very start of the project,** the EISPP CERTs are confident that **a significant amount of uncoordinated re-use of advisory parts would have occurred** during the experimentation phase.

4.3.2. Coordinated re-use of advisory data

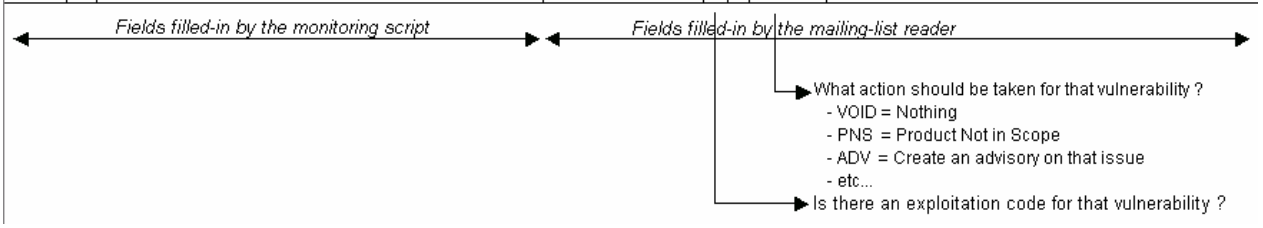
Significant work-load sharing for authoring advisories is only possible through coordinated re-use of advisory data: two or more CERTs have to agree on processes that regulate which advisory is written by which CERT, so that on one hand, no superfluous work is done in parallel, but on the other hand all relevant vulnerabilities are treated in a timely fashion. The differences in advisory style noted in the previous sections already explain one of the big obstacles to coordinated re-use of advisory data encountered during the EISPP project: because of the large differences between the advisory styles of the EISPP CERTs, re-use on a large scale was out of the question. When putting this technical problem aside and concentrating on possible processes for dividing the work of authoring advisories between CERTs, the EISPP CERTs further realized the difficulties involved in defining proper rules and regulations for coordinated re-use: CERTs usually are bound to a certain service level, e.g. through a service-level agreement(SLA), regarding the issued advisories and may even be liable for late, missing or wrong information disseminated through advisories. **The coordinated re-use of advisory data therefore is only thinkable between CERTs that not only fit to each other in terms of advisory style and SLA, but also know each other well and trust each other**. Furthermore, **rules that regulate coordinated re-use can only be established bilaterally between CERTs**.

4.4. Co-operation in monitoring new vulnerabilities

Because coordinated reuse of advisory data proved to be difficult to implement, the EISPP CERTs decided to also experiment with other cooperation schemes, to share the workload required to produce advisories. Based on the model defined for the advisory creation process (see Section 3), it was decided to experiment with cooperation on the "watch for new vulnerabilities" task, and more precisely to experiment with jointly monitoring a relevant mailing-list.

The experiment was made on the "Bugtraq" mailing-list. As a first step, to establish a common view on that mailing-list, a "daily summary" of the new vulnerabilities published in the mailing-list was sent by email each morning to all the EISPP CERTs. An example of such a summary is shown below.

Mailing-L	Nbr	Subject	Affected product	xe(	(pl	Status	Comment
Bugtraq	1	ANNOUNCE: New mailing list for secure application development, SC-L	NA	N		VOID	
Bugtraq	1	Cutenews 1.3 information disclosure	Cutenews 1.3	N		PNS	
Bugtraq	1	GNU screen buffer overflow	GNU screen	N		PNS	
Bugtraq	1	Jason Maloney's CGI Guestbook Remote Command Execution Vulnerability.	Jason Maloney's CGI guestbook	Y		PNS	
Bugtraq	**1**	**MDKSA-2003:110 - Updated kernel packages fix vulnerability**	**Linux kernel**	**Y**		**ADV**	
Bugtraq	1	Multiple Remote Issues in Applied Watch IDS Suite (advisory attached)	Applied Watch IDS Suite	N		PNS	
Bugtraq	1	Remote execution in My_eGallery	My_eGallery	N		PNS	
Bugtraq	1	Surfboard <= 1.1.8 vulns	Surboard webserver	Y		PNS	
Bugtraq	1	TSLSA-2003-0046 - kernel	Linux kernel	Y		PNS	
Bugtraq	1	Virtual Programming VP-ASP Shopping Cart 5.0 multiple SQL Injection Vulnerabilities	VP-ASP Shopping Cart 5.0	N		PNS	
Bugtraq	1	[ANNOUNCE] glibc heap protection patch	glibc	N		VOID	
Bugtraq	**1**	**[Full-Disclosure] [SECURITY] [DSA-403-1] userland can access Linux kernel memory**	**Linux kernel**	**Y**		**ADV**	
Bugtraq	1	phpBB 2.06 search.php SQL injection	phpBB 2.06	N		PNS	
Bugtraq	1	where to discuss common criteria issues?	NA	N		VOID	



