



SUBJECT

Approved minutes of the 31st TF-CSIRT meeting
16 September 2010, Istanbul, Turkey

Page 1/6

31st TF-CSIRT meeting

16 September 2010

Marmara University Rectorate, Istanbul, Turkey

Please note that a seminar was held the following day. The presentations can be found at <http://www.terena.org/tf-csirt/meeting30/>

1. Approval of Minutes

The minutes of the last meeting held on 20 May 2010 were approved.

2. Actions from last meeting

- 30.1 Kevin Meynell to liaise with Carlos Fuentes and Ulak-CSIRT to organise RTIR Workshop in Istanbul.
Done, the workshop was held the following day.
- 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.
Done.
- 30.3 Serge Droz to formulate work item on anti-spoofing filters for new Terms of Reference.
Done.
- 30.4 Kevin Meynell to draft new Terms of Reference for TF-CSIRT.
Done, although these had subsequently been revised by the TERENA Secretary-General.

3. Ulak-CSIRT presentation

Murat Soysal gave a presentation about Ulak-CSIRT (see <http://www.terena.org/tf-csirt/meeting31/soysal-ulak-csirt.pdf>). This had been established in 2005 as part of ULAKBIM (the Turkish NREN) to provide incident handling for the Turkish research and education community. This had over 125 directly connected sites and around 1 million users.

Ulak-CSIRT was formed in response to a growing number of abuse complaints and the need to improve security in the network. There was also a demand for information in Turkish, as well as training of university staff.

The CSIRT itself is comprised of six staff who work part-time on incident handling issues. Two are ULAKBIM staff members, and the others are drawn from member universities. It has a 75% success rate in closure of incidents and has preempted a number of others through the ULAKNET Honeypot initiative.

As well as its national activities, Ulak-CSIRT is working with the NATO/CEENet CLOSER project which aims to build a network of operational CSIRTs in former CIS countries. It is

also participating in security related work in GN3, and is leading the CSIRT collaboration in the HP-SEE project for South Caucasus countries.

Lionel asked whether Ulak-CSIRT handled all incidents in Turkey. Murat replied that incidents outside of the ULAKNET constituency were handled by TR-CERT, although that was also part of their parent organisation TÜBİTAK.

4. RoCSIRT presentation

Manuel Subredu gave a presentation about RoCSIRT (see <http://www.terena.org/tf-csirt/meeting31/subredu-rocsirt.pdf>). This was a new CSIRT that primarily served RoEduNet, the Romanian NREN community, although in the absence of any other CSIRTs it also handled incidents in the entire .ro domain. It had been formed in January 2009 and had been accredited in August 2009.

In the past year the team had handled more than 1,600 incidents of which around 30-40% were resolved. Of the remaining 60-70%, there was insufficient data available for about half of these cases, which illustrated the difficulties faced within their constituency. Another issue was that the team was only part-time and was very short on manpower, so efforts were limited. However, they were building up a reliable network of contacts in the ISP and financial sectors, so it was hoped these statistics would improve.

5. CERT-MD presentation

Alexandr Golubev gave a presentation about CERT-MD (see <http://www.terena.org/tf-csirt/meeting31/golubev-cert-md.pdf>). This is part of RENAM, the Research and Education Network in Moldova which had around 30 sites and 80,000 users.

CERT-MD was formed in January 2007 in response to a NATO initiative, and primarily handles incidents from within the RENAM network, although it is also handles incidents from other constituencies in Moldova. It maintains a website where users as well as other teams can raise and track incidents.

Future plans include the improvement of security within the RENAM network, the development of a national CSIRT infrastructure, and the creation of an anti-DDOS network within Moldova.

Andrew Cormack asked whether it was good idea to allow users to trace the progress of incident resolutions. Alexandr replied they largely relied on users to report problems, and this aimed to show that their submissions were being acted upon.

6. EGI CSIRT

Michael Hausding gave an update on EGI CSIRT (see <http://www.terena.org/tf-csirt/meeting31/hausding-egi-csirt.pdf>). This provided incident response and security handling for the European Grid community, although it actually consisted of four groups.

The Incident Response Task Force (IRTF) handled day-to-day operational security issues and coordinated incident response across the EGI infrastructure. It was comprised of volunteers from more than 10 NRENS and NGIs who were on duty for a week at a time in rotation. The group also undertook vulnerability assessment using the monitoring tools developed by the Security Monitoring Group (SMG) and by examining critical components of the EGI infrastructure.

The Security Drills Group (SDG) undertakes realistic incident simulations to test the procedures of the constituent CSIRTs, and the communications channels between them. Each NGI or site is then graded to help formulate mitigation solutions.

