30th TF-CSIRT meeting
20 May 2010
FORTH, Heraklion, Greece

Please note that a seminar was held the following day.

1. Approval of Minutes

The minutes of the last meeting held on 25 January 2010 were approved.

2. Actions from last meeting

There were no outstanding actions from the previous meeting.

3. CESNET-CERTS presentation

Andrea Kropáčová gave a presentation about CESNET-CERTS (see https://www.terena.org/tf-csirt/meeting30/kropacova-cesnet-certs.pdf). This had been established in 2003 and provided incident handling for the CESNET community. It also provided services on behalf of CSIRT.CZ, a national incident handling coordination effort.

The team was currently comprised of 7 part-time staff. As well as conducting incident handling, it also provided intrusion detection, auditing, and training services.

4. Danish GovCERT presentation

Thomas Kristmar gave a presentation about the Danish GovCERT (see http://www.terena.org/tf-csirt/meeting30/kristmar-danish-govcert.pdf). This was a new CSIRT created in May 2009 by the Danish National IT and Telecom Agency, with the aim of protecting critical infrastructures in national, regional and local governmental institutions, as well as certain critical sectors such as finance, energy and ICT. It has also had a close working relationship with the Danish intelligence services, DK-CERT (research and education) and MILCERT (military).

The team was comprised of 12 staff, and was expected to become fully operational by the end of 2010. It was currently entering a pilot phase, and would provide several reactive and proactive services to ensure the Danish state could provide a coordinated response to cyberattacks and other threats to information security.

They would be applying for FIRST membership and TI listing later in the year, and aimed to become TI accredited by 2011.

Lionel Ferette asked where incident reports could be sent. Thomas replied that the contact e-mail address was 'info@govcert.itst.dk'.

Leon Kaplan asked whether there was a legal oversight body to ensure collection of network data was in accordance with the law. Thomas replied that financial auditors had been asked to make unannounced inspections and report on their findings to the Danish

Parliament.

Giannis Askoxylakis asked who operated and funded the network monitoring probes. Thomas replied this came from their own budget.

5. SITIC presentation

Oskar Bergquist gave a presentation on the Swedish IT Incident Centre http://www.terena.org/tf-csirt/meeting30/bergquist-sitic.pdf). This was currently a department of the Swedish Post and Telecom Agency, but would be transferred to the Swedish Civil Contingencies Agency in 2011.

SITIC provided a 24 x 7 incident response service for government institutions, as well as having a coordination function for other Swedish CSIRTs. It was also involved in identifying and raising awareness of threats, as well as developing intrusion detection and information collection tools. These tools included Megatron which collects and processes information about bad hosts on the Internet, and MolluskNG which collates and examines security related information found on websites.

Kauto Huopio asked whether they were willing to share the information collected by Megatron with other CSIRTs. Oskar replied this might be possible, although they would need to consider this further.

6. EGEE → EGI

Serge Droz gave a presentation on the transition from EGEE to EGI, and the establishment of EGI-CSIRT (see http://www.terena.org/tf-csirt/meeting30/droz-egi.pdf). The European Grid Initiative (EGI) had been established in order to coordinate the various National Grid Initiatives, and to give some permanence to the international infrastructure created by the EGEE project. It was based in Amsterdam, and would be funded by the EU for four years.

EGEE OSCT was a virtual CSIRT that had been established by various NGIs within the EGEE project, in order to handle incidents affecting grid infrastructure. This was already TI listed, but with the establishment of EGI, its activities would be put on a more permanent footing as EGI CSIRT. This became operational on 1 May, although it would still primarily focus on coordinating NGI CSIRTs; escalating issues up to GRID-SEC where necessary.

Lionel Ferette asked whether the EGI CSIRT functions were still rotated between NGI teams. Serge replied this was the case for most, but not all, countries that each did this for one week at a time.

Kauto Huopio asked whether the NGI CSIRTs ever coordinated with national CSIRTs. Serge felt the most appropriate contact was with NREN CSIRTs, as grid infrastructure by definition fell within the research and education community. National CSIRTs were generally not familiar with the grid community, and their involvement would probably not add much.

7. GN3 Security activities

Wayne Routly gave an update on the security activities within the GN3 project (see http://www.terena.org/tf-csirt/meeting30/routly-gn3-sec.pdf). These fell within Service

Activity 2 (SA2) which was concerned with multi-domain services, and Task 4 was charged with supporting the secure deployment of these.

