TSec(05)043

Minutes of the 15th TF-CSIRT meeting
Zürich, 13 May 2005

[Please note that a seminar was held the previous day. Presentations from the seminar and the meeting can be found at http://www.terena.nl/tech/task-forces/tf-csirt/meeting15/programme.html]

1. Welcome and apologies

Gorazd Božič welcomed the participants. The list of those present and the list of people who sent their apologies are below at the end of these minutes.

2. Approval of the Minutes and Status of Actions from the last meeting

The minutes of the last meeting held on 28 January 2005 were approved.

Action items:

14-01 Damir Rajnovic – to give a report about the Product vulnerabilities workshop in the next TF-CSIRT meeting.
Done. See agenda item 12.

14-02 Karel Vietsch – to report about the results from the meeting with FIRST about the responsibility for TRANSITS in Europe.
Done. See agenda item 4.1.

14-03 Gorazd Božič – to investigate if ENISA could give some funding for the TRANSITS workshops.
Ongoing. Gorazd Božič has mentioned this to Mr. Pirotti, but has not received any reply.

14-04 Baiba Kaškina – to send information about the LOBSTER questionnaire to the TF-CSIRT mailing list.
Done.

14-05 Andrew Cormack – to give an overview about the legal situation regarding network monitoring issues.
Done. See seminar's presentations.

14-06 Udo Schweigert – to discuss funding issues of joint meetings with the FIRST SC and report back to the TF-CSIRT group.
Done. See agenda item 6.

14-07 Jacques Schuurman – to circulate the final version of the Memorandum of Understanding to the TF-CSIRT mailing list.
Done. See agenda item 7.

14-08 All the teams – to Provide input to CHIHT.
Ongoing. See agenda item 8.

14-09 Marco Thorbrügge, Jacques Schuurman – to Review SURFnet's special language for incident handling and send the details to the TF-CSIRT mailing list.
Done. See agenda item 8.

12-08 Wilfried Wöber and Jan Meijer – to investigate which certificates are possible to use for the IRT objects and how to extend this list.
Done.

3. Update on e-coat

Don Stikvoort gave an update on the European cooperation of abuse fighting teams (e-coat) activities. The forum was founded to discuss pragmatic abuse handling issues. The 4th European Abuse Workshop was held on 11 May 2005 in Zürich before the TF-CSIRT seminar.

The forum was established almost two years ago and the participants felt that it needed a stronger structure. The operational framework was drafted in January 2005 and discussed in the 4th workshop. A few representatives have been elected to implement the framework. It has been decided that the participation costs in the forum for a team would be 300 EUR per year. Individual membership would be also possible for 100 EUR per year.

The e-coat would meet two times per year, at least one meeting would be adjunct to the TF-CSIRT event. The next e-coat meeting would be co-located with the RIPE-51 meeting in Amsterdam in October 2005.

Gorazd Božič asked if Don Stikvoort could give a more detailed presentation about the issues e-coat is working on in one of the following TF-CSIRT seminars. Don Stikvoort agreed to do that. He will investigate whether September or January event would be more appropriate.

ACTION 15-01: Don Stikvoort – to give a presentation about the issues e-coat is working on in one of the following TF-CSIRT seminars.

4. Update on the EC funded projects

4.1. TRANSITS

Karel Vietsch spoke about the TRANSITS project. He gave details about the 7 training courses which have been held during the lifetime of the project, including number of participants, represented countries, sectors, etc.

Karel Vietsch spoke about the agreement between TRANSITS and FIRST that FIRST would use the TRANSITS materials for courses in Latin America and the Asia-Pacific region during the lifetime of the TRANSITS project. A very successful course has been held in November in Rio de Janeiro for Latin America. The second training course organised by FIRST was held in Guilin, China on 22-23 March 2005. 91 trainees from 8 countries participated. The style of the workshops were different, but the feedback received has been very similar in all the regions.

The future of the TRANSITS materials and courses in Europe was discussed. An agreement was going to be prepared between TERENA and FIRST such that FIRST would continue organising training workshops in the Latin America and Asia-Pacific regions. FIRST would also provide funding for the FIRST secretariat (Don Stikvoort) to be the editor-in-chief and the repository for updating the TRANSITS materials. Between mid-2005 and mid-2006 FIRST and TERENA would jointly organise two training courses in Europe where participants would have to cover the real costs of the course. The agreement would be reviewed in mid-2006.