Meanwhile, the Training and Dissemination Group (TDG) raises awareness of security issues amongst system administrators by providing training and developing best practice.

7. GN3 Tools Deployment Survey

Wayne Routly presented the results of the tools deployment survey that was undertaken by SigmaNet on behalf of the GN3-SA2/T4 activity (see <http://www.terena.org/tf-csirt/meeting31/routly-gn3-sa2-t4.pdf>). The aim was to describe the tools and procedures used across the GÉANT network, identify any missing components, and to provide input when designing and rolling out GÉANT services.

38 NRENS were surveyed in the areas of communication, network monitoring, service monitoring, and incident handling and tracking. The results revealed the most method of communication was e-mail, closely followed by the telephone. Other forms of communication included web forms, instant messaging and SMS.

The most widely used network flow tool was NFDump/NFSEN followed by tcpdump, Peakflow and other assorted off-the-shelf and home-grown tools; whilst with network monitoring it was Nagios followed by MRTG, CACTI and Munion. In the area of tracking and ticketing, RTIR was by far the most popular system.

Overall conclusions were that 10% of the respondents were still without an incident handling and tracking mechanism. In addition, 24% did not make their public PGP keys available even though secure communications are important for establishing trust mechanisms, whilst 16% did not have any contact information in English. Finally, 20% of the respondents did not have any incident reporting forms online, although some questioned whether this was actually desirable.

8. TRANSITS/TRANSITS2 update

Don Stikvoort gave an update on the recent and forthcoming TRANSITS courses (see <http://www.terena.org/tf-csirt/meeting31/stikvoort-transits.pdf>).

A TRANSITS workshop had been held on 7-8 September 2010 in Karlsruhe and had involved more than 30 participants. The next workshop would be held in January 2011, probably also in Germany (venue to be confirmed).

A TRANSITS II workshop was also being held on 5-7 October 2010 in Amsterdam. This would consist of more advanced topics such as network forensics, monitoring and communications skills, and the aim was to evaluate these new modules as well as determine whether any subject matter should be added or removed. This event would also be used to judge whether or not standalone TRANSITS II workshops would continue, or whether individual modules would be taught on a standalone basis in future.

9. AbuseHelper Discussion

Christian Van Heurck raised the issue of a collaboration to improve the AbuseHelper system (see <http://www.terena.org/tf-csirt/meeting31/vanheurck-abusehelper.pdf>). This

was a open source framework originally developed by CERT-EE and CERT-FI to automate incident report processing based on a variety of inputs such as blacklists, intrusion detection systems and Whois.

BELNET CERT and CERT.be were increasingly using this system for their own activities, but had discovered a few things that could be improved and wondered whether any other CSIRTs were interested in helping with this. This included better integration with RTIR and exchange of intrusion detection data amongst other things.

There followed a discussion on the suggested improvements, and CSIRTs interested in following these up were asked to contact Christian.

10. Spamhaus Discussion

Varis Teivans opened the discussion about Spamhaus by outlining the problems experienced by SigmaNet (see <http://www.terena.org/tf-csirt/meeting31/teivans-spamhaus.pdf>). SpamHaus had incorrectly blacklisted certain IP addresses, and then failed to address these issues when this had been pointed out to them. This was contrary to the principles of fair justice, but it effectively also prevented innocent users from sending e-mails because of the actions of someone else.

The intentions of Spamhaus had originally appeared to be good, but their method of operation and refusal to respond to the concerns of legitimate organisations was now a concern. Varis asked whether others had experienced similar problems, and whether TF-CSIRT could take any action to address this problem.

Several other teams said they'd had similar problems with Spamhaus, which seemed to have become increasingly heavy handed over time. However, it was felt this more an issue for Trusted Introducer, and that appropriate courses of actions should be discussed further by the TI Review Board. Varis was asked whether CERT NIC.LV could document specific cases so these could be used as evidence.

Action 31.1 – TI Review Board to discuss how to deal with Spamhaus problems and what further action to take.

Action 31.2 – CERT NIC.LV to document specific problems they had experienced with Spamhaus.

11. Date of next meeting

The next meeting will be held on 1-2 February 2011 in Barcelona. Spain (hosted by la Caixa). This would be in conjunction with the FIRST Symposium.

