



SUBJECT

Approved minutes of the 34th TF-CSIRT meeting
22 September 2011, Luxembourg City, Luxembourg
Version 1.1

Page 1/7

34th TF-CSIRT meeting

22 September 2011

Abbaye de Neumünster, Luxembourg City, Luxembourg

Please note that a seminar was held the following day. The presentations can be found at <http://www.terena.org/tf-csirt/meeting34/>

1. Approval of Minutes

The minutes of the last meeting held on 2 June 2011 were approved.

2. Actions from last meeting

- 31.1 TI Review Board to discuss how to deal with Spamhaus problems and what further action to take.
Ongoing - awaiting information from CERT.LV
- 32.2 Marco Thorbrügge to send pointer to information about Article 13a to the mailing list.
Ongoing.
- 33.1 Serge Droz to invite CENTR to participate in TF-CSIRT meeting in Luxembourg.
Done, although no-one was able to come to Luxembourg.
- 33.2 Kevin Meynell to draft proposal for new TF-CSIRT group and circulate to TF-CSIRTng Working Group.
Done.

3. GOVCERT.LU presentation

Patrick Houtsch gave a presentation about GOVCERT.LU (see <http://www.terena.org/tf-csirt/meeting34/houtsch-govcert.lu.pdf>).

This is a new team created in July 2011 to provide incident handling and response capabilities to government ministries and other administrations (covering approximately 12,000 personnel). It is operated by the Ministry of State and was formed as a result of collaboration between CTIE, HCPN, ANS, CCG/ANSSI and CASES/CIRCL. It is located in secure premises at CTIE (State IT Centre) which previously acted as the de-facto government CSIRT.

There are currently seven employees who provide incident handling, notification and response services under Phase 1 of the deployment plan, as well as provide secretariat services to the national Cybersecurity Board. The aim is to expand these services to malware and vulnerability analysis and eventually security consultancy in Phases 2 and 3.

Bob van der Kamp asked about the composition of Cybersecurity Board. Patrick replied that all government ministries were represented on this.

Lionel asked about the timetable for Phases 2 and 3 of the deployment plan. Patrick replied there was no specific timetable, although Phase 2 was expected to begin sometime next year.

4. CERT-DEVOTEAM presentation

Olivier Caleff gave a presentation about CERT-DEVOTEAM (see <http://www.terena.org/tf-csirt/meeting34/caleff-devoteam.pdf>). This was a re-branding of the former APOGEE SecWatch in order to provide CSIRT activities for the whole DEVOTEAM group across 24 countries.

APOGEE Communications had been offering security watch activities to the banking sector since 1996, and incident handling and forensics services since 2000. In 2003, they were acquired by DEVOTEAM, an ICT consultancy company, and were listed by TI in 2007. They had recently become accredited.

They offered a full range of reactive and proactive services, as well as security quality management. They particularly specialised in security alerting, anti-fraud techniques and forensics in the banking and travel sectors, but also involved with ISPs, national governments and international organisations.

5. XS4ALL Abuse presentation

Jacques Schuurman and Arjan van Hattum gave a presentation about XS4ALL Abuse (see <http://www.terena.org/tf-csirt/meeting34/schuurman-xs4all.pdf>). This was a medium-sized ISP based in the Netherlands that had started in 1994, and now offered xDSL and fibre connectivity as well as hosting services. Although it was acquired by KPN in 1998, the company maintained a lot of independence, and in particular a commitment to social engagement. This specifically meant user-friendly services, extending Internet access to deprived societies, and participation in the Internet (self-)regulation process.

As a result, XS4ALL Abuse was established as the incident handling and response team for XS4ALL, although KPN-CERT also provided support to the whole group. The challenges of dealing with average Internet users were different as they were often unaware of problems. Moreover, the lack of precautionary measures, prevalence of malware, and often legacy equipment often made it difficult to provide support to users who perceived the Internet as a utility rather than a complex service. Nevertheless, they were developing a central abuses database that could log and recognise particular problems, and allow fine grained control over end user access in response to changing circumstances.

Andrew Cormack noted there seemed to be a higher prevalence of quarantining users, whereas there was more resistance to doing this in the UK. Jacques replied that he felt the ISP market was more competitive in the Netherlands which meant that abuse issues needed to be addressed more quickly otherwise custom would be lost.