SA2/T4 aimed to pre-empt problems by educating developers, administrators and users about good security practices, whilst ensuring security was a consideration at every stage in the design and implementation of GN3 services. This would be undertaken through the development of a best practices cookbook, and security training for those developing GN3 components.

The activity also aimed to help NREN CSIRTs deploy a consistent set of security tools and working practices that could quickly allow problems to be identified when they did occur. The first stage had been a survey of current tools and practices, which had resulted in about 40 responses. This was now being used to identify missing elements, and develop work flows in line with what was needed.

8. TRANSITS/TRANSITS2 update

Lionel Ferette reported on the previous TRANSITS course in Uppsala, and the forthcoming event in Germany in the autumn (see http://www.terena.org/tf-csirt/meeting30/stikvoort-transits.pdf).

In addition, an advanced TRANSITS course (TRANSITS2) was provisionally planned for 5-7 October 2010 in Amsterdam. This was aimed at more experienced team members, and would include modules on forensics, NetFlow analysis, communications skills, as well as practical exercises. More information on this would be circulated in due course.

9. Proposed RTIR Workshop

Lionel Ferette said there was a proposal to organise a workshop on the RTIR at the next meeting, and asked who would be interested. This would provide training on how to use the software, and an opportunity to identify what (if any) features were still missing.

A total of sixteen people expressed interest in this, which was sufficient to organise a workshop. Kevin Meynell would therefore liaise with Carlos Fuentes and Ulak-CSIRT to set this up.

Action 30.1 – Kevin Meynell to liaise with Carlos Fuentes and Ulak-CSIRT to organise RTIR Workshop in Istanbul.

10. ISO Liaison

Lionel Ferette reported that at previous meetings, there had been some discussion as to whether TF-CSIRT (through TERENA) should be involved in the drafting process for the ISO/IEC 27035 "Security Incident Handling" standard. However, after further investigations, it was concluded there was little that could be contributed as this was already close to completion and would not be revised for several more years.

It was nevertheless still important to follow the development of such standards as it may be necessary to implement these at some stage in the future. The question was therefore whether TF-CSIRT should follow other standards (e.g. forensics), bearing in mind the workload was quite high, and that representatives needed to actually attend the meetings if they wanted their changes to be accepted.

Baiba Kaskina suggested that someone should be invited to speak about the relevant ISO standards every year or so. An initial point of contact could be the national ISO representatives.

11. Rechartering of the Task Force

Lionel Ferette said the TF-CSIRT mandate expired on 15 May 2010, and so the group needed to be re-chartered. This was the regular practice with TERENA Task Forces to ensure the work they were doing remained relevant, but it also provided an opportunity to review the objectives and tasks. He therefore proposed to go through the existing Terms of Reference to determine whether any activities should be added, modified or dropped, with a view to drafting revised Terms of Reference for approval by TERENA.

It was agreed that TF-CSIRT was still relevant and useful, and so a request to re-charter the group should be made to TERENA.

It was also agreed that the objectives of the group as outlined in Article 2 of the existing Terms of Reference remained valid, although 2.6 should be amended to read "to provide a vehicle for CSIRTs to liaise with policy making bodies, law enforcement agencies, and other relevant organisations". In addition, the categorisation of CSIRTs in Article 4 should be removed, and simply replaced with 'recognised CSIRTs'.

Lionel said he was happy to continue as Chair of TF-CSIRT for a further term, and there were no objections. Kauto said he was willing to stand down as Deputy Chair, if anyone was willing to volunteer for this.

Lionel proposed that in order to better progress the work items, individuals should be assigned to lead and coordinate them. This was in line with activities in other TERENA Task Forces.

The following was agreed with respect to existing activities:

Meetings and Seminars
The existing format of the meetings and seminars should continue unchanged, although there was some support for moving the business meeting to the afternoon of the first day, and the seminar to the morning of the second day. Lionel Ferette would take responsibility for this.

Trusted Introducer Service
This was a well-established and useful service which should continue to organise regular meetings of accredited CSIRTs adjacent to TF-CSIRT meeting. S-CURE were already contracted to take responsibility for this.

