MINUTES of the MEETING

TO DISCUSS
FUTURE COLLABORATIVE ACTIVITIES BETWEEN CERTs IN EUROPE

Amsterdam, 24 September 1999

Agenda

1. Welcome and apologies
2. Round of Introductions
3. Verbal Report on the completion of the SIRCE pilot
4. Purpose of the Meeting
5. Analysis of CERTs' requirements for European-level activities

- Inventory of suggestions for activities/actions/joint work
- Discussion of suggestions
- Scope, resources, costs
- Methods of achieving prioritised activities/actions/joint work

6. Follow-up actions and time schedules
7. Any Other Business

APPENDIX. ATTENDEES of the MEETING

1. Welcome and apologies

The meeting was attended by 27 delegates representing 18 organisations / networks from 15 countries. A list of the attendees can be found in the appendix to these minutes. Apologies were received from : SWITCH (CH), Nextra-CERT (CH), LATNET (LV), DFN (DE), DFN-CERT (DE), ACONET (AT).

2. Round of Introductions

Although some of the delegates around the table had some involvement in the SIRCE pilot, some did not. As a consequence it was useful to invite attendees to introduce themselves and their interest in the topics under discussion.

3. Verbal report on the completion of the SIRCE Pilot

Karel Vietsch said that the collaboration and co-ordination between CERTs in Europe had been under discussion since 1992. The report of the TERENA Task Force "CERTs in Europe" (1995) led to a pilot known as SIRCE for a European CERT co-ordination service. This pilot, which started in May 1997 was until recently provided by UKERNA.

The pilot came to an end on 15 September 1999, slightly earlier than anticipated due to Damir Rajnovic resigning from UKERNA. In general, the responses to the pilot service have been positive and many have expressed their appreciation for the work done and the experiences gained during the past 2.5 years. Nevertheless, it has become clear that it will not be possible to establish a permanent operational European CERT co-ordination service to follow on from the SIRCE pilot phase. This is mainly because the needs of the various networks in Europe and their CERTs are so different that it is not possible to reach consensus on the definition of a single permanent service.

There is a clear need for and willingness of CERTs in Europe to collaborate on issues of common interest. Such collaboration can take the form of exchange of information, limited work provided by one or more CERTs for the entire European CERT community or joint activities of CERTs who are interested in jointly solving a particular common problem. The purpose of the meeting was to identify issues that can be addressed through collaborative actions.

Andrew Cormack said that the initial remit of the SIRCE activity had been to act as an information resource for the community and that UKERNA would continue to host the web server until other arrangements could be made. He reported that UKERNA knew of 36 CERTs in Europe with a further embryonic CERT in the process of starting. During the past 17 months, they had dealt with more than 5,400 incidents all bar 100 of which had been closed. EuroCERT had been accepting new incident reports right up until 15 September and aim to close those remaining open as best they can however no new incidents will be accepted. Although the web and email addresses are still active, requests for new action are met with a response directing the enquirer to their local CERT.

Dr Vietsch concluded this agenda item by reporting that the costs of running the CERT pilot had been lower than that budgeted. This was as a result of the EUROCERT activity being understaffed due to recruitment difficulties at UKERNA and also the early termination of the project. As a consequence TERENA is holding a surplus of approximately 100k EURO that was collected contributions. TERENA will contact the contributors to ascertain if they wish the money to be returned or used in some appropriate manner by TERENA for instance to fund a short term solution to follow on from the SIRCE pilot.

4. Introduction to the purpose of the meeting

Brian Gilmore reported that there had been an open meeting at the TERENA Nordunet Conference in Lund (June 1999) and that the majority view was that TERENA should do something to follow on from the SIRCE pilot even though it was unlikely that it would get sufficient funding contributions to provide a full service as originally envisaged. The purpose of this meeting was to get people back together to discuss in some detail what they would like to see done and to prioritise that list.

5. Analysis of CERTs' requirements for European-level activities

Karel Vietsch extracted a list of 18 items from the existing reports and the subsequent emails as a starting point. This list is as follows :

1. Maintaining and providing on-line information about existing CERTs
2. Encourage the establishment of new CERTs
3. Raise awareness of security problems; publicity about CERTs' work
4. Provide assistance to new CERTs
5. Provide PGP key server
6. Provide Certification Authority (to serve only CERTs in Europe)
7. Maintain mailing lists for CERTs (and others)
8. Organise regular meetings of CERTs
9. Co-ordination of the handling of incidents
10. Round-the-clock available Point of Contact
11. Liaison with CERTs and CERT Co-ordination Teams outside Europe
12. Early warning for incidents
13. Pointers to legal information
14. Statistics on incidents
15. Advice on how to handle incidents
16. Vulnerability reports
17. Education: courses for management and CERTs
18. Emergency back-up for CERTs

Brian Gilmore asked if there were any additional items that needed to be added which resulted in the opening of the general discussions that are reported below.