6. Funet CERT team update

Harri Sylvander gave a short update on forthcoming changes at Funet CERT (see <http://www.terena.org/tf-csirt/meeting34/sylvander-funet.pdf>). He announced that he would shortly be leaving to take a new position elsewhere, whilst Pekka Savola was currently on extended leave to undertake a law degree. Leila Pohjolainen was also now only working part-time.

Timo Porjamo would be the new team leader, with Otto Mäkelä joined him on a half-time basis. However, it did mean the team would have limited effort for a while.

Lionel Ferette wished Harri success in his future position and thanked him for his contributions to TF-CSIRT over the years.

7. RtirBot demonstration

Harri Sylvander demonstrated RtirBot (see <http://www.terena.org/tf-csirt/meeting34/sylvander-rtirbot.pdf>).

The AbuseHelper software currently under development by several CSIRTs allowed for automated collection and handling of incident data, but lacked an easy way of tracking trends and creating alerts. One solution was therefore to utilise the RTIR tracking software by feeding in AbuseHelper data to generate and link tickets that would allow batch resolution of common incidents. RtirBot was a modified version of WikiBot that uses pre-configured templates and the RT REST API to submit tickets.

8. Security Awareness Raising

Varis Teivāns gave a presentation about the Esi Drošs portal that had been launched by CERT.LV in May 2011 (see <http://www.terena.org/tf-csirt/meeting34/teivans-raising-awareness.pdf>). This aimed to raise user awareness of security issues by providing information on the newest viruses and threats, as well as offering useful articles and recommendations on security. Many of the most popular web pages contained malicious links or malware, and it was important to educate users on the steps they should take to minimise risk.

There was not yet any funding for the project, so all the contributions were currently made on a voluntary basis. However, the aim was promote this activity through social media, seminars and information days and the press, with a view to soliciting more input.

Varis was asked whether the CERT.LV statistics included schools. He replied they were not currently included.

9. Privacy in Incident Handling: 2011 update

Andrew Cormack provided an update to his earlier paper on incident response and data protection (see <http://www.terena.org/tf-csirt/meeting34/cormack-privacy.pdf>).

This paper had originally been published in 2010 and had suggested how to balance individual privacy against the need for CSIRTs to respond to incidents. The latest update addressed how improved automated processing can limit the need for manual inspection, and the issues surrounding the identification of DDoS victims.

Andrew asked whether the TF-CSIRT community was happy to publish this update on the TF-CSIRT website as input to the forthcoming ENISA report on legal barriers to information sharing. It is hoped this may inform the current revision of the existing EU Data Protection Directive.

It was agreed this could be published on the TF-CSIRT website, where it can found at <http://www.terena.org/tf-csirt/publications/data-protection-v2.pdf>

10. AbuseHelper update

Christian Van Heurck reported on the progress of AbuseHelper, as well as developments at the SEC-T workshop earlier in September (<http://www.terena.org/tf-csirt/meeting34/vanheurck-abusehelper.pdf>).

The aim of the pilot installation was to test the automated report generation against the initial inputs, with a view to extending it to use IDS/IPS logs, honeypots and other sources. The goal was let the systems do all the work up until the creation of the incident ticket, and thereby free up manpower for value-added tasks. The system appears to work fairly well, but there needs to be 100% confidence that no information is being lost.

However, AbuseHelper still has quite a steep learning curve as it requires Python programming skills and there is limited/no documentation. It also uses components such as MangoDB and RIS which have an unclear development path, and the flow-centric architecture limits customised querying. A central database interfacing to existing incident handling tools (e.g. RTIR) and customisable visualisation capabilities is also desirable, along with an API that would allow the querying and export of data.

At SEC-T, CERT-SE offered a BGP routing table to match AP-ASNs, and a BGP-ranking bot was developed during the event. CERT-EE also offered to setup a S2S XMPP server for push and/or retrieval of data, whilst Megatron will develop a XMPP connector. At the present time though, no IPv6 sources are available.

11. TRANSITS I & II update

Don Stikvoort reported on the recent TRANSITS I course, and provided an update on developments (see <http://www.terena.org/tf-csirt/meeting34/stikvoort-transits.pdf>).

The latest TRANSITS I course had been held on 8-9 September 2011 near Dublin, Ireland. This had again been well attended and the new operational module had been presented for the first time.

