TSec(00)111

Minutes of the 1st TF-CSIRT meeting

Paris, 29 September 2000

---

1. Welcome and Apologies
2. Round of Introductions
3. Minutes of Last Meeting (Vienna, 12 May 2000)
4. Formal Establishment of TF-CSIRT
5. Trusted Introducer Pilot Service
6. Update on FIRST
7. Results of yesterday's Seminar sessions
8. Security contact entry in the RIPE database
9. Requirements for a Training Workshop for New (Staff of) CSIRTs
10. Relations with CEC. CSIRTs in eEurope 2002 Action Plan
11. Legal Issues and Relations with Law Enforcement Agencies
12. Other Work Items
13. Encouraging and Assisting New CSIRTs
14. Date and Venue of Next Meeting
15. Any Other Business
16. SUMMARY OF ACTIONS

---

1. Welcome and Apologies

The chairman, Gorazd Bozic, welcomed the participants. Apologies had been received from John Dyer (TERENA), Tony Falenius (FUNET), Kick Fronenbroek (Concert), David Harmelin (DANTE), Denise Heagerty (CERN), Leila Pohjolainen (FUNET) and Wilfried Wöber (ACOnet).

2. Round of Introductions

Meeting was attended by 40 people: representatives of 26 CSIRTs from 15 countries. List of attendees is in Appendix A.

3. Minutes of Last Meeting (Vienna, 12 May 2000)

Status report on Actions from Last Meeting. The minutes of the previous meeting were approved without change.

Actions List:

Action 0-1. Finalise negotiations with M&I/Stelvio on TI contract and have contract signed
Responsibility: K. Vietsch
done; see agenda item 5
Action 0-2. Produce document(s) to explain benefits of TI to managers
Responsibility: TI
open; see agenda item 5

Action 0-3. Discuss and arrange server certificate for TI Web site
Responsibility: TERENA and TI
open; see agenda item 5
Action 0-4. Arrange seminar session about experiences of CSIRTs with PKI, adjacent to next TF-CSIRT meeting
Responsibility: Secretariat
done
Action 0-5. Arrange separate agenda item for update on FIRST at all future TF-CSIRT meetings
Responsibility: Secretariat
done
Action 0-6. 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
Responsibility: Secretariat
done, respectively not done
Action 0-7. Present work on taxonomy at FIRST conference in Chicago in June 2000
Responsibility: Taxonomy subgroup
done; see agenda item 6
Action 0-8. Prepare discussion at September 2000 RIPE meeting about security contact entry in RIPE database
Responsibility: W. Wöber and others
done; see agenda item 8
Action 0-9. Arrange seminar sessions about experiences with specific incident handling tools, adjacent to a future TF-CSIRT meeting
Responsibility: Secretariat
open
Action 0-10. Give a presentation at a future RIPE meeting
Responsibility: TI
open
Action 0-11. Arrange separate agenda item at the next TF-CSIRT meeting about requirements for the programme of training workshops
Responsibility: Secretariat
done; see agenda item 9
Action 0-12. Revise draft Terms of Reference of TF-CSIRT and send them to mailing list for further discussion
Responsibility: K. Vietsch
done; see agenda item 4
Action 0-13. Organise next TF-CSIRT meeting in Paris on 28-29 September 2000
Responsibility: Crochemore, Secretariat
done

4. Formal Establishment of TF-CSIRT

After the kick-off meeting of TF-CSIRT in Vienna on 12 May 2000, Karel Vietsch had sent the revised draft Terms of Reference of TF-CSIRT to the mailing list for further discussion. No objections or new suggestions had been received. The TERENA Technical Committee had formally established TF-CSIRT with these Terms of Reference in its meeting of 12 September 2000.

5. Trusted Introducer Pilot Service

Karel Vietsch reported that the contract negotiations between Stelvio and TERENA had been successfully completed and the contract had been signed. The pilot service had been launched on 1 September 2000 and would run for a one-year period. The start date had been a bit later than originally planned, but this had the advantage that Stelvio could make a flying start, offering the full package of services from the very first day.