Karel Vietsch emphasised that volunteers would be needed to update all five TRANSITS modules (approximately 3 people per module) as well as trainers for the upcoming TRANSITS courses in Europe.

Andrew Cormack informed the group that there will be “Train the Trainers” event during the FIRST conference in Singapore mainly targeting the Asia-Pacific region representatives. David Crochemore will participate as trainer in a one-day TRANSITS course for Africa which will be organised together with the Africa network operators’ conference.

4.2. Relation to GN2, discussion on GN2/JRA2 advisory panel

Christoph Graf spoke about GN2's relationship with TF-CSIRT. He gave an overview of the GN2 project and all five JRA2 work items.

WI4 was the relationship with TF-CSIRT. The GN2 project could ask for advice from the task force, but no requests have been received so far. Christoph Graf mentioned a few requests where he has asked for more details but have not heard back.

WI5 was the establishment of the advisory panel. The panel was established two meetings ago. Christoph Graf also mentioned SWITCH's activities regarding the Critical Information Infrastructure Protection, see the seminar presentations.

The JRA2 meeting was held after the TF-CSIRT meeting.

5. ENISA update

Gorazd Božič gave an update about the latest developments regarding ENISA. The agency has been established, the director Mr. Pirotti participated in the last TF-CSIRT seminar in London. There was almost no permanent staff for the agency yet, was and they were still housed in the temporary offices in Brussels.

In order to move the agency to Heraklion, the Greek government has agreed to open daily direct flights Heraklion – Brussels, to establish an international school and nursery in Heraklion as well as to find a separate building for ENISA in the technical park of Crete. A total of 38 staff members would have to be recruited in two waves. They would be expected to start working respectively in September 2005 and November 2005.

The work plan 2005 has been approved. It will focus mainly on the staffing and logistical issues. Other sections of the work plan addressed awareness raising issues, enhancing cooperation regarding information sharing and other issues. Co-operation on European initiatives had a strong emphasis on collaboration with CERTs.

Andrew Cormack spoke about the ENISA Permanent Stakeholders Group (PSG). The PSG consisted of 30 people representing various communities and it had only an advisory role. The PSG would meet three times per year with the ENISA director and staff. The purpose of these meetings would be to maintain dialogue with external stakeholders and to advise ENISA on outputs useful to the stakeholders. The 2nd PSG meeting will take place in Brussels, Belgium on 2 June 2005.

The PSG did not comment on the work programme for the year 2005. This work programme was focusing on good practice sharing, awareness raising and co-operation with CERTs including promotion on creating new teams. Working groups would be created for these areas.

The PSG meeting has discussed the creation of the working groups, their Terms of Reference. There will be three working groups created in the year 2005, i.e. awareness raising, risk assessment techniques, CERTs and similar information sharing entities. The call for experts for these working groups has been issued, Andrew Cormack thanked all who has applied. The first meeting of the working groups was scheduled on 20 June 2005 in Brussels, Belgium.

The work programme for the year 2006 has been discussed in the PSG meeting, it should be approved in autumn 2005. ENISA would carry on all the activities from 2005 as well as start focusing on network and information security policies and technologies, computer incident response and handling policy and other areas. Andrew Cormack thought that there would be some possibilities to promote the TRANSITS approach. ENISA and TF-CSIRT both would benefit by advertising already achieved results. Instead of duplicating some results, ENISA would focus on promoting success stories in all the EU countries.

Andrew Cormack encouraged people to get involved and to express their opinion via all different channels possible.

6. Update on FIRST

Klaus-Peter Kossakowski spoke about the latest activities in FIRST. He gave an overview of the European activities historically and pointed out TERENA's role there. Regarding the future, he

proposed to discuss possibilities of joining effort of both organisations for organising European meetings.

It has been agreed to organise the FIRST Technical Colloquium (TC) and the TF-CSIRT January 2006 meeting together. It should be a three-day event with seminar, business meeting, hands-on day and working group meetings. Klaus-Peter Kossakowski spoke about the access rules for the joint event and emphasised that both groups should agree to limit the restrictions to the minimum possible.

Damir Rajnovic asked whether a Steering Committee (SC) meeting would be held during those three days as well. Klaus-Peter Kossakowski replied that the SC meeting should be held either before or after the event.