The technical module was currently being updated and was due to be completed in December. The legal module was also scheduled to be updated in early-2012 as this was now starting to get outdated. It had been decided to drop the advisories as few CSIRTs now issued these, which would leave more time for the roleplay based on the ENISA exercises.

The next TRANSITS I workshop was planned for March/April 2012, possibly in Portugal. Another TRANSITS II workshop was also planned for early-2012 in Prague, Czech Republic.

12. TF-CSIRT& TI: Next Steps

Kevin Meynell provided an update on the proposal to restructure TF-CSIRT and Trusted Introducer (see <http://www.terena.org/tf-csirt/meeting34/meynell-tf-csirtng.pdf>).

Some ideas had been presented at the previous meeting, and Kevin had been asked to produce a paper that summarised the current situation, made the case for change, and provided more detail on the specific ideas. A Working Group had also been formed to provide feedback on this paper, and this had been sent to them on 2 August 2011.

A number of comments were received that were taken into account when this was

discussed further within TERENA. These comments were positive, but some small changes needed to be made to the paper before it could be circulated to the whole TF-CSIRT community. Unfortunately, this could not be done in time for this meeting, but the plan was to publish the paper well in advance of the next meeting in January 2012. The aim would be to achieve a consensus in Rome, and if this happened, the next steps would be to draft new terms of reference and seek approval from the appropriate TERENA bodies.

The Working Group had made a number of suggestions, one of which was that increasingly artificial distinction between the TF-CSIRT meeting and seminar be abolished. Informational presentations often took place in the meeting itself, and similarly it might be useful to schedule discussion sessions on the second day. The proposal was therefore to just allocate slots for presentations or discussions as appropriate.

Another suggestion was that the TRANSITS training courses should formally fall under the TF-CSIRT umbrella, and this was something that had come out of internal TERENA discussions as well.

TI should also be better promoted beyond its traditional NREN focus by identifying teams in different sectors and making contact. Indeed, steps had already been made in this direction with the new TI team's effort to contact all national and government CSIRTs in Europe. In addition, there should be a clear statement about what TF-CSIRT/TI is, what it does, and the benefits of being involved.

Finally, a TF-CSIRT logo should be introduced which would complement the 'new' TI logo.

Kevin reaffirmed that TERENA was committed to supporting TF-CSIRT and TI, and the administration would continue to be funded from the GN3 project until April 2013. The CSIRTs themselves though, could decide how to organise their meetings and appoint their officials. It was felt that TF-CSIRT should become an umbrella for TI and TRANSITS, as well as other security-related activities, and it should be clearly established that TI was a TERENA and TF-CSIRT service. More specifically though, the TI accredited, listed and associate categories should be used as the basis for TF-CSIRT participation.

Andrew Cormack pointed out that the list of TF-CSIRT activities was rarely covered in meetings these days. Kevin replied that was because most were now a generic nature and took place in the context of activities such as TI and TRANSITS anyway. In addition, whilst the list of activities were revised every couple of years, there were some currently dormant items (e.g. RTIR and CSIRT mentoring), although they could conceivably be revived if there was sufficient interest.

13. Date of next meeting

Lionel Ferette thanked RESTENA and CIRCL for hosting the meeting in Luxembourg.

The next meeting will be a joint FIRST/TF-CSIRT Technical Colloquium that will held on 30 January – 1 February 2012 in Rome, Italy (hosted by TERENA & GARR-CERT).

Open Actions

- 31.1 TI Review Board to discuss how to deal with Spamhaus problems and what further action to take.
- 32.1 Marco Thorbrügge to send pointer to information about Article 13a to the mailing list.

SUBJECT

Approved minutes of the 34th TF-CSIRT meeting
22 September 2011, Luxembourg City, Luxembourg

