26th TF-CSIRT meeting
19 January 2009
Institute of Mathematics and Computer Science, Riga, Latvia

Please note that a joint FIRST/TF-CSIRT seminar was held the following day. The presentations can be found at http://www.terena.org/activities/tf-csirt/meeting26/

1. Approval of Minutes

The minutes of the last meeting held on 26 September 2008 were approved.

2. Actions from last meeting

25.1 Gorazd Božič to provide report on TF-CSIRT delegation to Russia at next TF-CSIRT meeting.
Done, a report was given during the meeting.

24.2 Marco Thorbrügge to present new proposal for CHIHT at the 25th TF-CSIRT meeting.
Ongoing, although a proposal was sent to the Chair before the 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.
Dropped.

3. Jumper CSIRT Presentation

Han van Thoor gave a presentation about Jumper CSIRT (see http://www.terena.org/activities/tf-csirt/meeting26/vanthoor-jumper-csirt.pdf). This is a commercial CSIRT based in Dublin and Rome. It currently offers both reactive and proactive services, as well as training, risk analysis, and disaster recovery consultancy. One of its main customers was the Italian government.

Kauto Haupio asked how an Irish-based company handled incidents in Italy. Han replied that Italian law was applicable, which meant no data could be transferred to Ireland. As a result they had a local team in Italy to handle these cases.

Lionel Ferette asked whether Jumper CSIRT was part of a larger organisation. Han replied that Jumper Consulting was a company of 15 staff that was involved with network monitoring, PCI-DSS payment data security, and reselling of security-related software. However, the CSIRT was separate.

4. CERT-LT Presentation

Rytis Rainys gave a presentation about CERT-LT (see http://www.terena.org/activities/tf-csirt/meeting26/rainys-cert-lt.pdf). This was originally known as CERT-RRT, and had

operated as the Lithuania Government CSIRT under the auspices of the Communications Regulatory Agency (NRA) since 2006. However, after many websites were defaced in June 2008 which generated a lot of media attention, it was decided that CERT-RRT should become responsible for national incident coordination as well. As a result, it was renamed CERT-LT.

The constituency is telecoms operators, ISPs, and Internet hosting companies in Lithuania. Its duties are to coordinate other CSIRTs in the country, collect and investigate incidents on public networks, disseminate information about threats and potential threats, and monitor the state of security in key infrastructures.

The team currently comprises three staff; a manager and two specialists, and had investigated a total of 661 incidents (343 in 2008) since it became operational. It also cooperates closely with the military (KAM-VRIST), academic (LITNET CERT) and government (Infostrucktura-CERT) teams, as well as those in neighbouring countries.

Kauto Haupio noted there were more than a hundred ISPs in Lithuania, and asked about the level of security knowledge in the country. Rytis replied it varied from ISP-to-ISP, and it was difficult to generalise.

5. Establishment of a Croatian National CERT

Darko Perhoč gave a presentation about a new CSIRT that had been established in Croatia (see http://www.terena.org/activities/tf-csirt/meeting26/perhoc-croatian-cert.pdf). The Croatian government had recently decided that a national CSIRT should be setup and run by CARNet, the Croatian research and education network. This was an independent unit within CARNet, although it would closely cooperate with the existing CARNet CERT.

The national CSIRT was expected to coordinate the operations of other CERT teams in the country, liaise with the National Security Council (NSA) and Information Systems Security Bureau (NCSA), and promote the need for computer security in the wider community. Operations were expected to start later in 2009.

Lionel Ferette asked how many staff the team had. Darko replied it was just himself at the moment, although they were currently recruiting for 2 or 3 specialists. At the present time, incidents were being handled by the CARNet CERT.

6. Grid Security

Romain Wartel gave a presentation about security considerations in the Grid community.

7. TF-CSIRT Delegation to Russia

Gorazd Božič gave a report on the TF-CSIRT delegation that visited Moscow on 7 November 2008 (see http://www.terena.org/activities/tf-csirt/meeting26/bozic-russian-delegation.pdf). This involved 13 teams from TF-CSIRT who met with RU-CERT, RU-CENTER, the FSB, and GOVCERT Bulgaria.

The programme covered incident response in Russia, e-commerce issues, ccTLD regulation, and RU-CERT plans for the future. The TF-CSIRT delegation provided overviews of specific topics based on their own experiences, and encouraged future collaboration between Russia and the wider CSIRT community.

8. GN2-JRA update

Serge Droz provided an update on JRA2, the security activity within the GN2 project (see http://www.terena.org/activities/tf-csirt/meeting26/droz-gn2-jra2.pdf).