Karel Vietsch proposed to keep the rules and organisation as simple as possible. Baiba Kaškina from the TERENA side and a person from FIRST side should come together and organise the event. Gorazd Božič proposed that he as the TF-CSIRT chairman could approve participations for the European meeting. Klaus-Peter Kossakowski agreed that FIRST could delegate the authority to control access to the TF-CSIRT chair, but that still should be discussed.

Andy Bone asked how easy it would be for new teams to join this event. Klaus-Peter Kossakowski replied that the last FIRST event in Latin America has been an open meeting. FIRST has been changing its policy and getting less bureaucratic, the conditions for new teams should be the same as for the TF-CSIRT event only.

The group agreed to co-locate the TF-CSIRT January 2006 meeting with the FIRST TC. The possible host for the meeting could be Cisco. The meeting will be organised joining effort from TERENA and FIRST.

7. Memorandum of Understanding with APCERT

Jacques Schuurman spoke about the Memorandum of Understanding (MoU) between TF-CSIRT and APCERT. The purposes of the MoU would be mutual recognition as regional expertise bodies, provision of an established channel of information exchange, establishment of a framework for joint project undertakings, direct operational contact points, etc. He pointed out that the third point regarding the information sharing has been changed according to the group's suggestions.

Wilfried Wöber wanted to clarify if teams or individuals were meant as members. Jacques Schuurman clarified that the individuals were meant. Kauto Huopio asked if the list of the TF-CSIRT members (individuals) existed. Gorazd Božič explained that it is the TF-CSIRT mailing list.

It was agreed that the MoU would be signed during the FIRST conference in Singapore in June 2005 by Gorazd Božič. The liaison person with AP-CERT would be approved after signing the MoU. Gorazd Božič asked the group to think about the possible liaison candidates and to discuss that in the next TF-CSIRT meeting.

8. Improvements to CHIHT

Marco Thorbrügge gave an update on the CHIHT improvements. The main goal of the CHIHT is to support new teams. He demonstrated different tool categories. Information about teams using the particular tool has been added lately. "More information" field has also been added for almost all tools.

So far 4 teams has filled the questionnaire regarding the tools they were using. Marco Thorbrügge informed other teams that in future he would gather information via phone interviews. He asked the teams to be ready to cooperate. He would start with the SI-CERT and SURFnet-CERT.

Marco Thorbrügge summarised that he was happy with the new CHIHT look and has received a lot of positive feedback.

9. Update on the IRT object

Jan Meijer informed the group about the latest developments of the IRT object in the RIPE database. The "signature:" and "encryption:" attributes have been made optional, the –c flag was working with the whois query tool, abuse-mailbox has been added. He presented the amount of various objects which had the "abuse-mailbox:" field added.

An open issue was whether to ask the RIPE NCC to implement the IRT object link from the aut-num objects. The issue was discussed and it was agreed that currently there was no strong demand from the group for that. Jan Meijer suggested continuing this discussion on the mailing list.

He asked which teams did not have the IRT object yet. Some teams complained that setting up their IRT object has been delayed from the TI side. Jan Meijer clarified that it should not take more than a week for the TI and RIPE to set up an IRT object.

10. Update on VEDEF WG

Ian Bryant gave an overview of the VEDEF working group. He recalled the background of this working group and spoke about the relationship to other initiatives.

The working group will organise a BoF during the FIRST conference, particularly to discuss collaboration with the JP-CERT/CC. The linkage to the ENISA work programme should be investigated. The VEDEF webpage would be on-line soon. Also interim BoFs at IETFs were considered for visibility.

11. Update on RTIR working group

Carlos Fuentes gave an overview of the RTIR tool and the working group activities. RTIR was the only open source incident handling tool. The RTIR WG met on 11 May 2005 in Zürich before the TF-CSIRT event.

It has been agreed to start a new project with BestPractical to improve the RTIR tool. Carlos Fuentes spoke about the new features of the tool. The money for the project would be collected from the participating teams. The teams will have an agreement with TERENA and TERENA with BestPractical. The Code of Conduct has been signed by all the teams. The last WG meeting had finalised the Statement of Work. The start of the project will be June or July 2005, duration – 18 months with 3 milestones. After the each milestone the teams would check the developed product against the requirements document.

A new mailing list rtir@terena.nl has been created for the WG. Carlos Fuentes encouraged new teams to join the WG.

Andy Bone asked if there would be training courses after the completion of the project. Carlos Fuentes thought that courses would be organised by BestPractical free of charge for the participating teams.

