Approved Minutes of the 23rd TF-CSIRT Meeting
28 January 2008 – Prague, Czech Republic

[Please note that a seminar was held the following day. All presentations can be found at http://www.terena.org/activities/tf-csirt/meeting23/]

1. Approval of Minutes

The minutes of the last meeting held on 20 September 2007 were approved.

2. Actions from last meeting

22.1 Jacques Schuurman asked Hillar Aarelaid if he could get in touch with the APCERT people regarding the incidents in Estonia.
- Done.

22.2 Jacques Schuurman to check with AuCERT (and perhaps JPCERT) who was already involved in the out-of-band communications project and what would be required from potential volunteer European teams.
- Ongoing.

22.3 Gorazd Božič to coordinate with the local organisers the dates for the May 2008 TF-CSIRT meeting.
- Done, the dates had now been set.

22.4 Gorazd Božič and the TF-CSIRT secretary to schedule discussion on holding a meeting in Russia at the next TF-CSIRT meeting in January.
- No information had been received as yet, but Gorazd would make a decision before the next TF-CSIRT meeting.

21.1 Christoph Graf to check the public flag on the GN2 JRA2 deliverables on the toolset and announce on the TF-CSIRT mailing list when they will be available.
- Ongoing.

18.1 Wilfried Wöber to report on the number of teams that have linked their Inetnum objects to their IRT object in the RIPE database.
- Superseded.

18.2 Wilfried Wöber to contact RIPE NCC regarding plans to include the RIPE NCC Whois client in Linux distributions.
- Done. The RIPE NCC had contacted the Linux distribution maintainers, but not sure of current status.

18.3 Wilfried Wöber to send updated text for Work Item D (assisting the establishment of new CSIRTs) of the TF-CSIRT Terms of Reference.
- Superseded.

3. TR-CERT Presentation

Mehmet Eris gave a presentation about TR-CERT, the Turkish government CSIRT that had recently been established (see http://www.terena.org/activities/tf-csirt/meeting23/eris-trcert.pdf). It was aiming to build an incident response capability within Turkey between government organisations, and any other related party. It also aimed to handle international incidents, build knowledge and experience within its constituency, and obtain a nationwide incident picture.

TR-CERT fell under the auspices of the Scientific and Technological Research Council of Turkey (TÜBITAK) which reported directly to the Prime Minister and acts as an advisory agency to the Turkish government. Under this was the National Research Institute of Electronics and Cryptology (UEKAE), of which the Network Security and Common Criteria was a part. This hosted TR-CERT at its two offices in Ankara and Gebze (40 km from Istanbul).

The TR-CERT project entered its pilot phase in January 2008 and aimed to go fully operational in September 2008. As well as providing incident coordination and handling services, it would also offer CSIRT training to the banking and telecommunications sectors as well as government organisations. However, TR-CERT had no authority over its constituency and provided its services on a voluntary basis only.

Kauto Huopio asked about the willingness of Turkish ISPs to respond to security issues. Mehmet replied that national legislation existed to ensure ISPs had to respond, although this did not cover phishing and certain other activities.

Gorazd Božič asked whether international CSIRTs could send incident reports to TR-CERT. Mehmet replied they could handle some, although they only had two people working full-time on CSIRT activities.

4. RIPE Database Update

Wilfried Wöber provided an update on the RIPE database (see http://www.terena.org/activities/tf-csirt/meeting23/woeber-ripedb.pdf). The IRT object was now returned by default, and abuse mailbox addresses had been added. This had triggered a major rework of the documentation set, which was now complete.

The RIPE Data Protection Task Force had been working on how to make the RIPE database compliant with EU data protection legislation. Although it was argued that a resource registry service was in the public interest, certain measures were still necessary to ensure compliance. As a result, it had been proposed to remove all orphaned person objects, as well as remove or strictly limit the White Pages functionality. A maintainer would also be required for all objects including person and role. There was a further proposal for a new NRTM (Near Real-Time Mirroring) service that excluded personal data, in conjunction with a limit on queries to the live database.

There were still some open issues with respect to the maintainer object, and how to deal with all the legacy information. This problem was being exacerbated with resource certification and by the scarcity of IPv4 addresses.

Andrew Cormack said that a possible solution to the problem of a non-responsive maintainer would be to replace them with the RIPE NCC, who could then make the necessary changes. Wilfried thought this was a good idea, although it would be quite a lot of work. However, they were increasingly in that situation anyway.

5. Update on CHIHT

Gorazd Božič gave a short report on the Clearing House for Incident Handling Tools. This had been maintained by Marco Thorbrugge when he was at DFN-CERT, and he proposed to continue this work now he was at ENISA. A few more teams had responded, and there should be more activity in the near future. Marco was planning to send an update to the mailing list shortly.

6. Update on TRANSITS Training Courses

Karel Vietsch reported on TRANSITS training courses. (see http://www.terena.org/ activities/tf-csirt/meeting23/vietsch-transits.pdf). These had started as an EU-funded project under whose auspices seven workshops were held. There followed two workshops in collaboration with FIRST, and since then TERENA had continued to organise at least two workshops per year in collaboration with other organisations.