The test results of the FlowMon and Advanced Anomaly Detection tools were expected in February. In addition, the second Toolset Training Workshop will be held on 2-4 February in Zürich, Switzerland. Registration is open to non-NREN participants.

There had been two site visits to BREN (Bulgaria) and RoEduNet (Romania) in July and August 2008, to promote the establishment of CSIRTs there. RoCSIRT was able to be established quickly, and became TI listed in October 2008.

The negotiations for the GN3 project were still ongoing, but security would play an important role. Claudio Allocchio was likely to be the GN3 Security Coordinator.

9. Report on Norwegian TRANSITS Courses

Øyvind Eilertsen reported on the training courses that had been organised in Norway using the TRANSITS material (see http://www.terena.org/activities/tf-csirt/meeting26/eilertsen-transits.pdf). Two courses per year had been organised since 2006, funded by the GigaCampus programme for the Norwegian higher education community.

The course had been slightly reduced in length to 1.5 days, and introduced a legal module specific to Norwegian law. In addition, the technical module had been supplemented by material from other presentations.

In general, feedback was very positive, although the comprehensive nature of the programme meant that not every module was suitable for every trainee. In particular, the technical module was various described as 'too difficult' or 'too simplistic'.

As GigaCampus was due to end in 2009, the last TRANSITS course was scheduled for the Spring. However, GigaCampus II was currently under discussion, and security would be an integral part of that. Future TRANSITS courses may therefore be held annually if there was sufficient demand for them.

Andrew Cormack pointed out that in relation to this, ENISA had produced advice on obtaining management support and funding for organising things like security training. More information was available at http://www.enisa.europa.eu/doc/pdf/deliverables/obtaining_support_and_funding_from_senior_management.pdf.

10. TRANSITS update

Don Stikvoort provided an update on the last TRANSITS training course that had been organised in the Czech Republic, and on future plans (see http://www.terena.org/activities/tf-csirt/meeting26/stikvoort-transits.pdf).

The next TRANSITS course would be held on 12-13 March 2009 in Dublin, Republic of Ireland (hosted by Jumper CSIRT). They were currently looking for tutors for this event, and hosts/sponsors for the following events in Autumn 2009 and Spring 2010.

There were also plans to organise a one-day get-together for the tutors to discuss

content, presentation and communication issues. This would probably be held in conjunction with the May or September TF-CSIRT meeting.

Finally, there was an idea to hold TRANSITS courses targeted at more experienced team members. These would cover issues such as forensics, improving communications, NetFlow, and incident scenarios, and would possibly be held over three instead of two days. Input to this was welcome.

Shehzad Ahmed said that DK-CERT might be willing to host a future TRANSITS course in Copenhagen. TERENA should contact him to discuss things further.

11. Update on ISO 27053

Pascal Steichen gave an update on the status of the ISO standards relevant to CSIRTs (see http://www.terena.org/activities/tf-csirt/meeting26/steichen-iso27053.pdf). There were several existing or developmental standards such as ISO/IEC 18043 that applied to deployment and operation of intrusion detection system, ISO/IEC 27035 that applied to security incident management, and ISO/IEC 29147 that dealt with responsible vulnerability disclosure.

These standards were being developed by the SC27 Committee which largely dealt with national ISO groups, but it was important for industry and expert groups to get involved in order to create good and workable standards. It was suggested that TF-CSIRT might appoint an official liaison to SC27 in order to facilitate this work.

Andrea Maida asked about cooperation between ISO, the ITU, and CSIRTs. Pascal replied that ISO and the ITU closely cooperated, but whilst there were some liaisons with CSIRTs, he was not aware of anything official.

There followed some discussion about whether TF-CSIRT should liaise with SC27. It was generally agreed that whilst the immediate relevance of the work was unclear, it was important to provide input and feedback in order to ensure that resulting standards were useful. Lionel Ferette therefore said he would investigate how to establish a liaison.

Action 26.1 – Lionel Ferette to investigate how to establish liaison with ISO 27035 drafting process.

12. Progressing TF-CSIRT work items

Lionel Ferette reviewed the current status of the TF-CSIRT work items that were listed in the current Terms of Reference (see http://www.terena.org/activities/tf-csirt/meeting26/ferette-workitems.pdf).

Work Item A (Meetings and Seminars) was clearly being fulfilled with three meetings and seminars organised each year. However, suggestions for improvements were always welcome.

Work Item B (Trusted Introducer) was also regularly reported on, although improvements to the accreditation model perhaps needed to be implemented.