12. Update on the vendor/product vulnerability workshop

Damir Rajnovic informed the group about the vendor/product vulnerability workshop which was held on 9 February 2005 in Paris, France. 10 vendors had participated - Alcatel, Skype, Netasq, Nokia, Ericsson, Sun, Hitachi and Cisco. CERT/CC was invited as a guest. All the participating vendors have been added to the FIRST vendor list.

The group discussed various product related issues. The consensus of the meeting was that it has been useful and should be repeated. The date and venue for the next meeting has not been determined yet. Most probably it will be later on this year in USA to involve teams from that region.

13. CSIRT mentoring scheme

Andrew Cormack spoke about the initiative to formalise assistance providing to the new teams. So far it had happened only informally. The goal of this initiative would be to make it easier to find a mentor team.

TERENA would provide a known point of contact. Teams willing to help others would inform TERENA about their possibilities and preferences. Teams seeking assistance would ask TERENA for a mentor team. TERENA would try to find an appropriate and willing partner.

Andrew Cormack emphasised that being in the list would not commit teams to provide help. It should always be decided by the team on a case-by-case basis. The entire proposed procedure was available on-line. Andrew Cormack also outlined expectations from the mentor and mentored teams.

Damir Rajnovic pointed out documents about site visits from Cisco and CERT.CC which might be useful for the mentor teams. Gilles Andre raised the issue on how to avoid hacker mentoring. The consensus was that in case of any suspicion the mentoring could be denied. Miroslaw Maj asked whether the mentoring process still could be done directly without involving TERENA. Andrew Cormack thought that it would be fine, but some feedback should be provided to the community. He emphasised that it would not be a rule for new teams to go through the mentoring process.

The group accepted this proposal. It was agreed that Baiba Kaškina would set up a special email address to collect information about mentor teams and those seeking assistance. When the list of mentor teams would be sufficiently long, the website should be linked and the initiative advertised in the TF-CSIRT community and elsewhere.

ACTION 15-02: Baiba Kaškina - to set up email address for the CSIRT mentoring initiative, link the webpage and advertise the initiative.

14. Results of the seminar sessions, ideas for the future sessions

Gorazd Božič summarised that the informal feedback after the first day regarding the new schedule has been positive. The same schedule will be used in the next TF-CSIRT event. He encouraged people to fill the evaluation forms.

The one-after-next TF-CSIRT event will be together with the FIRST Technical Colloquium, the schedule for that should be discussed in the next TF-CSIRT meeting.

15. Status of the Terms of Reference and other TF-CSIRT work items/deliverables

Gorazd Božič summarised that the progress of the work items and deliverables has been discussed during the meeting and there was no need to review the Terms of Reference.

Andrew Cormack mentioned that there might be some additions in the ToR regarding the ENISA work item of supporting new CERT teams.

16. Date of the next meetings

The next meeting will be held on 15-16 September 2005 in Lisbon, Portugal (hosted by FCCN/CERT.PT). The group was invited to Lisbon and some pictures from the city and the planned venue were showed.

The subsequent TF-CSIRT meeting will be hosted by Cisco either in Amsterdam or Brussels on 25-27 January 2006. It was tentatively agreed to have the following meetings in Lithuania and Finland.

17. Any Other Business

Gorazd Božič and the group expressed their thanks to SWITCH-CERT for organising a perfect meeting.

Damir Rajnovic raised the issue about the deputy chair of the task force. He thought that since Andy Bone has left JANET-CERT a new deputy chair should be found. The participants discussed how to find the deputy chair and it was agreed that Gorazd Božič would choose the deputy chair and the group would have to approve the candidate.

ACTION 15-03: Gorazd Božič – to choose the candidate for the deputy chair and to ask the approval from the TF-CSIRT group.