Example of a "Daily summary" of the new vulnerabilities posted in "Bugtraq" mailing-list. The 3 first columns are automatically generated by a script, while the others are filled manually by the people who read the mailing-list emails.

The experiment's main results were the following :

- For CERTs to cooperate on a given task, a common agreement must be first established on the process adopted to perform that task. Because each CERT has its own internal organisation (e.g. a single full-time dedicated person in charge of the monitoring, versus several product oriented persons performing the monitoring in parrallel), it is difficult to establish that common process. Getting an agreement on only the process outputs (e.g. the "status" affected to each mailing-list email) is also difficult to reach.

- Once that process has been established, it is not necessary that all CERTs perform the same task in parallel; instead, some CERTs could rely on the results produced by the others CERTs. To avoid possible errors, though, some redundancy probably must be maintained (for example, there could be always two CERTs that monitor the same mailing list on a given day), and a mechanism must be in place to compare the results.

- **To be successful, a process designed to enable collaboration between CERTs must be integrated into each CERT's workflow such that the collaboration aspect requires little or no extra work over the CERT's internal processes.** On a long term perspective, a CERT can only spend limited resources to produce "collaboration compliant" outputs. A CERT has a strong incentive to use a collaborative process (or tool) if that process/tool helps it to carry out its regular activities. The fact that such a process also enables collaboration between CERTs must be an additional capability that requires little or no extra work for the participating CERTs.

- Sharing workload between several CERTs raises issues regarding trust, service-level, liability, etc. These questions cannot be answered in general terms (e.g. in an agreement defined at the CEISNE level) but must be agreed upon between CERTs that fit to each other (bi/multilateral agreements).

5. A POSSIBLE STRUCTURE FOR CEISNE

Based on the experience gained from experimenting with cooperation on security advisories, the EISPP project has designed a blueprint for a Co-operative European Information Security Network of Expertise (CEISNE). This network should become the infrastructure for cooperation between European CERTs in the field of security advisories. CEISNE is not envisioned as an organisation on top of existing CERTs, but rather a set of procedures and services that helps existing CERTs to work together.

- Section 5.1 sums up the experiences collected in EISPP and draw conclusions regarding the establishment of CEISNE.
- Section 5.2 suggests policies and regulations required to run CEISNE.
- Section 5.3 explains the services that define CEISNE, each service targeting a particular aspect of the cooperation between CERTs; also a roadmap is presented of how CEISNE can be implement gradually, from the very basic immediate needs toward additional aspect that should be covered later.

5.1. Analysis of EISPP experiences

From the experimentations performed, EISPP learned the following key points:

- Close co-operation in the later stages of the advisory creation process require a similar advisory style , detailed rules that regulate the co-operation, and – last, but not least – a high degree of trust between the co-operating CERTs.
- Co-operation between CERTs in the early stages of advisory creation is mostly about information exchange.
  - The regular exchange of advisory data supports mostly quality control and quality improvement.
  - Sharing the workload of advisory creation in its early stages can be achieved through unstructured information exchange, e.g., via mailing lists.
  - Further workload sharing can be achieved through structured information exchange or, rather, joint maintenance of information, e.g., on monitoring mailing lists.
- For substantial information exchange between CERTs, a "critical mass" of participating CERTs must be reached.
- Adequate tools that support co-operation have to be in place