One delegate thought that what was missing is the vision and incident co-ordination, however it was quickly pointed out that including such functions makes the service at least initially impossible to fund, and the message that had been clearly given to TERENA in Lund is to take out the incident co-ordination and see what other useful things could be provided. It was agreed that whatever was agreed in terms of co-operation, it should not divert service effort from the local CERTs.

There was common agreement that to enable the CERTs to undertake operational services collaboratively between themselves there is an essential need for a "trust broker". Such an entity would be used to develop a trusted relationship between new CERTs and the established CERT network by proving their credentials in some approved manner. Once approved, the new CERT would be placed in a database of bona-fide CERTs, rather than just on some public list. - A New item 19 "Trust Broker" was added to the original list of 18 items. A further item to provide a clearing house for security related tools and software was also added.

In view of this discussion - It was agreed to drop the following items from the list as they were seen as largely operational in nature:

9. Co-ordination of the handling of incidents
10. Round-the-clock available Point of Contact
12. Early warning for incidents>br> 16. Vulnerability reports
18. Emergency back-up for CERTs
It was agreed that the functions of item 12 would be handled by CERTs communicating between themselves and would reality be covered by item 7 "Maintain mailing lists for CERTs". It was also pointed out that in the original Task Force report vendors may want to send their vulnerability reports to trusted groups. The operation of a closed distribution list such as proposed under item 7 would satisfy part of that requirement. It was agreed that whilst setting out to discover vendors vulnerabilities was a large and interesting research activity, it would not be practical within the scope of this initiative, however attracting European vendors to use us as a information dissemination route would be very useful.

DANTE tabled a "Best Efforts Service" proposal indicating that they would offer up to 0.5FTE at no (additional) costs to the NRNs although it might have to be charged to non-NRN customers. The project would be highly focussed on network service and could be funded from the infrastructure budget. If accepted by the meeting, a proposal could be made to the Quantum Policy Committee (QPC) which would be charged with controlling the project and reviewing it on an annual basis. DANTE said they would be interested in running a trusted server and email lists and would maintain their membership of FIRST. DANTE would expect TERENA to run an open forum (such as a Task Force) to provide consultation with the community.

There was no enthusiasm to accept the DANTE proposal. It was pointed out that the service being proposed had already been crossed off the wish-list. It was also felt that the proposal was to fund this important independent piece of work from a project that was scheduled to end in May 2000 was unacceptable and that this work should stand alone. It was also thought by several that the DANTE CERT did not display the required visibility and neutrality to support this initiative.

After further discussion, it was agreed that the total package of work that is needed in an unconstrained world includes two major elements

- An forum in which to exchange incident handling and co-ordination taking in NRNs, ISPs, vendors and the public. This is likely to consume 3-5 FTEs per year and is impractical to fund at the present time.
- A closed and trusted group of accredited CERTs that have a mechanism to evaluate and accredit new CERTs and bring them into the trusted circle with some level of co-ordination support.

It was agreed that the DANTE proposal most closely fits with the first bullet item above and will not be practical at the moment. TERENA's role fits with the running of a neutral, closed and trusted group. The difficulty in carrying out the accreditation is that if the task is delegated from one organisation down through many generations it becomes difficult for the original trusted group to have much knowledge about the rigour with which

further accreditation has been carried out. It may be possible to avoid this problem by seeking to have only one bona-fide accreditation agency (such as an NRN) in each country. These approved authorities would follow a documented accreditation process (which might include site visits) in such a way as to demonstrate its effectiveness. It was suggested that it would be beneficial for such a European accreditation authority to have some sort of formal relationship with FIRST. It was agreed that this could best be organised as a European group in FIRST, rather than as a European-FIRST.

It was suggested that one approach to incident co-ordination might be for each CERT to hold its own incident data locally in a database, but make the database open to other CERTs, thus forming one distributed information source. At least one CERT indicated that they would not legally be allowed to do this (under the conditions of the local data protection act) so the idea was un-viable. DANTE said they could pitch a best efforts service somewhere between a full database and an email distribution list however there was still no interest in pursuing the DANTE proposal.

There was a some confusion by some delegates that what was being proposed was the exchange of full data on all incidents, however Karel Vietsch point out that this had not been the intention of this activity and the most that might be expected was an exchange of numbers of incidents in particular classes. Several delegates thought that exchange of numbers would enable the identification of trends and would therefore be useful added value.