Don Stikvoort presented a status report on the Trusted Introducer, which was now one month old. He had formulated the TI mission statement as follows: "The TI must foster trust and co-operation between CSIRTs in Europe, both new and experienced. The vehicle used to achieve this is to invite CSIRTs to present themselves and describe their service according to an established baseline - thus enabling objectivity, which is regarded as the pre-requisite of trust.". Don Stikvoort reminded the meeting of the various levels, and the ways in which a CSIRT can be moved from one level to another. The TI is managed by M&I/Stelvio. The TI service manager is Klaus-Peter Kossakowski; other staff members involved include Don Stikvoort and Mark Koek. The TI review board will review the TI work and deal with special cases and problems. The review board will consist of representatives of level-2 teams. Until the board can be composed in that way, it will consist of Brian Gilmore (chair), Karel Vietsch (secretary), Andrew Cormack, Christoph Graf and Wilfried Wöber. The public Web site www.ti.terena.nl has been up since 1 September 2000. It currently lists 51 level-0 teams and contains descriptions of the TI process and background information. Three CSIRTs have asked to become level-2 and have been sent the draft Invitation Package. Currently the TI is working on the final version of the Invitation Package; a note for managers on the benefits of the TI service; the Web site for level-2 teams only (SSL), a server-side certificate for the Web sites; and a presentation at a RIPE meeting.

Klaus-Peter Kossakowski told that some people had expressed the view that joining the TI service was more attractive than becoming a member of FIRST. He wondered why. Some of the suggested answers were that the TI has a European focus, that the benefits of FIRST membership are not clear, that FIRST is so large that an individual member becomes anonymous, and that for outsiders it is not easy to find out about the activities of FIRST.

In the discussion of Appendix B (the form to be filled out when applying for level-2 status) the request was made that CSIRTs should be able to indicate whether or not it was in their remit to deal with problems caused by viruses or (another example:) spam.

Concluding the discussion on this agenda item Don Stikvoort invited all CSIRTs present to apply for level-2 status.

6. Update on FIRST

Klaus-Peter Kossakowski gave a short update. Of the 86 current members of FIRST, 34 are in Europe. The next FIRST event will be a Technical Colloquium, which will take place in Karlsruhe in October. For 2001 two Technical Colloquia are planned, both in the USA. Technical Colloquia are open only to FIRST members. The next FIRST conference will be held on 17-22 June 2001 in Toulouse, and is organised by Michel Miqueu and David Crochemore.

Michel Miqueu mentioned that the Toulouse conference is announced on the FIRST Web site. The call for papers has been published, and sponsorship is being sought. He underlined that the FIRST conference is open to everyone.

David Crochemore added that it was the intention to focus the conference on the real work of CSIRTs. The event will start on Sunday evening and run until early afternoon on Friday. It will consist of 2 days for tutorials, 3 days of conference sessions and a members meeting.

There followed some discussion as to whether TF-CSIRT should organise its planned workshop for new (staff of) CSIRTs on these two tutorial days. In the end it was concluded that it would be best not to combine that workshop with the FIRST conference.

Claudia Natanson suggested that European CSIRTs should be presented at the FIRST conference. Klaus-Peter Kossakowski thought that this might be done at the beginning of the conference, e.g. 30 minutes on TF-CSIRT followed by short presentations by two or three European CSIRTs. It was agreed that Gorazd Bozic would submit a paper to present TF-CSIRT. It was agreed that in addition the TI team would submit a paper to present the TI pilot service.

7. Results of yesterday's Seminar sessions

The seminar sessions on the day before this meeting had been very worthwhile. All speakers were asked to send their slides to Yuri Demchenko, who would put them up on the TF-CSIRT Web site.

The first seminar session had been on current practice in CSIRTs, with presentations by Le CERT RENATER, DFN-CERT and BTCERT. The meeting found this kind of seminar session very useful and asked the Secretariat to organise a similar session at the next TF-CSIRT meeting.

The second session had been on PKI. The conclusion was that PKI was a very important issue for CSIRTs, but in most cases it was not the CSIRT teams themselves but their

close colleagues in the NRENs who were working on PKI and setting up a certification authority.

Karel Vietsch mentioned that PKI/CA had come up recently in a number of TERENA activities: in TF-CSIRT but also in the Middleware Workshop and in the new TERENA Task Force on LDAP service deployment. Adjacent to the TERENA General Assembly meeting in Paris in October there would be a mini-symposium on PKI with speakers from CREN and IBM. TERENA planned to set up a separate activity for harmonisation between PKI/CA work of NRENs in Europe.