Work Item C (Security Contact Information) had been somewhat undertaken, with the IRT objects now being shown by default by RIPE. Nevertheless, although accredited teams could maintain their IRT objects through the Trusted Introducer Service, what other efforts could be undertaken to encourage more widespread uptake.

Gilles Massen said that some guidance on how to use the IRT objects would be useful, and asked whether some sort of tutorial could be organised. Lionel replied that he would speak to Wilfried Wöber to see if something could be organised at a future TF-CSIRT meeting.

Action 26.2 – Lionel Ferette to speak to Wilfried Wöber about organising tutorial on IRT objects at a future TF-CSIRT meeting.

Work Item D (Clearing House for Incident Handling Tools) had not made much progress in the past year, as ENISA had been awaiting the hiring of a webmaster. However, they were now starting to migrate the CHIHT structure, and it was hoped this could be completed before the next TF-CSIRT meeting in May.

Work Item E (Training of CSIRT Staff) was being undertaken in the context of the TRANSITS courses. These had proved to be very successful, and there were plans to update the existing material as well as run courses for more experienced users. Nevertheless, ongoing funding was an issue that needed to be resolved.

Work Item F (Assistance to the Establishment of New CSIRTs) had largely been taken up by the GN2-JRA2 activity. This had undertaken consultancy work to establish new CSIRTs in at least four countries over the past year. There had not been much take up of the mentoring scheme to date though.

With respect to Work Item G (Collaboration with FIRST and organisations in other regions), TF-CSIRT had established a regular liaison with APCERT, and had attended an OIC-CERT meeting during 2008. Collaboration with FIRST might be improved, although the Joint FIRST/TF-CSIRT Symposiums was a step in this direction.

There had been no specific activity in Work Item H (RTIR) since the last updates to the software. However, there would be a discussion about future developments during the FIRST/TF-CSIRT seminar the following day.

There had been regular reports on Work Item J (GN2-JRA) during TF-CSIRT meetings, and there had been active progress in relation to Work Item F. The GN2 project was due to finish in March 2009, and it was not yet clear what security activities would be undertaken by the successor GN3 project.

There had been limited contact in past years with respect to Work Item K (Liaison with the European Commission), although this was largely because EC priorities had changed following the establishment with ENISA. Nevertheless, there was an active liaison with ENISA, and the EC was also providing an update on security policy initiatives at the meeting.

Work Item L (Liaison with e-CoAT) was somewhat dormant due to the uncertainty over the current status of e-CoAT. However, there had recently been a revival of interest in anti-spam initiatives amongst certain NRENs, so there may be scope to undertake this in the context of this work item.

Work Item M (Incident Handling and Security Guidelines for Grid) had made limited progress to date, but there had been a presentation and discussion about Grid security at the meeting. TF-CSIRT participants clearly considered it important to improve coordination with the Grid community, so these contacts should be followed up.

Work Item N (Drill Exercises) had been added when TF-CSIRT was re-chartered in May 2008, but there had yet to be any progress. It was suggested that Lionel start discussion

about this on the mailing list.

Action 26.3 – Lionel Ferette to start discussion on the mailing list about potential drill exercises.

The plan for Work Item O (Evaluation of New Tools) was to provide an update on a specific incident handling tool at each meeting. This needed to be progressed, although a tutorial on IRT objects might be considered a start in this direction. It was again suggested that Lionel start a discussion about this on the mailing list.

Action 26.4 – Lionel Ferette to start discussion on the mailing list about which incident handling tools to evaluate.

13. Date of next meeting

The next meeting will be held on 18-19 May 2009 in León, Spain (hosted by INTECO).

The provisional dates for the following meeting are 24-25 September 2009, to be held in Tallinn, Estonia (hosted by CERT-EE).

