

19th TF-CSIRT meeting

September 21-22, 2006

Espoo, Finland

Author: Cătălin Meiroșu – Issue 2

1. Welcome and apologies

Gorazd Božič welcomed the participants to the 19th TF-CSIRT meeting. The list of registered attendees is attached at the end of these minutes.

2. Address by the directors of CSC and FICORA

Welcome to CSC - Kimmo Koski, Managing Director of CSC

Kimmo Koski welcomed the TF-CSIRT meeting participants to CSC. CSC was founded in 1971, and is operated as a not-for-profit organisation. The organisation was headquartered in Keilaniemi, Espoo, since March 2005. Some 140 people carried on research and technical work at CSC during 2005. CSC provides services to universities, polytechnics and companies in a number of areas, including FUNET, computational services, applications services and information management services. The FUNET CERT was founded in 1995. It has an increased focus on international cooperation. New development projects include the HAKA federation and Grids-related activities.

Welcome to TF-CSIRT 19 - Rauni Hagman, Director-General of FICORA

Rauni Hagman welcomed the TF-CSIRT members to the meeting co-hosted by CSC and FICORA. Rauni Hagman presented the activity areas of FICORA, Finland's national network and information security authority. FICORA operates the CERT-FI team, the registrar of the .fi domain name and was developing ENUM services. CERT-FI was established in January 2002 as a coordination civil authority for Finnish CERT teams, with a focus on telecommunication service providers and critical national infrastructures. Additional resources to serve organisations in the area of critical infrastructure protection will be made available in 2007.

3. Approval of the minutes and status of the Action Items from last meeting

The minutes of the last meeting, held on the 24th of May, were approved.

4. Action Items from previous meetings

All actions items were cleared, except item 17.1. Gorazd Božič suggested Wilfried Wöber to contact Jacques Schuurman, the TF-CSIRT liaison office with APCERT.

5. Availability and Robustness of Electronic Communications Infrastructures (ARECI) study - Alexei Resetko

Alexei Resetko gave an overview of the ARECI study, carried out by Lucent under a contract with the European Commission's Directorate-General Information Society and Media. ARECI will provide an analysis of the factors influencing the availability of electronic communications infrastructure in Europe. The study will make recommendations at policy level.

The study will aggregate information obtained through a variety of sources, including interviews with several categories of actors like the European Union's member states, telecommunications operators, industry associations, etc. The result is expected to provide a balanced view of network resources and security risks associated to them. An important contribution to the study will be brought by Bell Labs experts.

Several workshops will be organised by different stakeholders in the timeframe from October 2006 to January 2007. The ARECI team will integrate the results of these workshops in a final report, expected to be released in February 2007.

CSIRTs have a strong role in assuring the availability and security of telecommunication infrastructures. Therefore, the ARECI project team would like to invite members of TF-CSIRT to participate in the ARECI workshops. By participating in the workshops, the CSIRTs will have the opportunity to influence guidance being prepared for the EC on the availability and robustness of Europe's networks.

6. Report from the E-CoAT workshop - Don Stikvoort

Don Stikvoort reported on the E-CoAT workshop held on the 20th of September in Espoo. The E-CoAT concept was born in 2004 to support the activities of large ISPs in fighting increasing abuse on their networks. The forum had a strong orientation towards operational aspects. The draft conclusions of the workshop could be summarised as follows:

- a bigger yearly workshop would be preferred instead of separate meetings
- closer cooperation with TF-CSIRT would be desired
- concentrate the workshop on a few topics, like whitelisting, best current practices and Trusted-Introducer-like schemes
- the need for involving professional people in fighting network abuse was reiterated.

Gorazd Božič thought that maybe members of TF-CSIRT or other people from their respective organisations would be interested to participate in future E-CoAT meetings. His personal opinion was that the best option for organising a larger event for E-CoAT would be to co-locate it with the TF-CSIRT meeting held during the month of May.