Other organisations have also organised training workshops using the TRANSITS material, both within and outside of Europe. The training material was available under licence from TERENA, and continued to be maintained and updated by Don Stikvoort.

The next TRANSITS workshop would be held on 24-25 April 2008 in Egmond-aan-Zee, The Netherlands. This was being organised by TERENA, with sponsorship from ENISA and GOVCERT.NL. More information could be found at http://www.terena.org/activities/csirt-training/holland/, although the deadline for applications was 29 February 2008.

7. Update on ENISA

Andrew Cormack provided an overview of the European Network and Information Security Agency (see http://www.terena.org/activities/tf-csirt/meeting23/cormack-enisa.pdf). This was not a European CSIRT, but rather advised EU member states and the European Commission on how to develop a culture of security.

The agency was created in 2004, initially for a period of five years, and had 54 staff. It was managed by a board comprised of representatives of member states (including Gorazd Božič), the EC, and consumer groups who dealt with financial and political

issues. There was also a Permanent Stakeholders' Group comprised of 30 individuals (including Andrew Cormack) that advised on the technical work programme.

The agency focused on raising awareness of network security, risk assessment, examining new technologies, supporting new CSIRTs, and handling requests from the EC. Its current mandate was due to end in 2009, and whilst it had received a favourable external review, it was felt to be too small. The EC was therefore proposing a larger agency, possibly combining ENISA and telecoms regulation, to run from 2011. Until then, ENISA would likely continue to operate.

The plans for coming year were to focus on making networks more physically resilient, and a workshop was being held in early March. It would also continue to support CSIRT cooperation and development of best practices. To this end, a CSIRT Working Group was being established, and CSIRTs were asked to submit proposals as to what could be included on its work programme.

Karel Vietsch commented that the establishment of a European telecoms regulatory agency was highly contentious with national governments, so any future remit was uncertain. Andrew replied the two-year extension until 2011 would probably be approved though.

The question was also asked whether ENISA would stay in its current location. Andrew replied nothing had been decided, but the creation of a new agency might cause the location to be reviewed.

8. GN2 Security Activity Update

Claudio Allocchio provided an update on JRA2, the security activity within the GN2 project (see http://www.terena.org/activities/tf-csirt/meeting23/allocchio-jra2.pdf). It was currently working on three main activities: Flowmon, a NetFlow exporting device being developed by INVEA-TECH (a CESNET spin-off); Netreflex, a NetFlow anomaly detection system being developed by GUAVUS; and a Toolset Training Workshop.

The main questions related to what to do with the collected data. Could this be used for automatic alerting, opening of incidents, and notification? In addition, what countermeasures could be enacted if detrimental traffic was detected.

In addition, JRA2 was helping NRENs participating in the GN2 project to reach minimum security standards, and was developing relationships with other organisations such as DICE (DANTE/Internet2/CANARIE/ESnet) and APAN.

9. APCERT Update

Wim Biemolt reported that he would be attending the next APCERT meeting on 10-12 March 2008 in Hong Kong. He said that if anyone wished to raise any particular issue at the meeting, they should contact him directly.

Wim added that he would report back on the APCERT meeting at the next TF-CSIRT meeting in Oslo.

10. Date of next meeting

The next meeting will be held on 13-14 May 2008 in Oslo, Norway (hosted by the UiO and Uninett CERTs).

There had previously been a proposal from RU-CERT to host a meeting in either Moscow or St. Petersburg in September. All foreign citizens required visas to enter Russia though, and therefore RU-CERT had been asked whether they could help expedite this process. However, at the time of the meeting, no further information had been received so it might be necessary to consider alternative venues, especially as travelling to Russia posed problems for certain CSIRTs anyway.

Wilfried Wöber and Baiba Kaskina both offered to host the following meeting in Vienna or Riga should it prove problematic to hold it in Russia.

Gorazd Božič also asked for views on whether attendees found it useful to hold joint events with FIRST. The general consensus was positive, although the increasing size of these events put quite a lot of strain on local hosts. The issue of how to cover hosting expenses would need to be examined.

11. Future of TF-CSIRT

Gorazd Božič said the TF-CSIRT mandate expired at the end of May 2008, and so the group needed to be re-chartered. He proposed to schedule a discussion about this at the next meeting in Oslo, but in the meantime attendees should think about the type of activities the group should work on.

ACTION 23.1: All to think about the type of activities that TF-CSIRT should work on.

Open Actions

23.1 All to think about the type of activities that TF-CSIRT should work on.

22.2 Jacques Schuurman to check with AuCERT (and perhaps JPCERT) who was already involved in the out-of-band communications project and what would be required from potential volunteer European teams.