There followed a discussion as to whether a PKI hierarchy should be set up for CSIRTs in Europe. Could the TI act as a certification authority for this community? Don Stikvoort felt that technically it would not be difficult to issue certificates but managerially it was a completely different matter. For the moment this seemed like a bridge too far. It was agreed to discuss this matter further at the next TF-CSIRT meeting; Don Stikvoort and Christoph Graf would prepare that discussion.

The third session had been on the Incident Description and Exchange Format, with Yuri Demchenko presenting the draft and participants in the meeting providing useful feedback.

8. Security contact entry in the RIPE database

In the previous meeting Wilfried Wöber had volunteered to take on this action item, but unfortunately he could not attend this meeting. Shortly before the meeting he had sent a progress report by e-mail, but that report consisted mostly of an object format description and it was unclear exactly what the current status of the discussion in RIPE was. It was also not clear if the discussion in TF-CSIRT could be postponed until the next meeting or decisions would have to be taken before then.

Gorazd Bozic would ask Wilfried Wöber to explain the current status on the TF-CSIRT mailing list, and then conduct the discussion further on that mailing list.

9. Requirements for a Training Workshop for New (Staff of) CSIRTs

In the previous meeting it had become clear that whether existing CSIRTs would be interested to send their new staff to a training workshop depended very much on the content and form of the workshop. It had been decided to discuss the requirements for such a workshop in this meeting.

Andrew Cormack reported that he had learned from CERT/CC that they are considering franchising the training courses that they had organised before in Pittsburgh. It was unclear if TF-CSIRT could use that material; some of it might be useful. It was remarked that these courses are long (3 days) and expensive. Andrew Cormack would find out more about them.

Don Stikvoort mentioned that he was developing some material that could be used in a TF-CSIRT training workshop.

Jan Meijer felt that the training workshop should address both organisational and technical issues. It should cover tools to be used regularly.

Gorazd Bozic underlined that different CSIRTs are organised in different ways. Usually starting staff members have a good general technical knowledge but are not specialists in IT security. Usually such staff members only know one or two systems and they lack knowledge of the broader picture. Also communication skills were something to be learnt: quite often beginning engineers were too undiplomatic in their communication for CSIRT purposes.

Don Stikvoort mentioned as elements for a training workshop: trace routers; WHOIS databases etc.; information about the everyday practice in CSIRTs; tools. He felt that such a workshop would really need two days.

Claudia Natanson said that an important skill to be learnt was the ability to correlate the effects observed to the (sometimes seemingly completely different) causes.

Andrew Cormack mentioned as elements for the workshop: finding out who is responsible for an IP address (WHOIS, DNS); interpreting mail headers to find out what has been forged.

Jan Meijer concluded that it would be impossible to teach all skills in one course. Some things would simply need to be shown so that participants could find out more about them later.

Christoph Graf mentioned that a 2-day course would have the additional advantage of offering people an opportunity to get to know each other.

It was concluded that the training workshop should be a 2-day event in the spring of 2001, but not related to the FIRST conference. Andrew Cormack, Jacques Schuurman and Claudia Natanson would draft a programme outline and send that to the TF-CSIRT mailing list for comments. A subsequent version of the programme would then be presented by them at the next TF-CSIRT meeting in January 2001, where the details and the teachers could be filled in.

10. Relations with CEC. CSIRTs in *e*Europe 2002 Action Plan

The EU summit in Feira in June 2000 adopted the Action Plan *e*Europe 2002 "An Information Society for All". This plan lists a large number of actions, which the EU, the member states and the private sector should undertake in 2000, 2001 and 2002 to promote the Information Society in Europe. See http://europa.eu.int/comm/information_society/eeurope/pdf/actionplan_en.pdf . One of the actions (on the private sector, the CEC and the member states and to be implemented

before end 2001) reads: "Stimulating public/private co-operation on dependability of information infrastructures (including the development of early warning systems) and improve co-operation amongst national computer emergency response teams.".

Karel Vietsch reported that he had discussed this action item with people from the unit in the CEC services responsible for its implementation. They had no preconceived idea how to go about implementing this action and were looking very much to the CSIRTs themselves for their input. They had been unable to attend this meeting, but had invited a delegation from TF-CSIRT to come to Brussels in the near future to discuss possible actions with them.