Open Actions

31.1 TI Review Board to discuss how to deal with Spamhaus problems and what further action to take.

31.2 CERT NIC.LV to document specific problems they had experienced with Spamhaus.

Participants

<i>Name</i>	<i>Organisation</i>	<i>Country</i>
Shehzad Ahmed	DK-CERT (UNI-C)	Denmark
Gokhan Akin	Ulak-CSIRT (ULAKBIM)	Turkey
Jimmy Arvidsson	TS-CERT CC (TeliaSonera)	Sweden
Morten Bartvig	DK-CERT (UNI-C)	Denmark
Wim Biemolt	SURFcert	The Netherlands
Vladimir Bodor	TS-CERT CC (TeliaSonera)	Sweden
Panos Chatziadam	FORTHcert	Greece
Andrew Cormack	JANET(UK)	United Kingdom
Goran Čuljak	ISSB	Croatia
Michelle Danho	CERT-RENATER	France
James Davies	JANET CSIRT	United Kingdom
Andrea Dufkova	ENISA	-
Lionel Ferette (Chair)	BELNET CERT	Belgium
Carlos Fuentes Bermejo	IRIS CERT	Spain
Manuel Garcia Cervigón	esCERT-UPC	Spain
Alexandr Golubev	RENAM	Moldova
Tilman Haak	DFN-CERT	Germany
Michael Hausding	SWITCH	Switzerland
Dmitry Ippolitov	RU-CERT	Russia
Thorben Jaendling	SWITCH-CERT	Switzerland
Przemek Jaroszewski	CERT Polska (NASK)	Poland
Robert Jonsson	Sitic	Sweden
Łukasz Juszczyk	CERT Polska (NASK)	Poland
Urpo Kaila	FUNET CERT	Finland
L. Aaron Kaplan	CERT.at	Austria
Domagoj Klasic	CARNet	Croatia
Susanna Kristza	ACOnet-CERT	Austria
Andrea Kropacova	CESNET	Czech Republic
Antonio Liu	PRESECURE	Germany
Egil Mannerheim	Swedbank SIRT	Sweden
Detlev O. Matthies	DFN-CERT	Germany
Branko Mažar	CARNet	Croatia
Kevin Meynell (Secretary)	TERENA	-
Maciej Milostan	PIONIER-CERT (PSNC)	Poland
Gustavo Neves	FCCN	Portugal
Thomas Nguyen-Van	Jumper Consulting	Ireland
André Oosterwijk	GOVCERT.NL	The Netherlands
Martin Peterka	CZ.NIC	Czech Republic
Ian Pomfret	BT CERT CC	United Kingdom
Wayne Routly	DANTE	-
Jacques Schuurman	SURFcert	The Netherlands
Luis Servin	PRE-CERT	Germany
Murat Soysal	Ulak-CSIRT (ULAKBIM)	Turkey
Pascal Steichen	CIRCL	Luxembourg
Don Stikvoort	Trusted Introducer	-
Erika Stockinger	Sitic	Sweden
Egils Stūrmanis	DDIRV	Latvia
Manuel Subredu	RoCSIRT (Agency ARNIEC)	Romania
Alexey Sukhikh	RU-CERT	Russia
Harri Sylvander	FUNET CERT	Finland
Alexander Talos-Zens	ACOnet-CERT	Austria
Melih Tasdizen	Mamara University	Turkey
Varis Teivans	CERT NIC.LV (SigmaNet)	Latvia

SUBJECTApproved minutes of the 31st TF-CSIRT meeting
16 September 2010, Istanbul, Turkey

Marius Urkis	LITNET CERT	Lithuania
Christian Van Heurck	BELNET CERT	Belgium
Simona Venuti	GARR-CERT	Italy
Torsten Voss	DFN-CERT	Germany
Adrian Wiedemann	KIT-CERT	Germany
Stefan Winter	RESTENA	Luxembourg
Michael Wozinski	DK-CERT (UNI-C)	Denmark
Wilfried Wöber	ACOnet-CERT	Austria
Husevin Yüce	Ulak-CSIRT (ULAKBIM)	Turkey
Emre Yüce	Ulak-CSIRT (ULAKBIM)	Turkey

Apologies were received from:

Mateo Araque	CCN-CERT	Spain
Jorge China Lopez	INTECO-CERT	Spain
Serge Droz	SWITCH CERT	Switzerland
Till Dörge	PRE-CERT (PRESENSE)	Germany
Ralf Dörrie	Telekom-CERT	Germany
Mikhail Ganev	RU-CERT	Russia
Vincent Hinderer	CERT-LEXSI	France
Baiba Kaskina	CERT NIC.LV (SigmaNet)	Latvia
Sergey Linde	RU-CERT	Russia
Margrete Raaum	UiO-CERT	Norway
Han van Thoor	Jumper CSIRT	Ireland