A further suggestion was that the way forward might be to ask particular CERTs take regional responsibility providing support in their own and neighbouring countries for recruiting new CERTs and education. This was compared to the model of delegation of IP address space and thought to be a viable model. This discussion lead to the thought that RIPE-NCC should be approached to see if a security contacts entry for each address could be put into the RIPE database. CERT-NL agreed to take this action and report back to the list.

It was universally agreed that it is vital to put in place something to continue after the SIRCE pilot, but there was no interest seeking to put in place a full incident co-ordination service at this stage (apart from DANTE). Many thought that incident co-ordination should be a long term goal, but we should not start with it right now.

Don Stikvoort said that his company (STELVIO) has made an proposal to FIRST to provide some secretariat services to them that would be on an independent and neutral basis. Whilst he could not make a firm proposal at the moment, it is likely that STELVIO would be willing to make a proposal for up to 1/4 FTE to provide a similar service to Europe. This could be provided at a later date if TERENA decided to proceed in that direction. The offer to make a proposal was left on the table by STELVIO.

Brian Gilmore summarised the decisions so far as :

- To maintain an information base of CERT related items

- Continue to maintain at least closed email distribution list and maybe open lists for public information dissemination
- We need a web of trust which might be housed.
    - At a single existing CERT
    - At DANTE
    - By a consortium of CERTs

- It would be useful to call at least one further meeting of this group to oversee progress.

It was further agreed to go through the list of items that had been produced and decide if each was necessary and if so how they might be achieved:

- **Item 20 Clearing House for Tools and Software**

There was general agreement that this would be a useful activity, but no suggestion of how to organise this in the context of the current framework. It was deferred for later investigation

- **Items 15 & 17 Education and Training**

Widespread agreement that this would be subsumed in the work of further meeting of this group or its successor. In the meantime CERT Teams are encouraged to make any education and training material they had produced available to other teams.

- **Item 5 & 6 Certification**

Subsumed as part of the mailing list activity

- **Item 14 Statistics of Incidents**

It was agreed that the first step in being able to deal with incidents on a consistent basis was to first reach consensus on a classification scheme. The JANET-CERT and CERT-NL have been working towards a single classification scheme and invited other interested CERTs to become involved with this work. Yuri Demchenko reported that the IETF had a working group looking at these issues.

- **Item 13 Pointers to Legal Information**

UKERNA and GRnet have been commissioned to undertake a survey of information on the legal process of prosecution in cases of computer related crime. Their initial contact with the authorities in several countries had resulted in no information being forthcoming. UKERNA is now following up a fresh line of enquiry with the Association of Chief Police Officers (ACPO) in the UK who are believed to be undertaking a similar exercise. Andrew Cormack agreed to provide feedback to TERENA after attending their conference. The mood of the meeting was not to show any great enthusiasm for this item

to be solved urgently and thought that it could be dealt with at a later meeting with the benefit of UKERNA feedback.

- **Item 3 Publicity**

It was agreed that raising awareness of security problems and publicity of CERTs work was an important item for all CERTs. It was agreed that this is not something to be dealt with as a European co-ordination activity but is best dealt with at the national level by each CERT individually. The exchange of education and training material between CERTs may have some impact on this activity however.

- **Item 1 Maintaining on-line Information about existing CERTs**

It was agreed that this is an essential element of EuroCERT Co-ordination to be provided under this umbrella. Andrew Cormack agreed to continue to host this service at UKERNA until an alternative arrangement can be made. In the meantime Andrew will ensure the information is updated.

- **Item 7 Maintaining mailing lists for CERTs (and others)**

There was general agreement that the provision of email distribution lists would be an essential element in encouraging collaboration and co-ordination between CERTs. At least a closed list of trusted members for exchanging sensitive information (including early warnings, vulnerability reports, signalling of trends and requests for assistance) is required and probably other open, public lists for wider dissemination of security related information. It was agreed that how these will be supported requires additional thought and should be discussed by interested parties by electronic mail after the meeting.

- **Item 4 Provision of assistance to new CERTs**

This was regarded by the meeting to be crucially important for successful security. It is the means by which good practice and high standards can be disseminated to all those working in the CERT field. There are some guidelines on the EuroCERT web server, more information can be found in a 100 page RFC and of course established CERTs may be asked for their advice and guidance

The meeting agreed that some of essential element assisting new CERTs include:

- Providing on site visits for individual new CERTs, but that would imply extra costs which would have to be borne by the site requesting the visit.
- Running tutorials at or around existing meetings
- A co-ordination centre should be considered as an "expertise broker" and be able to identify experts to fulfil the needs of new CERTs (or others). This would however require existing CERTs to be willing to contribute effort to the activity.

CERT-NL agreed to provide initial assistance to new CERTs in the short term on the clear understanding that the activity will be handed on for long term support. This offer was accepted by the meeting.