As a consequence, CEISNE can only be a facilitator for CERT co-operation and needs to focus in the beginning on the first stages in the advisory creation process such as information exchange and quality control. CEISNE therefore should start by promoting information exchange between a large number of CERTs. Later, using CEISNE as a 'market place' to find co-operation partners, smaller groups of CERTs that fit to each other can move towards closer co-operation – with the already existing CEISNE services and the EISPP Common Advisory Format as a well-established basis.,

Because proper tools support can best be provided via a central server and because a certain amount of administration will be necessary for keeping CEISNE running in a smooth way, CEISNE requires some sort of central organization. Building yet another organization from scratch, however, is neither desirable nor realistic. Therefore, CEISNE should be implemented under the auspices of

an already well-established association of CERTs such as TERENA TF-CSIRT or rather the Trusted Introducer TI, which is run by TERENA.

Making CEISNE part of the Trusted Introducer also has advantages with respect to the rules and regulations required for running CEISNE, as the following section shows.

5.2. Rules and regulations for CEISNE

Membership in an organization like CEISNE cannot be open to every organization: steps must be taken to insure that (1) only organizations with a certain level of competence can join and (2) CEISNE members can be trusted not to abuse the facilities of CEISNE. Therefore, CEISNE must define requirements for joining CEISNE and a code of conduct regulating the way CEISNE and the information exchanged via CEISNE is used.

With respect to the requirements for joining CEISNE, an already existing process for CERT accreditation such as that provided by the Trusted Introducer, TI, should be used. Optionally, additional measure can be defined, e.g., that a new CEISNE member be recommended by a certain number of CEISNE members.

Regarding the code of conduct, the easiest way to establish a proper code of conduct – once CEISNE has been defined – would be to adapt one of the codes of conduct already in use within the CERT community (e.g., the code of conduct of German CERT Association or the eCSIRT.net project) to the special needs of CEISNE.

5.3. CEISNE services roadmap

As mentioned above, CEISNE can only be a facilitator for CERT co-operation and needs to focus in the beginning on the first stages in the advisory creation process such as information exchange and quality control. For this, CEISNE must establish and run certain services through which CEISNE members can co-operate. Because co-operation between CERTs must be built up gradually, the CEISNE service can also be implemented gradually.

- As a first step, CEISNE must implement the "Information sharing tools" service to support information exchange on a broad basis. This service is a pre-requisite and must be available when CEISNE starts to operate. (Section 5.3.1)
- As a second stage, CEISNE must offer its members a way to exchange advisory data through the "Central advisory repository" service. (Section 5.3.2).
- Information sharing tools and a central advisory repository are absolutely essential to establish CEISNE as a network of expertise regarding security advisories. For closer co-operation, additional services will be necessary. (Section 5.3.3)

5.3.1. Step 1 : Information sharing tools

The suggestions regarding tools and processes for information sharing within CEISNE are based on lessons learnt from experimentation as well discussions between the EISPP CERTs and general experiences with information sharing tools.

The value of information exchange was demonstrated within the EISPP project; also feedback from other CERTs collected, for example, during the CERT workshop organized by EISPP, indicated that information exchange between CERTs is seen as a top priority for closer CERT co-operation.

In the following, three possible ways of sharing information are discussed.

- Information exchange via mailing lists

  The provision of a mailing list dedicated to the discussion of vulnerabilities and counter measures seems a reasonable first step for CEISNE:

  - There is widespread use of mailing lists as a means for information exchange within the CERT community, i.e., mailing lists are accepted as a means of information exchange.
  - Mailing list technology is relatively simple and easily deployed. (An important caveat regarding simplicity is encryption, which will be necessary to insure confidentiality. CEISNE can, however, build upon experiences collected by organizations/projects such as FIRST and eCSIRT.net. The approach of eCSIRT.net is especially interesting: a list server that encrypts each message individually for every participant of the mailing list is used.)
  - Mailing lists follow the 'push' paradigm, i.e., new information is brought to each member rather than having to be collected. New information, questions, etc., are therefore brought to the attention of the recipients in a timely fashion.

