25th TF-CSIRT meeting
26 September 2008
Austrian Academy of Sciences, Vienna, Austria

Please note that a seminar was held the previous day. The presentations can be found at http://www.terena.org/activities/tf-csirt/meeting25/

1. Approval of Minutes

The minutes of the last meeting held on 14 May 2008 were approved.

2. Actions from last meeting

24.1 Wilfried Wöber to draft new text for Work Item C in the TF-CSIRT Activity List.
Done.

24.2 Marco Thorbrügge to present new proposal for CHIHT at the 25th TF-CSIRT meeting.
Ongoing. Marco Thorbrügge had sent a proposal for discussion, but was not present at the meeting.

24.3 Robert Morgan to draft new text for Work Item H in the TF-CSIRT Activity List.
Done.

24.4 Kevin Meynell to contact Martijn van der Heide about the current status of E-CoAT.
Done. E-CoAT had become rather dormant for various reasons, but it was suggested the whitelisting activities might be taken over by TF-CSIRT.

24.5 Kevin Meynell to draft new Terms of Reference for TF-CSIRT.
Done. These had been approved by the TERENA Technical Committee.

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.

3. CERT.at Presentation

Robert Schischka gave a presentation about CERT.at. This is operated under the auspices of NIC.at (the Austrian domain registry) to provide a primary contact for IT security in Austria.

Lionel Ferette asked whether CERT.at was responsible for critical infrastructure as well. Robert replied this was still under discussion, but it was likely that Austria would follow the Swiss model of having a separate organisation for this.

4. DDIRV Presentation

Egils Sturmanis gave a presentation about DDIRV (see http://www.terena.org/activities/tf-csirt/meeting25/sturmanis-ddirv.pdf). This was a department of the Latvian State Information Network Agency which provided incident response services to Latvian governmental authorities, municipalities, and other customers under the AS8194 domain. It currently served a constituency of around 50,000 users.

Staffing consisted of team manager and IT security engineer, who undertook incident handling, published details of vulnerabilities and viruses, collated and published incident statistics, and provided security consultations and recommendations to government agencies. DDIRV was also designated as ENISA's National Liaison for Latvia, and within Latvia cooperated with the Ministry of Transport, State Police, the Secretariat for Electronic Governmental Affairs, and Latvian CERT Working Group. They were currently working towards accredited status within Trusted Introducer, and would be applying for FIRST membership shortly.

5. CCN-CERT Presentation

Carlos Abad gave a presentation about CCN-CERT. This is the incident response team within the Spanish Centre of Intelligence, which is an agency of the Spanish Ministry of Defence. It aims to provide centralised security incident management, coordination and technical support to central and provincial government, as well as local public administrations.

6. TF-CSIRT Delegation to Russia

Gorazd Božič and Mikhail Ganev provided an update on the TF-CSIRT delegation that would visit Moscow on 7 November 2008 (see http://www.terena.org/activities/tf-csirt/meeting25/bozic-russia.pdf). Those CSIRTs that had registered to attend, would meet with RU-CERT and several representatives of various Russian government agencies. A report would be provided at the next TF-CSIRT meeting.

Action 25.1 - Gorazd Božič to provide report on TF-CSIRT delegation to Russia at next TF-CSIRT meeting.

There was still time to register for the visit, but registration would close in the next couple of days. A simplified visa process had been arranged, and attendees would be notified how they could collect these.

Wim Biemolt asked whether it was possible to stay for additional days on these visas. Mikhail replied that he did not think this should be a problem.

Lionel Ferette also said there was still time to add items to the agenda, if people thought something in particular should be discussed.

7. GN2-JRA update

Claudio Allocchio provided an update on JRA2, the security activity within the GN2 project (see http://www.terena.org/activities/tf-csirt/meeting25/allocchio-jra2.pdf).

The 1 Gb/s version of the NetFlow exporting appliance had now been shipped to project participants by INVEA-TECH (a CESNET spin-off), and a report on the test results was due

in October. In addition, there had been several trials undertaken with the NetFlow-based anomaly detection system being developed by GUAVUS, and a report on these was expected in November.

The second toolset training workshop was planned for 2-4 February 2008 in Zürich, Switzerland. This would be a one-day event, with an optional second day for taking the 'training-the-trainer' module. This was initially only open to NREN staff, but any spare places would be offered to others.

JRA2 was also helping GN2 member NRENs to establish CERT functions, and had undertaken site visits to BREN (Bulgaria) in July, and RoEduNet (Romania) in August. This had led to active steps being taken to set-up CSIRTs, with a view to TI accreditation.

Looking ahead, the GN3 proposal had been submitted on 11 September, and stressed moving services and activities towards users who are both the victims and sources of security problems. There would likely be both service and research activities in the area of security, with a global security coordination service being envisaged.

The question was asked when the GN3 work programme was likely to be approved. Claudio replied the initial review was planned for November, so plans were likely to be finalised by February 2009 with a view to commencing work the following month.

