TSec(00)048

Minutes of 3rd meeting to discuss collaborative activities between CSIRTs in Europe

Vienna, 12 May 2000

Karel Vietsch - Draft 1, issued 17 May 2000

1. Welcome and Apologies

The meeting chairman, Brian Gilmore, welcomed the participants and expressed his gratitude to Wilfried Wöber and ACOnet for hosting this meeting and organising logistics in an excellent way.

Apologies had been received from John Dyer (TERENA), Klaus-Peter Kossakowski and Jacques Schuurman (CERT-NL)

2. Round of Introductions

Present:

	Name	Organisation
1	Jaime Agudo	ESCERT
2	Preben Andersen	DK-CERT
3	Christos Aposkitis	GRNET-CERT
4	Jimmy Arvidsson	Telia CERT
5	Gorazd Bozic	ARNES
6	Roberto Cecchini	GARR-CERT
7	Andrew Cormack	JANET CERT
8	David Crochemore	Le CERT RENATER
9	Pascal Delmoitié	BELNET
10	Michel Dupuy	CERTA
11	Per Arne Enstad	UNINETT CERT
12	Tony Falenius	FUNET CERT
13	Brian Gilmore	TERENA
14	Christoph Graf	SWITCH
15	David Harmelin	DANTE

16	Denise Heagerty	CERN CERT
17	Peter Janitz	DFN-CERT
18	Xander Jansen	CERT-NL
19	Mark Koek	M&I/Stelvio
20	Flemming Laugaard	DK-CERT
21	Jordi Linares	ESCERT
22	Chelo Malagon	RedIRIS
23	Jan Meijer	CERT-NL
24	Francisco Monserrat	RedIRIS
25	Robert Morgan	JANET CERT
26	Claudia Natanson	BT-CERT
27	Gareth Price	BT-CERT
28	Don Stikvoort	M&I/Stelvio
29	Karel Vietsch	TERENA
30	Wilfried Wöber	ACOnet

3. Minutes of Last Meeting (Amsterdam, 21 January 2000)

- Status report on Actions from Last Meeting.

The minutes of the previous meeting (revised draft issued 28-1-2000) were approved without change.

Actions List:

1	TERENA	Prepare an implementation plan and timeline and documentation for the TI scheme	done; see agenda item 4
2	A. Cormack	Obtain copy of Law Enforcement Agents list of minimum requirements for taking legal action	Andrew Cormack had circulated EU guidelines; he would continue watching developments; see also agenda item 9

3	Cert-coord	Mail information to Y. Demchenko about incident response tools	ongoing; see agenda item 9
4	J. Schuurman	Draft 1-page statement of requirements for security entry in RIPE database and mail to RIPE list	done ; see agenda item 8
5	TERENA	Open new Incident Classification email distribution list	done
6	TERENA	Draft TF charter, circulate to cert-coord list and submit to TTC once agreed	draft available; to be discussed under agenda item 10
7	TERENA	Organise next meeting (11-12 May 2000), cert-coord and seminar	done

4. Status of Trusted Introducer call for proposals

TERENA staff had drafted the documents for the Call for Proposals for the provision of the TI function. The discussion of these documents on the mailing list had led to some small changes, and subsequently the call had been published by TERENA. Before the deadline of 2 May 2000, only one proposal had been received. It is a proposal from M&I/Stelvio. The key persons in this proposal are Klaus-Peter Kossakowski (TI-manager), Don Stikvoort (contract manager and back-up TI-manager) and Mark Koek (technical and information support services). They offer to provide the TI function for the first year for a fixed-price sum of EUR 30,000.

A small committee was appointed from among the participants in the cert-coord meetings to review the proposal. That committee, consisting of Brian Gilmore (chairman), Andrew Cormack, Christoph Graf, Wilfried Wöber and Karel Vietsch (secretary) met on 11 May 2000. They found no surprises in the proposal and recommended accepting it, subject to some administrative details that Karel Vietsch would discuss with the proposers.