7. TRANSITS Courses – Karel Vietsch

Karel Vietsch presented the TRANSITS courses. This successful series of training courses addressed to computer security professionals started as a TF-CSIRT initiative. It was partly funded as a European project by the European Commission from July 2002 until September 2005. The structure of the training course was based on five modules covering organisation, operational, technical, legal and vulnerability-related topics. The two days of the workshop were always very intense with 12-14 hours of work. In addition to the technical content, the TRANSITS courses were also a good introduction for new members to the CSIRT community. The European project finished in September 2005, but a memorandum of understanding between FIRST and TERENA made the continuation of the courses possible. The course material is being maintained by the FIRST Secretariat. The updating of the material depends on volunteers from the CSIRT community. Last year, a major overhaul of the course content was done by the SWITCH CERT team. Two training courses were organised in Europe after the end of the TRANSITS project: in Vienna (November 2005, sponsored by ISPA) and Vilnius (March 2006, co-organised and sponsored by ENISA). Karel Vietsch concluded his presentation by announcing the third post-TRANSITS edition of the training courses. This will take place in Morschach, Switzerland, on 30 November – 1 December 2006. The workshop will also be co-organised and sponsored by ENISA. The registration fees were priced very competitively.

8. Summary of the IRT object workshop - Wilfried Wöber

Wilfried Wöber reported on the RIPE IRT object workshop, held on the 20th of September in Espoo. The attendance was limited to about 20 people by the places available in the room. The content of the session was well appreciated by the participants. The slides will be made available on the TF-CSIRT website. Wilfried Wöber received several suggestions on how to improve the material. For some people, most of the work was related to maintaining the IRT objects that they stored in the database. Wilfried Wöber announced that there will be a database group meeting during the RIPE meeting in Amsterdam, on Oct 6th. Wilfried Wöber urged the community to subscribe to this working group. He also invited all the TF-CSIRT members interested in the topic to participate in the RIPE meeting. In case the community would be interested in a re-run of the workshop, Wilfried Wöber asked the attendees to get in touch either with him or with Gorazd Božič or Cătălin Meiroșu. He thought that part of the material could be included in the TRANSITS courses, or a workshop could be organised adjacent to TF-CSIRT meetings as would be considered useful.

Gorazd Božič asked if Wilfried Wöber had data on how many teams connected inetnum objects to their IRT object. Wilfried Wöber answered that he could not give a number on the spot, but he could ask Ulrich Kiermayer to re-run his scripts and Wilfried Wöber would report on the results at the next TF-CSIRT meeting.

Action item 18-1. Wilfried Wöber to report on the number of teams that connected inetnum objects to their IRT object in the RIPE database.

Gorazd Božič asked Wilfried Wöber whether he received any replies on his question regarding the cyberabuse.org website. Wilfried Wöber thought the website contained a good write-up about the mechanisms used to build that service. However, he noted that there was no mention of AfriNIC on the site, and he tried several queries but only a few of his examples worked. Wilfried Wöber received some comments from people on the FIRST chat, but those were not very useful. Wilfried Wöber agreed with Gorazd Božič that what was available right now seemed to be an abandoned website. Gorazd Božič asked the attendees whether somebody was using this site on a regular basis. None of the attendees appeared to be doing so.

Gorazd Božič asked Wilfried Wöber if he knew who was developing the whois client that was available in Linux. Wilfried Wöber answered that some of the Linux distributions just used an alias to finger commands. He was aware of discussions within the RIPE community to get the RIPE NCC whois client to become part of Linux distributions, but had no feedback on that yet. He offered to contact RIPE NCC for an update.

Action item 18-2. Wilfried Wöber to contact RIPE NCC regarding the plans to include the RIPE NCC whois client in Linux distributions.

9. Update on ENISA activities - Marco Thorbrügge

Marco Thorbrügge provided the audience with an outlook on the activities of ENISA. ENISA is a centre of expertise that was setup to advise the member states as well as various bodies of the European Union. During 2006, the focus of the relationship between the organisation and CSIRTs was supporting new teams. For 2007, the accent will be put on supporting existing teams for successfully serving their constituency. ENISA will consider funding other training courses, like the CERT-CC training for example. In addition to the support for existing CSIRTs, ENISA will add a new focus on users and user groups. This will be related to user needs for security services deciding what would be the best entity that should provide these services. An ad-hoc working group was already setup in 2006, analysed user group need for specific CSIRT services and provided a list of possible measures for quality assurance. Marco Thorbrügge invited the attendees to participate in a series of events organised by ENISA during the autumn of 2006.