- **Item 19 Trust Brokerage**

The long term future of the first point of contact for new CERTs and the process of accreditation of such organisations formed a large part of the meetings business. It was agreed that such an activity will need to be regulated in a transparent manner to ensure the continuation of trust by existing CERTs. It was agreed by the meeting that the best way forward was to document the requirements of the process. Brian Gilmore suggested that this could form the basis of a small TERENA project, funded from TERENA's own project budget. This idea was accepted by the meeting and Brian agreed to put a proposal to the next TERENA Technical Committee on 6th October 1999 for approval.

Brian Gilmore asked people knowledgeable in this area to write down ideas of what needs to be done in the process specification project and send them to him. Vincent Berkhout made it clear that DANTE did not what to be the trust broker.

- **Other Items**

Of the remaining items on the list : item 2 "Encouragement of new CERTs" had been subsumed into items 19 and 4. Liaison activities with CERTs and CERT Co-ordination Teams outside Europe could partly be covered by the email list activities and partly by the trust brokerage activity.

6. Follow-up actions

It was agreed that it is important to keep this group together and to have a framework in which regular meetings could be co-ordinated. A future meeting was planned for January 2000 at which the accreditation of new CERTs process resulting from the TERENA project could be discussed along with the items unresolved by the days discussions (including running workshops for education and training) and other regular meetings.

Summary of Actions

ACTION ITEM	RESOLUTION
1. Web Information on existing CERTs	UKERNA to continue to support in the short term
2. Mailing lists to support CERT activities	To be discussed by email

3. Assistance to new CERTs	CERT-NL to provide in short term only
4. Trust Brokerage	TERENA to support specification of process definition to be completed by next meeting in Jan 2000. Open competition to find suitable operator of brokerage to take place after definition
5. Classification of Incidents to allow statistics to be gathered and trend analysis	Initial working being undertaken by JANET-CERT and CERT-NL. Further wider discussions on TERENA email list
6. Clearing House for Tools and Software	To be discussed at next meeting
7.Organisation of Regular Meetings	To be discussed at next meeting
8. Organisation of Workshops	To be discussed at next meeting
9. Contact RIPE-NCC regarding security entries	CERT-NL
10. Date of Next meeting	To be organised by TERENA in January 2000 in Amsterdam.

ISSUED By JOHN DYER
TERENA
<John.Dyer@terena.nl>
13 October 1999

APPENDIX to Minutes of 24th September 1999

ATTENDEES of the MEETING
TO DISCUSS FUTURE COLLABORATIVE ACTIVITIES BETWEEN CERTs IN EUROPE

Avgust Jauk	ARNES	jauk@arnes.si
Marc Roger	BELNET	Marc.Roger@belnet.be
Paolo Moroni	CERN	Paolo.Moroni@cern.ch
David Crochemore	CERT-RENATER	David.Crochemore@renater.fr
Vincent Berkhout	DANTE	vincent.berkhout@dante.org.uk
Jamie Agudo	ESCERT	jagudo@escert.upc.es
Jordi Linares	ESCERT	jlinares@escert.upc.es
Joao Moreira	FCCN	jmm@rccn.net
Tony Falenius	FUNET-CERT	falenius@csc.fi
Roberto Cecchini	GARR-CERT	roberto.cecchini@fi.infn.it
Christos Aposkitis	GRNET-CERT	apochr@noc.ntua.gr
Francisco Monserrat	IRIS-CERT	Francisco.Monserrat@rediris.es
Norbert Meyer	POL-34	meyer@man.poznan.pl
Stanislaw Starzak	POL-34	starzak@man.lodz.pl
Klaus Peter Kossakowski	Secunet	klaus-peter@kossakowski.de
Don Stikvoort	Stelvio	don@stelvio.nl
Jacques Schuurman	SURFnet/CERT-NL	jacques.schuurman@surfnet.nl
Henrik Sandell	Telia Internet, IRT	sandell@telia.net
Daniel Johansson	Telia Internet, IRT	danne@telia.net
Jimmy Arvidsson	TeliaCERT CC	jimmy.j.arvidsson@telia.se
Pege Gustafsson	TeliaCERT CC	Pege.P.Gustafsson@telia.se
John Dyer	TERENA	John.Dyer@terena.nl
Brian Gilmore	TERENA	B.Gilmore@ed.ac.uk
Yuri Demchenko	TERENA	demchenko@terena.nl
Karel Vietsch	TERENA	vietsch@terena.nl
Andrew Cormack	UKERNA	Andrew.Cormack@ukerna.ac.uk
Olav Schjelderup	UNINETT	Olaf.Schjelderup@uninett.no