The committee had discussed in some detail how the TI provision should be paid for. For the first year this was not a problem because 30 kEUR was a limited amount of money. If needed even TERENA alone could supply this sum, but also there was more than 85 kEUR left-over money from the SIRCE pilot, which after the approval of the original SIRCE Contributors might be used for funding the TI function provision. However it was important to set the funding scheme up in such a way that after an initial subsidy the system would automatically grow to a self-financing state. After comprehensive deliberations the committee proposed the following:

- CSIRTs applying for level-2 status (so: level-1 teams) will be charged a one-off amount of EUR 450, regardless of whether they acquire level-2 status or not
- During the first year of the provision of the TI function, TERENA will pay (possibly from the money left over from SIRCE) this charge of EUR 450 for any CSIRT of a TERENA member organisation applying for level-2 status
- Level-2 CSIRTs will be charged EUR 600 per year. For teams having level-2 status during only part of a year the charge will be proportional, so EUR 50 per month.

The committee asked the meeting if these charges would be acceptable. The general consensus was that they would, although it would be important to explain the benefits of the TI function to managers. This also in view of the FIRST membership, which brings an annual membership fee of a similar size. It would be important to emphasise that paying for the TI function is not becoming a member of yet another club but buying a service. Don Stikvoort promised that the TI would produce one or more documents aimed at managers to explain the benefits of obtaining level-2 status and hence of paying for the TI service.

The TI structure also encompasses a board that will oversee the work of the subcontractor. It is envisaged that this board will consist of representatives from level-2 teams. This poses a start-up problem, since at the start of the TI function provision there are no level-2 teams yet. The meeting therefore agreed that the committee that had reviewed the proposal (composition: see above) would continue for the time being, but no longer than for one year, as the interim-board. As soon as more than just a few teams had reached level-2 status, board members would be appointed to take over from the interim-board.

5. Deploying PKI for CSIRTs and web-of-trust (incl. relation to LDAP)

Andrew Cormack and Don Stikvoort together gave a short introduction. PGP works well but only within a relatively small community; it is also mostly used for e-mail only. X.509 is widely supported but it has in practice a limited set of applications. How could X.509 be used in the context of the cert-coord group? Using it for e-mail would be a bridge too far for most participants. One useful suggestion would be to have a server certificate for the TI Web site. (A simple common password to the confidential information would not be an adequate solution, also because it is foreseen that teams might lose their level-2 status.) A third idea was to have a client certificate for TI use, but that seemed still difficult and should therefore not be tried now.

After a lively discussion the meeting concluded the following:

- TERENA should promote in its Technical Programme work on X.509, but this is outside the scope of the cert-coord group.
- There should be a server certificate for the TI Web site. By whom this certificate should be issued was the subject of a discussion that should be continued between TERENA and the TI subcontractor.

- Several CSIRTs represented in the meeting (including DK-CERT, SWITCH, ESCERT, FUNET) mentioned that they were "working on PKI". In a seminar attached to the next meeting some speakers from CSIRTs should tell about their experiences.

6. FIRST and relations with FIRST

Don Stikvoort gave a short presentation. Since 1 April 2000, M&I/Stelvio have been contracted to provide the FIRST secretariat. FIRST has now established a funding model with funds coming in through membership fees. The annual membership fee is USD 550, and there are currently about 100 FIRST members. The main functions of the FIRST secretariat are: accounting, facilitating meetings, action item maintenance, co-ordinating membership applications, keeping the FIRST Web site up-to-date, PGP key distribution, the mail address FIRST-SEC@FIRST.ORG, committee support.

As to the relations between FIRST and the cert-coord group, the conclusion from the meeting was that time was not yet ripe to institutionalise those. The cert-coord has another remit than FIRST, among others by its geographical scope and its activities, but also by being open to teams that are not FIRST members.