Participants

Name	Organisation	Country
Hillar Aareleid	CERT-EE	Estonia
Bente Christian Åsgård	UiO CERT	Norway
Shehzad Ahmad	DK-CERT	Denmark
Antti Alinen	Ericsson PSIRT	Finland
Claudio Allocchio	GARR	Italy
Oskar Bergquist	SITIC	Sweden
Wim Biemolt	SURFcert	The Netherlands
Vladimir Bobor	TS CERT CC	Sweden
Gorazd Božič (Chair)	SI-CERT (ARNES)	Slovenia
Matej Breznik	SI-CERT (ARNES)	Slovenia
Ian Bryant	ITsafe Warning Service	United Kingdom
Andreas Bunten	DFN-CERT	Germany
Ian Cook	Team Cymru	United Kingdom
Andrew Cormack	JANET(UK)	United Kingdom
Serge Droz	SWITCH-CERT	Switzerland
Till Dörges	PRESECURE Consulting	Germany
Oyvind Eilertsen	Uninett CERT	Norway
Haythem El Mir	CERT-TCC	Tunisia
Per Arne Enstad	Uninett CERT	Norway
Mehmet Eris	TR-CERT	Turkey
Lionel Ferette	Belnet CERT	Belgium
Carlos Fuentes	IRIS-CERT (RedIRIS)	Spain
Cyril Gayet	CERTA	France
Stefan Grinneby	SITIC	Sweden
Tomasz Grudziecki	CERT Polska (NASK)	Poland
Peter Haag	SWITCH-CERT	Switzerland
Anders Hardangen	NorCERT	Norway
Kauto Huopio	CERT-FI (FICORA)	Finland
Przemek Jaroszewski	CERT Polska (NASK)	Poland
Geoff Jones	GovCertUK	United Kingdom
Thorben Jändling	JANET CSIRT	United Kingdom
Andras Kabai	CERT-Hungary	Hungary
Urpo Kaila	FUNET CERT	Finland
Aaron Kaplan	NIC.AT	Austria
Baiba Kaskina	CERT NIC.LV	Latvia
Morten Knutsen	Uninett CERT	Norway
Jozsef Komli	CERT-Hungary	Hungary
Klaus-Peter Kossakowski	DFN-CERT Services	Germany
Vytautas Krakauskas	LITNET CERT	Lithuania
Andrea Kropáčová	CESNET	Czech Republic
Pavel Kácha	CESNET	Czech Republic
Otmar Lendl	NIC.AT	Austria
Antonio Liu	PRESECURE Consulting	Germany
Stelios Maistros	GRNET-CERT	Greece
Miroslaw Maj	CERT Polska (NASK)	Poland
Chelo Malagón	IRIS-CERT (RedIRIS)	Spain
Robert Malý	NESS	Czech Republic

Arturs Medenis	CERT NIC.LV	Latvia
Kristians Melins	CERT NIC.LV	Latvia
Jens Melle	CERT-VW	Germany
Kevin Meynell (Secretary)	TERENA	-
Michelle Danho	CERT-RENATER	France
Robert Morgan	JANET CSIRT	United Kingdom
Tom Mullen	BT	United Kingdom
Sigurd Mytting	UiO CERT	Norway
Kresimir Nesek	CARNet CERT	Croatia
Gustavo Neves	CERT.PT	Portugal
Katsuyuki Okazawa	CFC	Japan
Andre Oostwijk	GOVCERT.NL	The Netherlands
Carol Overes	GOVCERT.NL	The Netherlands
Luka Pauk	CARNet CERT	Croatia
Oliver Pietsch	CERT-VW	Germany
David Pybus	Diageo	United Kingdom
Margrete Raaum	UiO CERT	Norway
Helmi Rais	CERT-TCC	Tunisia
Tarmo Randel	CERT-EE	Estonia
Morten Schioenning	TeliaSonera DK subCERT	Denmark
Robert Schischka	NIC.AT	Austria
Udo Schweigert	Siemens CERT	Germany
Anthony Short	CPNI	United Kingdom
Derek Simpson	BT CERT CC	United Kingdom
Murat Soysal	Ulak-CSIRT	Turkey
Pascal Steichen	Ministry of the Economy	Luxembourg
Don Stikvoort	Trusted Introducer	-
Thomas Stridh	SUNet CERT	Sweden
Harri Sylvander	FUNET CERT	Finland
Alexander Talos	ACOnet CERT	Austria
Rafal Tarlowski	CERT Polska (NASK)	Poland
Varis Teivans	Sigmanet	Latvia
Marius Urkis	LITNET CERT	Lithuania
Simona Venuti	GARR-CERT	Italy
Karel Vietsch	TERENA	-
Dimitra Vitsa	FORTH	Greece
Torsten Voss	DFN-CERT	Germany
Torbjörn Wictorin	SUNet CERT	Sweden
Wilfried Wöber	ACOnet IRT	Austria

Apologies were received from:

Jimmy Arvidsson	TS-CERT CC	Sweden
Martin Camilleri	mtCERT	Malta
Ralf Dörrie	Telekom-CERT	Germany
Christoph Graf	SWITCH-CERT	Switzerland
David Parker	CPNI/CSIRTUK	United Kingdom
Jacques Schuurman	SURFcert	The Netherlands
Egils Sturmanis	DDIRV.LV	Latvia