  However, mailing lists also have considerable weak points:

  - There is no possibility to focus on information that really interests one (discussion threads somewhat but offer, of course, only limited possibilities).
  - Searching for relevant items/mails is not easy.
  - Information is often scattered over various emails.
  - No maintenance of information is possible.

- Information exchange using dedicated, structured tools

  Because of the drawbacks of mailing lists above, a more structured approach should be considered for information sharing within well-defined areas such as vulnerability information:

  - It may be possible to configure standard tools such as a bulletin board system or bug-tracking tool ("vulnerability tracking" instead of "bug tracking")
  - A tool that allows to structure information has the chance to be accepted as a useful tool to store information for later retrieval. Such a tool might thus be used for information collection/maintenance that occurs as part of the daily work at a CERT. As the experimentation phase within the EISPP project showed, information sharing works significantly better, if providing information is not perceived as an additional task but as directly useful for the CERT's own work such that the "sharing" aspect is merely a side effect of information collection/maintenance for oneself.

  At time of writing, there are plans within the German CERT community to establish a shared vulnerability database; developments in this area should be closely monitored by CEISNE.)

- Information exchange using a WIKI system

  Dedicated tools resolve the inherent problem of mailing lists regarding structure. However, structure can only be enforced for well-defined areas such as information sharing regarding vulnerability information; for 'spontaneous' co-operation on some topic of interest or co-operation regarding information with less structure, a general purpose tool for collaboration could be useful within CEISNE. Several of the EISPP CERTs have made good experiences with so-called Wiki tools.To cite a frequently used definition of a WIKI system:

  > *Wiki is a piece of server software that allows users to freely create and edit Web page content using any Web browser. Wiki supports hyperlinks and has a simple text syntax for creating new pages and crosslinks between internal pages on the fly.*
  >
  > *Wiki is unusual among group communication mechanisms in that it allows the organization of contributions to be edited in addition to the content itself.*

  A Wiki system would offer CEISNE an easy-to-use tool not only for sharing but for jointly editing and maintaining information. Both short-term and long-term co-operation projects could be conducted using the Wiki. Consider, for example, collection of best practice information, which, depending on what type of best practice information is collected, might either be a short-term or a long-term project:

  - During the the BLASTER worm incident, many CERTs were compiling best practice information for containing the worm. Had a Wiki system been available, then one CERT could have posted a first draft of best practices to be checked and augmented by other CERTs.
  - A project of collecting best practice information regarding forensic analysis could be carried out as a long term project via a CEISNE Wiki.

All in all, CEISNE should start operations offering both a mailing list and a Wiki system. While the mailing list offers an established, ready to use medium for sharing information, the Wiki system can be used both to consolidate important information collected via the mailing list and to experiment with new forms of co-operation. Lessons learnt both from using the mailing list and using the Wiki may then provide a basis for designing dedicated tools for information exchange and further co-operation.

While information sharing using the tools described in this section probably will take some time to get started, the exchange of considerable amounts of valuable information can be organized in a relatively short time through a central advisory repository as described in the following section.

5.3.2. Step 2 : Central advisory repository

One of the central services of CEISNE must be a central advisory repository, through which CEISNE members can make their advisories – or parts of them – available to other CEISNE members. The service should consist of two components: (1) an overview of the advisories published by all member CERTs and (2) access (partial or complete) to the published advisories. The EISPP common advisory format is the enabling technology for providing a useful overview:

- If standard vulnerability identifiers and vendor advisories are referenced in accordance with the EISPP advisory format, then an automated grouping of advisories regarding the treated vulnerabilities can be carried out. As the EISPP CERTs found during the experimentation period, collecting advisories without support for grouping, adds little value, because one quickly loses the overview.
- If the vulnerability classification scheme of the EISPP advisory format is used, then risk assessments made by various CERTs with respect to the same vulnerability become comparable. As the EISPP CERTs found during the experimentation phase, comparing risk assessments for new vulnerabilities is extremely useful for quality control

There are two obvious problems with respect to the central advisory repository:

- As it should be expected that some CEISNE members will not use the common format, measures must be taken to insure that the advisories of these organizations can at least be integrated partly into the central advisory repository. This means that for advisories not published in the EISPP format, at least the minimum data necessary for the functioning of the central advisory repository must be converted to the EISPP format:
    - For the identification data (i.e., reference number) and advisory title, this conversion process obviously is straightforward.
    - Additionally, proprietary risk ratings should be mapped on the EISPP scheme in order to make the risk rating comparable.
    - References to standard vulnerability IDs and vendor advisories must be given in an EISPP-compatible format to support automated grouping.
- For commercial CERTs, it will not always be possible to publish their complete advisories within CEISNE, because one of their competitors may be a member of CEISNE, as well. Therefore, it must be possible to publish advisories only partly, possibly with the option to publish the whole advisory after a certain period. It should, however, be obligatory to publish at least the data described above for CEISNE members not using the EISPP advisory format: the fact that an advisory has been published, which vulnerability it refers to, and what the risk rating is must be communicated via the central advisory repository. (Wellfounded exception from this rule may be made, e.g., in case the advisory of a company CERT treats sensitive information about the company's policies or IT infrastructure.)

The central advisory repository is a cornerstone of CEISNE, because it automates the exchange of structured information useful to all CEISNE members. Furthermore, the repository is the basis for every initiative to closer co-operation regarding advisories, e.g., to reuse parts of advisories written by other CERTs for one's own advisory. Also, further information exchange regarding vulnerabilities could be structured via the central advisory repository by relating advisory groups about a vulnerability with discussions regarding that vulnerability in the discussion system.

5.3.3. Step 3 : Additional services

Drawing from experiences made during the EISPP project, two additional services/projects that could lead to closer co-operation have been. These and other services, which CEISNE members will start to design to support closer co-operation, should be realized after information sharing tools and a central advisory repository have been implemented.

5.3.3.1. Mailing-list monitoring service

A lot of new vulnerabilities are first disclosed through dedicated mailing lists (such as "bugtraq" or "full-disclosure" mailing-lists). Monitoring such mailing lists is one of the tasks that many CERTs (at least those that publish security advisories) have to perform. A CERT usually monitors several mailing lists for interesting and important information. The process usually involves reading all postings and deciding for each posting what kind of action – if any – needs to be taken.

Providing a service that supports the monitoring of E-mail lists will be beneficial for all CEISNE participants :

- The service would **provide a common foundation for discussions** on new vulnerabilities: A lot of discussions between CERTs on new vulnerabilities are based on postings on mailing-lists, or at least, take postings as reference material. Providing a way to reference that material in a non-ambiguous and stable manner will be beneficial for the CEISNE partners
- The service should help **minimize the workload** for teams to monitor E-mail lists. Although a lot of important information is found on these lists, such mailing-lists also include a lot of "noise",e.g., discussions that are irrelevant, and a lot of unconfirmed or unreliable information. Qualifying that information is a time consuming activity; any service that could help in sharing that task between CEISNE participant would be a great improvement.

On the other hand, the experimentation EISPP conducted in the field of sharing the monitoring task shown that establishing a process for joint mailing-list monitoring that fits the needs of all participants is difficult (see Section 4.4). Therefore, a service that supports joint monitoring of mailing lists should be implemented step-wise:

- Level 1: Maintain a list of relevant mailing lists

  Maintaining a list of mailing-lists considered as relevant by CEISNE members, possibly with comments and judgments about the quality of the list, is a form of best-practice sharing between the members of CEISNE.
- Level 2: Provide an archive of the main mailing lists

  Archiving the most relevant mailing lists on the CEISNE site establishes a common basis for easy reference within discussions between the CEISNE members. It also establishes the CEISNE web site as a "one-stop shop" for the most important security information. Furthermore, level 2 is a necessary technological basis for level 3.
- Level 3: Provide functionality for flagging and/or commenting on postings

  Once postings can be flagged and commented on the CEISNE site, the mailing list archive turns into a tool that should be useful for many CEISNE members as a support for the process of watching for new vulnerabilities and reacting to them. At least parts of the annotations made by each CERT, for example assessments of the a posting's contents, certain flags ("action", "no action",…), etc., could be shared with other CEISNE members so as to enable "unregulated" joint monitoring of mailing lists.
- Level 4: Define processes for joint mailing-list monitoring

With proper tool support in place and first experiences with joint monitoring of mailing lists made, interested CEISNE members can define processes that support real workload sharing through joint monitoring of mailing lists.