The meeting concluded as follows:

- Good information exchange between the cert-coord group and FIRST is important. This can be achieved in an informal way by people who are in both bodies acting as the linking pin. An update on FIRST should be a regular agenda item in meetings of this group, and it was hoped that conversely updates on cert-coord would be given at the appropriate FIRST meetings.

7. Results of yesterdays Seminar sessions

The seminar sessions on the day before this meeting had been very worthwhile. Thanks were expressed to the presenters. It was felt that the format of 2-day meetings, the first day for seminar sessions and the second day for a meeting in the strict sense, was a good one. Also the joint dinner on the evening of the first day is an important element of the format, because it provides an excellent opportunity for informal discussions.

In the first seminar session, JANET CERT, CERT-NL and Telia CERT had presented their practice, organisation, structure, working methods. Conclusions from the meeting were:

- A similar seminar session should be organised at the next meeting, with (three) other teams telling about their current practice.
- Presenters should be given a list of topics to address. This list could be prepared via a discussion on the mailing list or by a small sub-group.
- Eventually these seminar sessions could lead to a document listing problems and possible solutions.

The second seminar session had been on incident taxonomy and classification, with presentations by Andrew Cormack and Jan Meijer. From this session the meeting noted with great interest that:

- A sub-group of the cert-coord group had been established, co-ordinated by Andrew Cormack and Jan Meijer, with participation also from CERT/CC and AusCERT.
- This group had a timetable of actions.
- The first results of the group would be presented and discussed (possibly in the form of a BoF) at the FIRST conference in Chicago in June.

8. The RIPE database and incident handling

Wilfried Wöber introduced the subject. In an analysis that had been performed of the value of the RIPE database for the community, also information about security contacts had been discussed. The RIPE database now has links to administrative and technical contacts at Local Internet Registries, and that could be extended with a pointer to a security contact. The initial thrust had been to attach that to different types in the RIPE database. Jacques Schuurman had drafted a proposal, which had been circulated only informally. The proposal would be on the agenda of the meeting of the RIPE database working group next week, but again it would probably be discussed there only informally. Probably the first implementation should be restricted to adding a pointer to the IP address object (and potentially the AS number object). A small subgroup of cert-coord, consisting of Jacques Schuurman, Wilfried Wöber, Jan Meijer and Denise Heagerty would continue to work on this. Thanks were due to Jacques Schuurman for the work he had done.

It was noted that a regular review process would be needed to ensure that the information is there and is up-to-date.

The further time schedule was as follows:

- After the discussions next week, Wilfried Wöber would collect some individuals to continue with the development until September.
- If consensus had been reached, then a decision could be taken in the RIPE meeting in Amsterdam on 12-15 September 2000.
- After that, the development and implementation would be a task of the RIPE NCC.

9. Other action items

9a. Clearing House for Incident Handling Tools

A simple Web-based reference to incident handling tools had been set up at the TERENA Web site. Questions were if this was felt to be useful and if it could be extended with

references to more tools and also with reviews explaining the value (or lack thereof) of specific tools.

A lively discussion produced the following conclusions and suggestions:

- The current clearinghouse was felt to be useful and should be extended. This required contributions from all.
- An extension with reviews of tools would be very useful.
- The Web could also contain pointers to people who have experience with a certain tool and are willing to share that experience.
- Presentations about experiences with specific tools would make an interesting seminar at a future meeting.

9b. Pointers to legal information

As mentioned under agenda item 3, Andrew Cormack had volunteered to continue watching developments. He called on the others to inform him about interesting developments or legal changes in their countries. Andrew Cormack would then make such information available to the entire group.

9c. Encouraging new CSIRTs

It had been agreed that it would be one of the tasks of cert-coord to encourage the establishment and development of new teams. It was not clear yet how this could be approached best.

Some actions were agreed as follows:

- Level-0 teams would be welcome at cert-coord meetings.
- The TI could point new teams to information that would be useful to them and to people who could provide such information.
- The TI should give a presentation at a future RIPE meeting.