Security Contact Information for Internet Resources
This activity was still felt to be relevant, and Wilfried Wöber should be asked whether he could take responsibility for this.

Action 30.2 – Kevin Meynell to ask Wilfried Wöber whether he is willing to be the responsible person for Work Item C in the Terms of Reference.

Clearing House for Incident Handling Tools
This was maintained by ENISA, and Marco Thorbrügge was already responsible for this.

Training of new (staff of) CSIRTs
There was still a demand for the TRANSITS training courses, and the material was also

being used by other organisations around the world. TERENA was already responsible for organising these.

Assistance to the establishment of new CSIRTs
This had been undertaken by the GN2 project, but was not really the focus of GN3. Whilst this could still be done on an individual request basis, it was decided this activity should be dropped.

Collaboration with FIRST and organisations in other world regions
TF-CSIRT organised a joint event with FIRST each year, and had an ongoing liaison with APCERT. Although a number of individuals were involved in these activities, it was felt Lionel Ferette should have primary responsibility for this.

Request Tracker for Incident Response
It was felt the development work was now complete, so this activity should be dropped.

Collaboration with the Joint Research Activity "Security" in the GN2 project
The GN2 project had now been replaced by GN3, although it was felt TF-CSIRT could provide useful input to the security activities within the new project. This work item should be updated in line with this, with Maurizio Molina (or Wayne Routly?) being assigned as the responsible person.

Liaison with the European Commission
It was felt more appropriate to liaise with ENISA rather than the European Commission directly, so this activity should be updated in line with this. Lionel Ferette should take formal responsibility, although a number of TF-CSIRT participants had advisory roles with ENISA.

Liaison with E-CoAT
The status of E-CoAT was unclear, and in any case there had been little communication in the past two years. It was agreed to drop this activity.

Incident handling and security guidelines for NREN Grids
This was still felt to be an extremely useful activity, and TF-CSIRT was directly liaising with the GRID-SEC group. Serge Droz and Torsten Voss already had responsibility for this.

Drill Exercises
It was felt this role had now passed to ENISA and national security agencies, so the activity should be dropped.

Evaluation of new tools
This activity had not really progressed in the past two years, so it was agreed it should be dropped.

The following new activity was suggested:

Deployment of Anti-spoofing Filters
Reflective attacks continue to be an issue on the Internet, and affect all stateless (i.e. UDP-based) services. Securing affected services does not fix the root cause of the problem, but if the majority of network providers implemented proper anti-spoofing filters, such attacks would not be possible any more. It was therefore proposed that TF-CSIRT members promote and support the deployment of anti-spoofing filters within their constituencies.

Action 30.3 – Serge Droz to formulate work item on anti-spoofing filters for new Terms of

Reference.

Kevin Meynell was asked to draft the new Terms of Reference, taking into account the above suggestions. These should first be circulated on the mailing list, before being submitted to TERENA for approval.

Action 30.4 – Kevin Meynell to draft new Terms of Reference for TF-CSIRT.

12. Date of next meeting

The next meeting will be held on 16-17 September 2010 in Istanbul, Turkey (hosted by Ulak-CSIRT).

Robert Schischka asked whether meetings could be announced further ahead than currently, as was the practice with CENTR. Kevin Meynell replied this was dependent on receiving offers to host the meetings, although meetings were already planned at least one year ahead. The dates and venues of TF-CSIRT meetings are listed at http://www.terena.org/events/ as soon as they are confirmed, and should also appear on the TF-CSIRT web pages at http://www.terena.org/tf-csirt/.

Open Actions

30.1 Kevin Meynell to liaise with Carlos Fuentes and Ulak-CSIRT to organise RTIR Workshop in Istanbul.

30.2 Kevin Meynell to ask Wilfried Wöber whether he is willing to be the responsible person for Work Item C in the Terms of Reference.