Gorazd Božič asked Marco Thorbrügge what was the ENISA view on the possibility to offer long-term support for the TRANSITS courses. Marco Thorbrügge said that TRANSITS was very well regarded by the European Commission. For the moment, ENISA just contributed financially to the courses, but he felt that they could do more.

Gorazd Božič was aware that a deliverable addressing fostering cooperation between CSIRTs was prepared by ENISA. He asked Marco Thorbrügge what would be the focus and depth of the document. The purpose of the document would be to show stakeholders how cooperation works and point towards how it could be deepened by the stakeholders. Marco Thorbrügge hoped that the document will be finalised by the end of October. When the document will be finalised it will be made publicly available by ENISA.

Marco Thorbrügge continued to maintain the Clearing House of Incident Handling Tools (CHIHT), located on the DFN-CERT website, in his spare time since he joined ENISA. He proposed that the CHIHT could be re-located to the ENISA website. ENISA would ensure a regular update of the pages, while still maintaining it as a TF-CSIRT initiative. Karel Vietsch noted that the CHIHT pages should remain branded as TERENA / TF-CSIRT in order to acknowledge the contribution of the community in its development. Marco Thorbrügge suggested that this, together with other aspects related to the maintenance of the content of the CHIHT, could be discussed with ENISA's legal adviser. He agreed to ask ENISA's legal advisor to discuss with Karel Vietsch the formalities that would allow ENISA to host the CHIHT.

Action item 18-3. Marco Thorbrügge to put ENISA's legal advisor in contact with Karel Vietsch regarding the CHIHT.

10. Christoph Graf – GEANT2 Security

Christoph Graf presented the new developments in the Joint Research Activity 2 (JRA2) work package of the GEANT2 project. The activity is targeted at improving the overall security within the GEANT2 community. Christoph Graf briefly reviewed the JRA2 activities to date. A requirements document for the JRA2 Toolset (composed of FlowMon and nfsen) was made public. The work subsequently focused on advanced anomaly detection. The first case of formalised network security advice from TF-CSIRT to GEANT2 was completed successfully and the result was made available as a deliverable. The focus of JRA2 within the third year of the GEANT2 project will be on service implementation and advanced services. A minimum set of security standards will be defined for all the GEANT2 project partners. JRA2 will actively help all partners reach this standard. The advanced services will include anomaly detection within the GEANT2 network and further development of the flow probe. The JRA2 meeting to be held on the 22nd of September after the TF-CSIRT seminar will address the GN2 Service Security deliverable. JRA2 will start working on a set of recommendations for all project partners on how the recommendations in this deliverable could be met.

11. Date and venues for the next meetings

It was agreed that the next (20th) TF-CSIRT meeting will be organised together with the FIRST Technical Colloquium in Budapest, on January 29-31, 2007. It was suggested that the format of the meeting follows that of the similar meeting held in January 2006 in Amsterdam. The host of the 20th TF-CSIRT meeting will be CERT-HUNGARY.

The 21th TF-CSIRT meeting will be held on May 3-4, 2007 in Prague and will be hosted by CESNET CERT.

Summary of the action points

17-1 – Wilfried Wöber – Ask Yuri Ito about possibilities to present the IRT object in the next APNIC conference.

18-1 – Wilfried Wöber – Report on the number of teams that connected inetnum objects to their IRT object in the RIPE database.

18-2 – Wilfried Wöber – Contact RIPE NCC regarding the plans to include the RIPE NCC whois client in Linux distributions.

18-3 – Marco Thorbrügge – Ask ENISA’s legal advisor to contact with Karel Vietsch regarding the CHIHT.