List of meeting participants

	Name	*Organisation*	*Country*
1.	Gilles André	CERTA	France
2.	Andy Bone	JANET-CERT	United Kingdom
3.	Gorazd Božič (Chair)	SI-CERT	Slovenia
4.	Ian Bryant	NISCC	United Kingdom
5.	Andrew Cormack	UKERNA	United Kingdom
6.	Michelle Danho	RENATER CERT	France
7.	Serge Droz	SWITCH-Cert	Switzerland
8.	Till Dörges	PRESECURE	Germany
9.	Ralf Dörrie	Telekom-CERT	Germany
10.	Renato Ettisberger	SWITCH-CERT	Switzerland
11.	Lionel Ferette	BELNET	Belgium
12.	Carlos Fuentes Bermejo	JANET-CERT	United Kingdom
13.	Manuel Garcia	esCERT-UPC	Spain
14.	Rolf Gartmann	SWITCH-CERT	Switzerland
15.	Luis Gomez	esCERT-UPC	Spain
16.	Christoph Graf	SWITCH-CERT	Switzerland
17.	Oliver Göbel	RUS-CERT	Germany
18.	Peter Haag	SWITCH-CERT	Switzerland
19.	Peter Hammond	NISCC	United Kingdom
20.	Hans Hoogstraaten	TNO	Netherlands
21.	Kauto Huopio	FICORA / CERT-FI	Finland
22.	Przemek Jaroszewski	CERT Polska / NASK	Poland
23.	Nino Jogun	CARNet CERT	Croatia
24.	Pavel Kacha	CESNET z.s.p.o.	Czech Republic
25.	Baiba Kaškina (Secretary)	TERENA	-
26.	Ulrich Kiermayr	ACOnet-IRT	Austria
27.	Adrian King	SI-CERT	Slovenia
28.	Klaus-Peter Kossakowski	PRESECURE	Germany
29.	Andrea Kropacova	CESNET z.s.p.o.	Czech Republic
30.	Jan Lönnqvist	Ericsson	Sweden
31.	Stelios Maistros	GRNET-CERT	Greece
32.	Miroslaw Maj	CERT Polska	Poland
33.	Chelo Malagón	IRIS-CERT, RedIRIS	Spain
34.	Stanislas De Maupeou	CERTA	France
35.	Jan Meijer	SURFnet / CERT-NL	The Netherlands
36.	John Millar	BT CERT	United Kingdom
37.	Maurizio Molina	DANTE	United Kingdom
38.	Robert Morgan	JANET-CERT	United Kingdom
39.	Gustavo Neves	FCCN (CERT.PT)	Portugal
40.	Tomasz Nowocien	PIONIER-CERT	Poland
41.	Carol Overes	GOVCERT.NL	the Netherlands
42.	Joao Pagaime	FCCN	Portugal
43.	Leila Pohjolainen	Funet CERT	Finland
44.	Peter Quick	Telekom-CERT	Germany
45.	Damir Rajnovic	Cisco Systems	United Kingdom
46.	Jacques Schuurman	SURFnet / CERT-NL	The Netherlands
47.	Sharon Sciberras	mtCERT	Malta
48.	Don Stikvoort	Trusted Introducer	the Netherlands
49.	Thomas Stridh	SUNet CERT	Sweden
50.	Harri Sylvander	Funet CERT	Finland
51.	Jouni Säkkinen	Ericsson	Finland
52.	Jonas Thambert	SITIC	Sweden
53.	Marco Thorbrügge	DFN-CERT	Germany
54.	Maris Urkis	LITNET CERT	Lithuania
55.	Koen Van Impe	BELNET CERT	Belgium

56. Karel Vietsch	TERENA	-
57. Peter Wallström	SITIC	Sweden
58. Wilfried Wöber	ACOnet-IRT	Austria

Apologies were received from:

Claudio Allocchio	GARR-CERT	Italy
Preben Andersen	DK-CERT	Denmark
Jimmy Arvidsson	TeliaSoneraCERT CC	Sweden
Martin Camilleri	mtCERT	Malta
Per Arne Enstad	UNINETT CERT	Norway
Mikhail Ganev	RU-CERT	Russia
Natasa Glavor	CARNet CERT	Croatia
Richard Jones	BT SBS	United Kingdom
Janos Mohacsi	NIIF/HUNGARNET	Hungary
Tom Mullen	BTCERT	United Kingdom
David Parker	UNIRAS/NISCC	United Kingdom
Olav Seyfarth	Telefónica Deutschland	Germany

RESULTING ACTION ITEMS

15-01	Don Stikvoort	Give a presentation about the issues e-coat is working on in one of the following TF-CSIRT seminars.
15-02	Baiba Kaškina	Set up email address for the CSIRT mentoring initiative, link the webpage and advertise the initiative.
15-03	Gorazd Božič	Choose the candidate for the deputy chair and to ask the approval from the TF-CSIRT group.
14-03	Gorazd Božič	Investigate if ENISA could give some funding for the TRANSITS workshops.
14-08	All the teams	Provide input to CHIHT.