30.3 Serge Droz to formulate work item on anti-spoofing filters for new Terms of Reference.

30.4 Kevin Meynell to draft new Terms of Reference for TF-CSIRT.

Participants

Name	*Organisation*	*Country*
Shehzad Ahmed	DK-CERT (UNI-C)	Denmark
Mateo Araque	CCN-CERT	Spain
Giannis Askoxylakis	FORTH	Greece
Agris Belasovs	ENISA	-
Oskar Bergquist	SITIC	Sweden
Wim Biemolt	SURFcert	The Netherlands
Vladimir Bodor	TS-CERT CC (TeliaSonera)	Sweden
Matej Breznik	SI-CERT	Slovenia
Tomas Bukowski	CERT Polska (NASK)	Poland
Daniele Cattedu	ENISA	-
Panos Chatziadam	FORTH	Greece
Jorge Chinea Lopez	INTECO-CERT	Spain
Frederic Coene	Deloitte	Belgium
Andrew Cormack	JANET(UK)	United Kingdom
Michelle Danho	CERT-RENATER	France
Jerome Devigne	BELNET CERT	Belgium
Serge Droz	SWITCH-CERT	Switzerland
Andrea Dufkova	ENISA	-
Tobias Dussa	KIT-CERT	Germany
Per Arne Enstad	UNINETT CERT	Norway
Lionel Ferette (Chair)	BELNET CERT	Belgium
Carlos Fuentes	IRIS CERT	Spain
Mikael Ganev	RU-CERT	Russia
Slawomir Gorniak	ENISA	-
Kauto Huopio	FICORA/CERT-FI	Finland
Przemek Jaroszewski	CERT Polska (NASK)	Poland
Nino Jogun	CARNet	Croatia
Pavel Kacha	CESNET	Czech Republic
L. Aaron Kaplan	CERT.at	Austria
Baiba Kaskina	SigmaNet	Latvia
Klaus-Peter Kossakowski	DFN-CERT	Germany
Thomas Kristmar	Danish GovCERT	Denmark
Susanna Kristza	ACOnet-CERT	Austria
Andrea Kropacova	CESNET	Czech Republic
Hillar Leoste	Council of the European Union	-
Toomas Lepik	CERT-EE	Estonia
Sergey Linde	RU-CERT	Russia
Antonio Liu	PRESECURE	Germany
Detlev O. Matthies	DFN-CERT	Germany
Kevin Meynell (Secretary)	TERENA	-
Maciej Milostan	PIONIER-CERT (PSNC)	Poland
Benôit Moreau	CERTA	France
André Oosterwijk	GOVCERT.NL	The Netherlands
Dimos Panagopoulos	FORTH	Greece
Stefanos Papadakis	FORTH	Greece
Darko Perhoc	CARNET National CERT	Croatia
Nikolaos Petroulakis	FORTH	Greece
Leila Pohjolainen	FUNET CERT	Finland
Manuel Ransan	INTECO-CERT	Spain
Wayne Routly	DANTE	-
Ramon Saez	CCN-CERT	Spain
Lino Santos	CERT.PT	Portugal
Panagiotis Saragiotis	ENISA	-

Robert Schischka	CERT.at	Austria
Jacques Schuurman	SURFcert	The Netherlands
Derek Simpson	BT CERT CC	United Kingdom
Marc Stiefer	RESTENA-CSIRT	Luxembourg
Erika Stockinger	SITIC	Sweden
Egils Stūrmanis	DDIRV	Latvia
Alexey Sukhikh	RU-CERT	Russia
David Tabatadze	CERT-GE (GRENA)	Georgia
Alexander Talos-Zens	ACOnet-CERT	Austria
Marco Thorbruegge	ENISA	-
Marius Urkis	LITNET CERT	Lithuania
Ando Veldre	CERT-EE	Estonia
Dimitra Vitsa	FORTH CERT	Greece
Michal Wodzinski	DK-CERT (UNI-C)	Denmark

Apologies were received from:

Jimmy Arvidsson	TS-CERT CC (TeliaSonera)	Sweden
Martin Camilleri	mtCERT	Malta
Matthew Cook	Loughborough University	United Kingdom
Ralf Dörrie	Telekom-CERT	Germany
Peter Haag	SWITCH	Switzerland
Vincent Hinderer	CERT-LEXSI	France
Miroslaw Maj	CERT Polska (NASK)	Poland
Robert Morgan	JANET CSIRT	United Kingdom
Margrete Raaum	UiO-CERT	Norway
Don Stikvoort	S-CURE	The Netherlands
Thomas Stridh	SUNET CERT	Sweden
Jan Vykopal	CSIRT-MU	Czech Republic
Wilfried Wöber	ACOnet-CERT	Austria