5.3.3.2. Advisory creation service

Even though the EISPP advisory format was designed to be as simple as possible while supporting the structures identified as absolutely essential, producing a tool that allows both import and export of EISPP compliant advisories and allows user-friendly authoring of advisories is not an easy task. Although already exporting proprietary advisories only partly to the EISPP format as outlined in Section 5.3.2 is enough to start co-operation within CEISNE, the full benefits of the common format can only be reaped with proper tool support for importing and authoring advisories in the EISPP format. In order to lower the entrance barrier to using the common format, an authoring tool could be developed jointly within CEISNE. (That joint development of non-trivial tools for the CERT community is feasible has been demonstrated by the initiative to build a common incident response tool based on Request Tracker.) The joint development of an authoring tool within CEISNE would help to share the costs of creating a powerful authoring tool that fits the needs of the CEISNE community; the existence of such a tool could boost acceptance of the EISPP advisory format not only within Europe and thus raise possibilities for co-operation to a new level.

6. CONCLUSIONS

When establishing EISPP, the EISPP partners hoped that close co-operation on advisories could be reached within the lifetime of the project, thus establishing a working model for a *Co-operative European Information Security Network of Expertise (CEISNE)* that could easily be expanded to further CERTs. The experiences collected within the EISPP project showed, however, that

- close co-operation can only be reached step-by-step
- co-operation must be supported by adequate tools
- the rules and regulations needed for close co-operation cannot be generalized, but have to be worked out bilaterally between the CERTs planning to co-operate.

At the same time, the project showed that, given proper tool support, co-operation in the early stages of advisory creation such as information gathering and vulnerability analysis can be fruitful at least for quality control and quality improvement, and in some instances, also for cost reduction. Based on these experiences, a roadmap for the establishment of CEISNE under the auspices of an already existing CERT organization has been defined. Once established, CEISNE will act as a facilitator and catalyst for the close co-operation between CERTs, which will be necessary to keep up with the rising number of vulnerabilities.

Document management information

Title	Agreement to join CEISNE CEISNE model and processes
Identifier	EISPP-D3-004-TR
Confidentiality[1]	PU
Status	A (Approved)
Creation Date	2003/10/08
Version	1
Revision	0
Revision Date	2003/12/17
Deliverable Reference	D3.04
Authors	Peter Bivesand, Philippe Bourgeois, Domingo Cardona, Bernd Grobauer.
Keywords	EISPP CEISNE exchange policy cooperation model processes

Approval Section

Company	*Alcatel CIT*	*Callineb*	*InetSecur*	*SIEMENS*	*UPC*
Date	2003/12/18	2003/12/18	2003/12/18	2003/12/18	2003/12/18
Comments	PGP	PGP	PGP	PGP	PGP
Approving Person	Brigitte Conchy	Peter Bivesand	Gema Gomez	Udo Schweigert	Manel Medina

[1] Confidentiality indicator according to the following table

PU	Public
PP	Restricted to other programme participants (including the Commission Services)
RE	Restricted to a group specified by the consortium (including the Commission Services)
CO	Confidential, only for members of the consortium (including the Commission Services)

Document History

Version	*Date*	*Reason for modification*	*No. of pages*		
			added	*modified*	*deleted*
0.1	2003/10/08	Document creation (skeleton)	All		
0.2	2003/11/14	New structure adopted		All	
0.3	2003/12/05	All contributions merged in the final document		All	
0.4	2003/12/09	Comments from WP3 integrated in the document		All	
0.5	2003/12/10	Version sent to peer-reviewers		§ 2, § 5.3.1	
1.0	2003/12/17	Taking into account peer-reviewer comments. **First public release of the document**		All	