Michel Dupuy referred to an e-mail with some suggestions that he had sent to the TF-CSIRT list on 25 September 2000. The CEC might sponsor the organisation of open meetings like EuroCERT had organised in the past, the organisation of training activities for new CSIRTs, the TI service and awareness raising actions, particularly directed towards commercial ISPs. As to the development of early warning systems, a first approach could be the set-up of a mail server reachable from the telephone network by means of a secure phone; CERTA could be the originator of such an initiative within TF-CSIRT.

Jacques Schuurman felt that such a mail server reachable by secure phone was a good proposal. It would however need a push mechanism and not be dependent only on the initiative of system managers to take action to make contact.

Pascal Delmoitié mentioned that in the EU context an emergency services network, based on radio links, is being built for the police, fire brigades and other emergency services. It could be a possibility to use that infrastructure.

It was agreed that the Secretariat would organise a meeting between a delegation from TF-CSIRT and the relevant CEC persons within the next weeks. The Secretariat would summarise the discussion under this agenda item in a briefing paper for the delegation. Don Stikvoort, Andrew Cormack, Michel Miqueu, David Parker, Jacques Schuurman and Gilles André volunteered to be part of the delegation.

11. Legal Issues and Relations with Law Enforcement Agencies

Andrew Cormack gave a short presentation. The Web site of the former SIRCE pilot http://www.eurocert.net contains pointers to computer law and legislation in European countries. He invited the meeting participants to have a look at these pages and send him more information and pointers to information on legislation and regulations in other countries.

Andrew Cormack also gave a short update on the legislation in the United Kingdom. Later this year a new law on "Regulation of Investigative Powers" will come into effect in England and Wales. Also the Human Rights Act will come into power in October.

These two acts will have significant consequences in a number of areas. One of them is anything related to interception.

12. Other Work Items

Clearinghouse for Incident Handling Tools

Yuri Demchenko mentioned that the clearinghouse page on the TF-CSIRT Web site contains links to freely available tools. It had been agreed earlier to discuss what to do about commercial tools and comments on them. He invited everyone to send him more information about tools.

Andrew Cormack reported that CERT/CC has stopped maintaining their archive of tools because it was too much work.

The meeting concluded that the reference page to tools should be kept on the TF-CSIRT Web site. If possible some testimonials on tools should be added. Yuri Demchenko will initiate a discussion on the TF-CSIRT mailing list.

13. Encouraging and Assisting New CSIRTs

Gorazd Bozic mentioned that it is difficult to convince networks that they should have a CSIRT. For example in August he had given a presentation at a CEENet workshop and found that there are almost no CSIRTs in the Central and Eastern European countries. Funding is the big problem there. A Europe directive might encourage the establishment of CSIRTs in those countries that are preparing to join the EU.

There were really two actions here: raising awareness, convincing networks that they should have a CSIRT; and helping those networks that do want to establish a CSIRT.

David Parker mentioned that this awareness raising was one of his main activities in the UK. There are national infrastructure protection agencies in other countries, and they could play a role here.

Claudia Natanson said that the arguments for establishing a CSIRT must be very different for commercial and for non-commercial networks. One question is whether a network is going to save money by having a CSIRT. She had some material on that from her own experience, which she would bring to the next meeting. A suggestion would be to ask the CEC for money to commission a study into the cost-benefits of having a CSIRT.

14. Date and Venue of Next Meeting

The next meeting will be hosted in Barcelona by ESCERT on 18 and 19 January 2001.

It was decided that the meeting after that will be in the spring of 2001, but not combined with the FIRST conference in Toulouse.

15. Any Other Business

According to the Terms of Reference of TF-CSIRT, criteria for subscription to the TF-CSIRT mailing list need to be defined before October 2000. Currently anyone can subscribe to the list via the Web page http://www.terena.nl/task-forces/tf-csirt/joinmail.html, subject to approval by the list owner. The list owner function is performed by Yuri Demchenko, who thus far had allowed people to subscribe if they claimed to have a reference from an existing TF-CSIRT member. However this had been abused and official rules were needed anyway.

After some discussion it was decided that from now on persons will only be subscribed to the mailing list if a current TF-CSIRT member asks to do so, by sending a request by e-mail to Yuri Demchenko. In the unlikely event that a person would want to subscribe to the list without knowing anyone on the list, Yuri will send a description of the person's background to the list, for TF-CSIRT members to decide electronically on the application. The TF-CSIRT Web pages must be changed to reflect this change in procedure.

Patrick Oonk mentioned that he had created a European incident mailing list where people can ask questions about incidents that they are confronted with.