List of attendees

First Name	Surname	Organisation
		Lucent Technologies, European Security Practice
Aleksei	Resetko	Practice
Andrea	Kropacova	CESNET
Andreas	Bunten	DFN-CERT
Andrew	Cormack	UKERNA
Antti	Tassberg	NIRT
Ari	Husa	FICORA / CERT-FI
Arto	Tuomi	CSC - Scientific Computing Ltd
Arturs	Medenis	LATNET
Asia	Slowinska	Vrije Universiteit
Baiba	Kaskina	LATNET
Barbara	Monticini	GARR-CERT
Carol	Overes	GOVCERT.NL
Chelo	Malagon	RedIRIS/IRIS-CERT
Christoph	Graf	SWITCH
Claudio	Allocchio	GARR-CERT
Cătălin	Meiroşu	TERENA
Dan	Bailey	NISCC
Daniel	Schirmer	ACOnet CERT
Darko	Androcec	CARNet
Derek	Simpson	BT CERT CC
Dmitry	Avramenko	RU-CERT
Erka	Koivunen	FICORA / CERT-FI
Francisco	Montserrat	
Jesus	Coll	RedIRIS/IRIS-CERT
François	KHOURBIGA	CERTA
Geoff	Jones	NISCC
Gilles	Andre	CERTA
Gorazd	Božič	SI-CERT (ARNES)
Gustavo	Neves	CERT.PT
Harri	Sylvander	Funet CERT/CSC
Hillar	Aarelaid	CERT-EE
Jaap	van Ginkel	Univeristeit van Amsterdam/SURFnet-CERT
Jacques	Schuurman	SURFnet-CERT
Jamie	Hughes	NISCC

Jan	Lönnqvist	Ericsson PSIRT
Janos	Mohacsi	NIIF/HUNGARNET
Jimmy	Arvidsson	TeliaSoneraCERT CC
Johanna	Kinnari	FICORA / CERT-FI
John	Harding	BT (Secure Business Services)
Juhani	Eronen	FICORA / CERT-FI
Jussi	Vahtera	NIRT
Jyrki	Yli-Paavola	TeliaSoneraCERT CC/TSF
Karel	Vietsch	TERENA
Kauto	Huopio	FICORA / CERT-FI
Konstantin	Knorr	Siemens
Ladislav	Lhotka	CESNET
Leila	Pohjolainen	Funet CERT/CSC
Lionel	Ferette	BELNET CERT
Luchesar	Iliev	IPP-BAS/ISTF
Marco	Thorbruegge	ENISA
Margrete	Raaum	NorCERT
Marius	Urkis	LITNET CERT
Mats	Melin	Ericsson PSIRT
Matthieu	Saussay	CERTA
Maurizio	Molina	DANTE
Mehis	Hakkaja	ENISA
Michelle	DANHO	CERT-RENATER
Mikhail	Ganev	RU-CERT
Milda	Mimiene	LITNET CERT
Natasa	Glavor	CARNet
Nino	Jogun	CARNet
Orod	Badjelan	DK-CERT
Paavo	Ahonen	CSC - Scientific Computing Ltd
Pavel	Kácha	Cesnet
Pekka	Kytölaakso	Funet CERT/CSC
Peter	Haag	SWITCH
Peter	Wallström	SITIC
Przemek	Jaroszewski	CERT Polska / NASK
Raymond	Azzopardi	mtCERT
Robert	Morgan	JANET-CERT
Roberto	Cecchini	GARR-CERT
Sergey	Bunyakov	RU-CERT
Sergey	Linde	RU-CERT
Stelios	Maistros	GRNET-CERT
Thomas	Stridh	SUNet CERT
Timo	Porjamo	CSC - Scientific Computing Ltd
Toni	Koivunen	FICORA / CERT-FI
Tony	Falenius	CSC
Urpo	Kaila	Funet CERT
Victor	Sant'Anna	Ericsson PSIRT
Wilfried	Wöber	ACOnet CERT
alexander	talos	ACOnet
christoph	sprongl	ita
teun	Nijssen	SURFnet-CERT
wolfgang	mader	ita