Participants

<i>Name</i>	<i>Organisation</i>	<i>Country</i>
Shehzad Ahmad	DK-CERT (UNI-C)	Denmark
Mowgli Assor	OSU-IRT	United States
Wim Biemolt	SURFcert (SURFnet)	The Netherlands
Vladimir Bobor	TS-CERT CC	Sweden
Jean-Pierre Borsa	Luxembourg Bankers' Association	Luxembourg
Pierre-Sébastien Bost	ANSSI/COSSI/CERTA	France
Olivier Caleff	CERT DEVOTEAM	France
Steve Clement	CIRCL	Luxembourg
Ian Cook	Team Cymru	United Kingdom
Andrew Cormack	JANET(UK)	United Kingdom
Michelle Danho	CERT-RENATER	France
Serge Droz	SWITCH-CERT	Switzerland
Alexandre Dulaunoy	CIRCL	Luxembourg
Jacqueline Dulmaine	BELNET	Belgium
Torsten Enquist	TS-CERT CC	Sweden
Lionel Ferette (Chair)	-	Belgium
Antoni Fertner	JANET(UK)	United Kingdom
Tilman Haak	DFN-CERT	Germany
Michael Hamm	CIRCL	Luxembourg
Arjan van Hattum	XS4ALL Internet	The Netherlands
Ingunn Holte	NorCERT	Norway
Patrick Houtsch	GOVCERT.LU	Luxembourg
Dimitry Ippolitov	RU-CERT	Russia
Przemek Jaroszewski	CERT Polska (NASK)	Poland
Thorben Jändling	SWITCH-CERT	Switzerland
Bob van der Kamp	GOVCERT.NL	The Netherlands
L. Aaron Kaplan	CERT.at	Austria
Domagoj Klasic	Croatian National CERT	Croatia
Klaus-Peter Kossakowski	PRESECURE	Germany
Andrea Kropacova	CZ.NIC	Czech Republic
Toomas Lepik	CERT-EE	Estonia
Morten Linneman	DK-CERT (UNI-C)	Denmark
Antonio Liu	Trusted Introducer	Germany
Peter Magula	CSIRT.SK	Slovakia
Mirek Maj	Cybersecurity Foundation	Poland
Chelo Malagón	RedIRIS	Spain
Gilles Massen	RESTENA CSIRT	Luxembourg
Kevin Meynell (Secretary)	TERENA	-
Milda Mimiene	LITNET CERT	Lithuania
Marie Moe	NorCERT	Norway
Dave Monnier	Team Cymru	United States
Otto Mäkelä	Funet CERT	Finland
Tomasz Nowocień	PIONIER-CERT	Poland
Tomas Plesnik	CSIRT-MU	Czech Republic
Bogdan Popescu	CERT-RO	Romania
Tomislav Protega	Croatian National CERT	Croatia
Bruno Prémont	RESTENA-CSIRT	Luxembourg
Juan Quintanilla	DANTE	-
Dennis Rand	DK-CERT (UNI-C)	Denmark
Sascha Rommelfangen	CIRCL	Luxembourg
Bart Roos	GOVCERT.NL	The Netherlands
Wayne Routly	DANTE	-
Philippe Schultz	European Commission	-

SUBJECT

Approved minutes of the 34th TF-CSIRT meeting
22 September 2011, Luxembourg City, Luxembourg

Timo Schulz	DFN-CERT	Germany
Jacques Schuurman	XS4ALL Internet	The Netherlands
Manual Silvosu	Ministère de l'Économie	Luxembourg
Derek Simpson	BTCERTCC	United Kingdom
Pascal Steichen	CIRCL	Luxembourg
Marc Stiefer	RESTENA-CSIRT	Luxembourg
Don Stikvoort	S-CURE	The Netherlands
Erika Stockinger	CERT-SE	Sweden
Alexey Sukhikh	RU-CERT	Russia
Harri Sylvander	Funet CERT	Finland
Alexander Talos-Zens	University of Vienna	Austria
Varis Teivans	CERT.LV	Latvia
Dan Tofan	CERT-RO	Romania
Colin Tomlinson	S-CURE	The Netherlands
Sebastien Tricaud	Picviz Labs	France
Marius Urkis	LITNET CERT	Lithuania
Christian Van Heurck	BELNET CERT	Belgium
Anto Veldre	CERT-EE	Estonia
Jan Vykopal	CSIRT-MU	Czech Republic
Gerard Wagener	CIRCL	Luxembourg
Stefan Winter	RESTENA-CSIRT	Luxembourg
Mirko Wollenberg	PRESECURE	Germany
Goran Čuljak	ISSB	Croatia

Apologies were received from:

Jorge Chinaa	INTECO-CERT	Spain
Matthew Cook	ESISS (Loughborough Univ.)	United Kingdom
Vincent Hinderer	CERT-LEXSI	France
Branko Mažar	CARNet	Croatia
Margrete Raaum	UiO-CERT	Norway
Thomas Stridh	SUNET CERT	Sweden
Wilfried Wöber	ACOnet-CERT	Austria