16. SUMMARY OF ACTIONS

Action 0-2. Produce document(s) to explain benefits of TI to managers
Responsibility: TI

Action 0-3. Discuss and arrange server certificate for TI Web site
Responsibility: TERENA and TI

Action 0-9. Arrange seminar session about experiences with specific incident handling tools, adjacent to a future TF-CSIRT meeting
Responsibility: Secretariat

Action 0-10. Give a presentation at a future RIPE meeting
Responsibility: TI

Action 1-1. Submit a paper to present TF-CSIRT activities at the FIRST conference 2001
Responsibility: Gorazd Bozic

Action 1-2. Submit a paper to present the TI pilot service at the FIRST conference 2001
Responsibility: TI

Action 1-3. Send their slides to Yuri Demchenko
Responsibility: Speakers at Paris seminar sessions

Action 1-4. Arrange seminar session about current practice of CSIRTs, adjacent to the next TF-CSIRT meeting
Responsibility: Secretariat

Action 1-5. Prepare a discussion at the next TF-CSIRT meeting about a certification authority for the European CSIRT community
Responsibility: Don Stikvoort and Christoph Graf

Action 1-6. Ask Wilfried Wöber to explain to the TF-CSIRT mailing list the status of the discussion in RIPE on the security entry in the RIPE database
Responsibility: Gorazd Bozic

Action 1-7. Find out about (the availability of) the material from CERT/CC courses
Responsibility: Andrew Cormack

Action 1-8. Send a draft programme outline of the training workshop to the TF-CSIRT mailing list for discussion. Then update the outline so that the programme can be completed in the next TF-CSIRT meeting.
Responsibility: Andrew Cormack, Claudia Natanson, Jacques Schuurman

Action 1-9. Arrange a meeting between a TF-CSIRT delegation and CEC representatives on the action in the *e*Europe 2002 Action Plan. Summarise the discussion in the Paris meeting in a briefing paper for that meeting with the CEC.
Responsibility: Karel Vietsch

Action 1-10. Send pointers to legal information to Andrew Cormack
Responsibility: all

Action 1-11. Send information about incident handling tools to Yuri Demchenko
Responsibility: all

Action 1-12. Change the TF-CSIRT Web pages, to reflect the new procedure for subscribing to the mailing list.
Responsibility: Yuri Demchenko

Action 1-13
Organise next TF-CSIRT meeting in Barcelona on 18-19 January 2001
Responsibility: Jaime Agudo and Secretariat

Appendix A. 1st TF-CSIRT meeting Attendees list

	Name	Organisation
1	Jaime Agudo	ESCERT
2	Preben Andersen	DK-CERT
3	Gilles André	CERTA
4	Christos Aposkitis	GRNET-CERT
5	Jimmy Arvidsson	Telia CERT
6	Peter Bivestrand	NSIC
7	Gorazd Bozic	ARNES CERT
8	Ian Bryant	UK MODCERT
9	Roberto Cecchini	GARR-CERT
10	Andrew Cormack	JANET CERT
11	David Crochemore	Le CERT RENATER
12	Michelle Danho	Le CERT RENATER
13	Pascal Delmoitié	BELNET
14	Yuri Demchenko	TERENA
15	Michel Dupuy	CERTA
16	Per Arne Enstad	UNINETT CERT
17	Alberto Estevez	Integra
18	Matthias Etrich	Deutsche Telekom
19	Brian Gilmore	TERENA
20	Christoph Graf	SWITCH
21	Didier Gras	NOOS-SIRT
22	Pege Gustafsson	Telia CERT
23	Klaus-Peter	Stelvio

	Kossakowski	
24	Flemming Laugaard	DK-CERT
25	Jordi Linares	ESCERT
26	Chelo Malagon	IRIS-CERT
27	Jan Meijer	CERT-NL
28	Michel Miqueu	CERT-IST
29	Klaus Möller	DFN-CERT
30	Francisco Monserrat	IRIS-CERT
31	Robert Morgan	JANET CERT
32	Claudia Natanson	BT-CERT
33	Patrick Oonk	
34	David Parker	UNIRAS
35	Andrew Powell	UNIRAS
36	Dirk Reimers	Secunet
37	Jacques Schuurman	CERT-NL
38	Don Stikvoort	M&I/Stelvio
39	Taizo Suzuki	NOOS-SIRT
40	Karel Vietsch	TERENA