Obviously these actions combined with training workshops (see next item) were not yet an adequate scheme to help (the establishment) of new CSIRTs. Other possible mechanisms should be discussed on the mailing list and in the next meeting.

9d. Training workshops for new (staff of) CSIRTs

It had been agreed that under the auspices of cert-coord, training workshops would be organised for new (staff of) CSIRTs. It was felt that one or two such workshops should be organised in the next two years. One opportunity would be to organise such a workshop adjacent to next year's FIRST conference, which would take place in Toulouse in June 2001 (David Crochemore is on the programme committee). However there might also be disadvantages in the combination of the two events.

Whether existing CSIRTs would be interested to send their new staff to such a workshop appeared to depend very much on the content and form of the workshop. For example, a workshop should have a clear added value compared to studying information from the available literature.

It was concluded that the requirements for the programme of the training workshop needed further clarification. A separate agenda item should be devoted to those requirements in the next meeting.

10. Establishing a TERENA Task Force

It had been agreed that the cert-coord group would continue as a TERENA task force. This required the adoption of Terms of Reference, which were useful to obtain a common understanding of the groups objectives and working methods and to introduce some planning in the form of deliverables and milestones.

The TERENA secretariat had provided a first draft of the Terms of Reference, which was discussed by the meeting. Specific remarks were:

- The envisaged participation in the task force as described in point 3, although materially correct, sounded somewhat too restrictive. This clause should be reformulated.
- The frequency of task force meetings should be described as "2 to 3 times per year" rather than "approximately 3 times per year".
- The various deliverables and milestones should be adjusted on the basis of the conclusions under the previous agenda items.

Karel Vietsch would circulate a revised draft for discussion on the mailing list. This discussion should lead to consensus by August.

By acclamation, Gorazd Bozic was elected chair of the task force.

11. Date of next meeting

Offers to host the next meeting had been made by RENATER (in Paris), ARNES (in Ljubljana) and ESCERT (in Barcelona). It was decided to have the next meeting in Paris and take up the other offers at a later date. Because of the success of the formula of this meeting and the number of suggestions for seminar topics, the next meeting will again be a 2-day event, with seminar sessions on the first day.

The next meeting will take place in Paris on Thursday and Friday 28-29 September 2000.

12. Any other business

The meeting expressed its thanks to Wilfried Wöber for the excellent organisation of the meeting facilities and the meals.

The meeting expressed its thanks to Brian Gilmore for his chairmanship of the past three meetings, which had been instrumental in getting an important new structured activity off the ground.

SUMMARY OF ACTIONS

1	Karel Vietsch	Finalise negotiations with M&I/Stelvio on TI contract and have contract signed
2	TI	Produce document(s) to explain benefits of TI to managers
3	TERENA and TI	Discuss and arrange server certificate for TI Web site
4	Secretariat	Arrange seminar session about experiences of CSIRTs with PKI, adjacent to next TF-CSIRT meeting
5	Secretariat	Arrange separate agenda item for update on FIRST at all future TF-CSIRT meetings
6	Secretariat	Arrange seminar session about current practice of CSIRTs, adjacent to next TF-CSIRT meeting. Via discussion on the e-mail list obtain list of topics that speakers should address
7	Taxonomy subgroup	Present work on taxonomy at FIRST conference in Chicago in June 2000
8	Wilfried Wöber and others	Prepare decision at September 2000 RIPE meeting about security contact entry in RIPE database
9	Secretariat	Arrange seminar session about experiences with specific incident handling tools, adjacent to a future TF-CSIRT meeting
10	TI	Give a presentation at a future RIPE meeting
11	Secretariat	Arrange separate agenda item at the next TF-CSIRT meeting about requirements for the programme of training workshops
12	Karel Vietsch	Revise draft Terms of Reference of TF-CSIRT and send it to mailing list for further discussion

13	David Crochemore and Secretariat	Organise next TF-CSIRT meeting in Paris on 28-29 September 2000