Lionel Ferette asked whether the GN3 Description of Work was available. Claudio replied this was currently under non-disclosure, although it had been approved by all the participating NRENs.

8. TRANSITS update

Wilfried Wöber provided an update on the two TRANSITS training courses that had recently been organised in Austria (see http://www.terena.org/activities/tf-csirt/meeting25/woeber-transits.pdf). These were targeted at the Austrian federal government; national railway, broadcasting and energy distribution companies; healthcare providers; the emergency services, the financial sector; and other public agencies.

The first workshop had been attended by 17 participants, and the second by 26 participants. There had also been a preliminary refresher course attended by 15 participants. In general, these workshops had been successful, although in such big groups, people obviously had different levels of knowledge. It was noted that the module on law probably needed some more work, as it needed more detail with respect to specific national laws.

Karel Vietsch also mentioned the forthcoming TRANSITS workshop that was being organised on 22-24 October 2008 in Roztoky u Prahy, Czech Republic (hosted by CESNET and sponsored by ENISA). This had been oversubscribed, and it had attracted participants from both Japan and South Africa.

TERENA also had an agreement with FIRST for them to use the TRANSITS training material, and a workshop had recently been organised by them in Seoul, South Korea. In addition, agreement had been reached with NTT to translate the material into Japanese.

TERENA was still looking for a host for the next workshop in Spring 2009, so any organisation interested in doing this should contact the TERENA Secretariat.

9. AIRT update

Wim Biemolt provided an overview of the AIRT (Application for Incident Response Teams) software that was used for incident handling by SURFcert and in major Dutch universities (see http://www.terena.org/activities/tf-csirt/meeting25/biemolt-airt.pdf). This was free software issued under a GPL licence that provided a framework for adding features using plug-ins, as well as both human and machine interfaces.

At the present time, development and maintenance of this software was funded by SURFnet, which amounted to around EUR 40K per annum. Around half of this was attributable to improving functionality, whilst the remainder was for adding new features. However, the problem was that SURFnet now had a new policy whereby it would no longer support software for which they were the only funder.

SURFnet were therefore trying to find out who was actually using AIRT, and whether anyone else was interested in helping to participate in its ongoing development – either through funding or effort. If three or four other CSIRTs could be found, a meeting could be organised to discuss further progress, and to formalise a consortium.

10. Cyberattacks on Georgia

Toomas Lepik gave a short presentation on the recent cyberattacks on Georgia, during the recent conflict in South Ossetia.

11. Format of future TF-CSIRT meeting & progressing work items

Lionel Ferette opened the discussion about the future format of TF-CSIRT meetings, and expressed concern about the progress some of the work items (see http://www.terena.org/activities/tf-csirt/meeting25/ferette-meetings.pdf).

It was generally agreed that the half-day seminar was useful and informative, but the business meetings were felt to have too many repetitive updates. From the organisational point-of-view, it had also become increasingly difficult to fill the agenda in a timely fashion, with many requests for timeslots coming at very short notice which made scheduling difficult. Whilst it was recognised that time should always be made available for late-breaking developments, neither could the Secretary rely on filling the whole agenda at the last minute. People needed, and indeed requested, advance notice of the programme in order to justify their travel. The Secretary therefore asked that if people had subjects of potential interest to the TF-CSIRT audience, to please contact the Chair or himself as early as possible.

Another issue was the lack of discussion that was devoted to work items. Whilst TF-CSIRT fulfilled the role of information exchange, as a TERENA task force, it was also expected to undertake practical and useful activities. A number of work items were effectively dormant, and even though the list had recently been reviewed with the re-chartering of the task force, those that had made little progress should perhaps be dropped.

Related to this were actions that were often not undertaken. Whilst it was recognised that actions had previously been recorded in a sometimes ambiguous fashion, people were in future asked to ensure they were able to undertake actions in a timely fashion if they agreed to take them.

Finally, it was felt that many of the useful discussions actually took place outside of the meetings during the lunch and coffee breaks. Whilst it wasn't really justifiable to extend

these any further, more time could perhaps be allocated during the meetings to having more freeform discussion. Another suggestion was to allocate time slots for very short talks on topics of current interest. This was certainly a willingness from the Chair and Secretary to be flexible with the format and agenda of the meetings, but they also needed to hear from the participants as to what they would like to see.

There was a comment that TF-CSIRT was really the only forum for CSIRT cooperation in Europe, and fulfilled a useful role in this respect. However, there was very little interaction between the four-monthly meetings, which might be improved if there was a greater focus on operational cooperation.

12. Date of next meeting

The next meeting will be held on 19-20 January 2009 in Riga, Latvia (hosted by CERT NIC.LV). This would be in conjunction with the FIRST Technical Colloquium.