Open Actions

26.1 Lionel Ferette to investigate how to establish liaison with ISO 27035 drafting process.

26.2 Lionel Ferette to speak to Wilfried Wöber about organising tutorial on IRT objects at a future TF-CSIRT meeting.

26.3 Lionel Ferette to start discussion on the mailing list about potential drill exercises.

26.4 Lionel Ferette to start discussion on the mailing list about which incident handling tools to evaluate.

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

Participants

Name	*Organisation*	*Country*
Jordi Aguila	e-la Caixa CERT	Spain
Shehzad Ahmed	DK-CERT	Denmark
Peter Allor	FIRST	-
Jimmy Arvidsson	TeliaSonera CERT	Sweden
Elliot Atkins	GovCertUK	United Kingdom
Javier Berciano	INTECO-CERT	Spain
Wim Biemolt	SURFcert	The Netherlands
Vladimir Bodor	TS-CERT (TeliaSonera)	Sweden
Gorazd Božič	SI-CERT (ARNES)	Slovenia
Matek Breznik	SI-CERT (ARNES)	Slovenia
Andreas Bunten	DFN-CERT	Germany
Jorge Chinea López	INTECO-CERT	Spain
Christian Compton	CPNI	United Kingdom
Andrew Cormack	JANET(UK)	United Kingdom
Mick Creane	BT	United Kingdom
Goran Culjak	CERT ZSIS	Croatia
Michelle Danho	CERT-RENATER	France
Till Dörges	PRESECURE	Germany
Serge Droz	SWITCH-CERT	Switzerland
Øyvind Eilertsen	Uninett CERT	Norway
Per Arne Enstad	Uninett CERT	Norway
Lionel Ferette (Chair)	BELNET CERT	Belgium
Carlos Fuentes	RedIRIS	Spain
Mikhail Ganev	RU-CERT	Russia
Cyril Gayet	CERTA	France
Natasha Glavor	CARNet	Croatia
Thomas Grenman	CERT-FI	Finland
Tomasz Grudziecki	CERT Polska (NASK)	Poland
Peter Haag	SWITCH-CERT	Switzerland
Vincent Hinderer	CERT-LEXSI	France
Kauto Huopio	CERT-FI (FICORA)	Finland
Przemek Jaroszewski	CERT Polska (NASK)	Poland
Maris Kalejs	CERT NIC.LV	Latvia
L. Aaron Kaplan	CERT.at (NIC.at)	Austria
Baiba Kaskina	CERT NIC.LV	Latvia
Daniel Kouril	CESNET	Czech Republic
Susanne Kriszta	IT Security & ACOnet	Austria
Toomas Lepik	CERT Estonia	Estonia
Antonio Liu	PRESECURE	Germany
Mingchao Ma	STFC	United Kingdom
Girts Mažonis	DDIRV	Lithuania
Stelios Maistros	GRNET	Greece
Chelo Malagón	IRIS-CERT (RedIRIS)	Spain
Gints Malkalnietis	CERT NIC.LV	Latvia
Gilles Massen	RESTENA	Luxembourg
Scott McIntyre	KPN-CERT	The Netherlands
Arturs Medenis	CERT NIC.LV	Latvia
Kevin Meynell (Secretary)	TERENA	-
Maciej Milostan	PIONIER CERT	Poland
Maurizio Molina	DANTE	-
Robert Morgan	JANET-CSIRT	United Kingdom
Tom Mullen	BT	United Kingdom
Andre Oosterwijk	GOVCERT.NL	The Netherlands

Carol Overes	GOVCERT.NL	The Netherlands
Darko Perhoc	CARNet	Croatia
Martin Peterka	CZ.NIC	Czech Republic
Toby Powell	GovCertUK	United Kingdom
Anu Puhakainen	Ericsson	Sweden
David Pybus	DCSIRT	United Kingdom
Margrete Raaum	UiO-CERT	Norway
Rytis Rainys	CERT-LT	Lithuania
Tarmo Randel	CERT-EE	Estonia
Wayne Routly	DANTE	United Kingdom
Katrina Sataki	Sigmanet	Latvia
Robert Schischka	NIC.AT	Austria
Udo Schweigert	Siemens CERT	Germany
Andrea Servida	European Commission	-
Derek Simpson	BT CERT	United Kingdom
Pascal Steichen	CIRCL	Luxembourg
Don Stikvoort	S-CURE	The Netherlands
Egils Sturmanis	DDIRV	Latvia
Yoshiki Sugiura	NTT	Japan
Harri Sylvander	CSC	Finland
David Tabatadze	CERT-GE (GRENA)	Georgia
Alexander Talos-Zens	ACOnet CERT	Austria
Rafal Tarlowski	CERT Polska (NASK)	Poland
Varis Teivans	CERT NIC.LV	Latvia
James Thorton	DCSIRT	United Kingdom
David Tresgots	Cert-IST	France
Marius Urkis	LITNET CERT	Lithuania
Koen Van Impe	BELNET CERT	Belgium
Marc Vilanova	e-la Caixa CSIRT	Spain
Torsten Voss	DFN-CERT	Germany
Romain Wartel	CERN	-
Arnold Yoon	FIRST	-
Takahiko Yoshida	NTT	Japan
Kimberley Zenz	VeriSign iDefense	United States
Edgar Weippl	Secure Business Austria	Austria
Wilfried Wöber	ACOnet IRT	Austria
Martin Zeilinger	TU Wien	Austria

Apologies were received from:

Claudio Allocchio	GARR	Italy
Christoph Graf	SWITCH	Switzerland
Marco Thorbrügge	ENISA	-