Open Actions

25.1 Gorazd Božič to provide report on TF-CSIRT delegation to Russia at next TF-CSIRT meeting.

24.2 Marco Thorbrügge to present new proposal for CHIHT at the 25th TF-CSIRT meeting.

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*
Bente Christine Åsgard	UiO-CERT	Norway
Carlos Abad	CCN-CERT	Spain
Claudio Allocchio	GARR	Italy
Mateo Araque	CCN-CERT	Spain
Jimmy Arvidsson	TeliaSonera CERT	Sweden
Gerhard Bauer	Austrian Academy of Sciences	Austria
Javier Berciano	INTECO-CERT	Spain
Wim Biemolt	SURFcert	The Netherlands
Vladimir Bodor	TS-CERT (TeliaSonera)	Sweden
Gorazd Božič	SI-CERT (ARNES)	Slovenia
Ian Bryant	ITsafe Warning Service	United Kingdom
Andreas Bunten	DFN-CERT	Germany
Sergey Bunyakov	RU-CERT	Russia
Jorge Chinea López	INTECO-CERT	Spain
Christian Compton	CPNI	United Kingdom
Andrew Cormack	JANET(UK)	United Kingdom
Goran Culjak	CERT ZSIS	Croatia
Michelle Danho	CERT-RENATER	France
Serge Droz	SWITCH-CERT	Switzerland
Lionel Ferette (Chair)	BELNET CERT	Belgium
Martin Fischer	ACOnet CERT	Austria
Mikhail Ganev	RU-CERT	Russia

Cyril Gayet	CERTA	France
Espen Grøndahl	UiO CERT	Norway
Peter Haag	SWITCH-CERT	Switzerland
Günter Hof	Austrian Academy of Sciences	Austria
Kauto Huopio	CERT-FI (FICORA)	Finland
Przemek Jaroszewski	CERT Polska (NASK)	Poland
L. Aaron Kaplan	CERT.at (NIC.at)	Austria
Igor Karpenko	RU-CERT	Russia
Baiba Kaskina	SigmaNet	Latvia
Ulrich Kiermayr	U. Vienna Computer Centre	Austria
Melitta Kimbacher	Austrian Academy of Sciences	Austria
Susanne Kriszta	ACOnet CERT	Austria
Andrea Kropáčová	CESNET	Czech Republic
Otmar Lendl	CERT.at	Austria
Toomas Lepik	CERT Estonia	Estonia
Chelo Malagón	IRIS-CERT (RedIRIS)	Spain
Thomas Mandl	Secure Business Austria	Austria
Branko Mažar	CARNet	Croatia
Ģirts Mažonis	DDIRV	Latvia
Kevin Meynell (Secretary)	TERENA	-
Maurizio Molina	DANTE	-
Robert Morgan	JANET-CSIRT	United Kingdom
Kresimir Nesek	CARNet	Croatia
Thomas Nguyen Van	Jumper CSIRT	Ireland
Carol Overes	GOVCERT.NL	The Netherlands
Goran Pestana	SITIC	Sweden
Christian Platzer	Vienna University of Technology	Austria
Leila Pohjolainen	FUNET CERT	Finland
Christian Proschinger	Raiffeisen Informatik GmbH	Austria
Tarmo Randel	CERT-EE	Estonia
Allan Lynge Rasmussen	DK-CERT (UNI-C)	Denmark
Wayne Routly	DANTE	United Kingdom
Jürgen Sander	PRESECURE	Germany
Linos Santos	CERT.PT (FCCN)	Portugal
Robert Schischka	NIC.AT	Austria
Jacques Schuurman	SURFcert (SURFnet)	The Netherlands
Derek Simpson	BT CERT	United Kingdom
Pascal Steichen	CIRCL	Luxembourg
Marc Stiefer	RESTENA-CSIRT	Luxembourg
Don Stikvoort	Trusted Introducer	-
Erika Stockinger	SITIC	Sweden
Mathias Stoffel	S-CERT	Germany
Egils Sturmanis	DDRIV	Latvia
Matthias Subik	funkfeuer.at	Austria
Marius Urkis	LITNET CERT	Lithuania
Bob van der Kamp	GOVCERT.NL	The Netherlands
Christian Van Heurck	BELNET CERT	Belgium
Han van Thoor	Jumper CSIRT	Ireland
Simona Venuti	GARR-CERT	Italy
Karel Vietsch	TERENA	-
Torsten Voss	DFN-CERT	Germany
Edgar Weippl	Secure Business Austria	Austria
Wilfried Wöber	ACOnet IRT	Austria
Martin Zeilinger	TU Wien	Austria

Apologies were received from:

Veronika Berglund	SUNet CERT	Sweden
Ralf Dörrie	Telekom-CERT	Germany
Christoph Graf	SWITCH	Switzerland
Mirosław Maj	CERT Polska (NASK)	Poland
Janos Mohacsi	NIIF/Hungarnet	Hungary
Margrete Raaum	UiO-CERT	Norway
David Tabatadze	CERT Georgia	Georgia
Marco Thorbrügge	ENISA	-