



SUBJECT

Approved minutes of the 28th TF-CSIRT meeting
25 September 2009, Tallinn, Estonia

Page 1/6

28th TF-CSIRT meeting

25 September 2009

National Library of Estonia, Tallinn, Estonia

Please note that a seminar was held the previous day. The presentations can be found at <http://www.terena.org/activities/tf-csirt/meeting28/>

1. Approval of Minutes

The minutes of the last meeting held on 18 May 2009 were approved.

2. Actions from last meeting

27.1 Marco Thorbrügge and Alexander Talos-Zens to update new CHIHT website.
Done.

27.2 Lionel Ferette to circulate some ideas about drill exercises on the mailing list.
Ongoing, although some ideas were presented later in the meeting.

3. TS-CERT Presentation

Jimmy Arvidsson gave a presentation about TS-CERT (see <http://www.terena.org/activities/tf-csirt/meeting28/arvidsson-teliasonera.pdf>). This is responsible for IT security within TeliaSonera, which was an amalgamation of the incumbent Swedish and Finnish telecommunications companies Telia AB and Sonera Corporation. It currently operates in 20 countries (primarily Scandinavia and the former Soviet Union) and has around 32,000 employees and 88 subsidiary companies. It also had around 128 million subscribers and revenue of approximately USD 15.7 billion in 2008.

TS-CERT has overall responsibility for IT security within the company, but has relationships with 12 sub-CERTs in various countries who deal with specific constituencies. Procedures and working practices are determined by operational level agreements, whilst incidents are logged and responses coordinated by the TS-CERT Coordination Centre. It also works closely with internal fraud investigators, and if necessary, external agencies such as the police and insurance companies.

Lionel Ferette asked how many employees were working in IT security. Jimmy replied it was around 60.

4. CSIRT-MU Presentation

Jan Vykopal gave a presentation about CSIRT-MU (see <http://www.terena.org/activities/tf-csirt/meeting28/vykopal-csirt-mu.pdf>). This was the incident response team of Masaryk University in the Czech Republic, which had more than 40,000 students in nine faculties and three institutes.

The team was established in 2008 and was currently comprised of 2 FTEs who provided

incident handling, intrusion detection, alerts and warnings, and penetration testing services. It was part of the wider CESNET-CERT constituency, and had been listed by Trusted Introducer in June 2009.

At the present time, the team dealt with about 10 external incidents per week, but had also discovered a number of new viruses internally with their NetFlow monitoring systems. They were also undertaking an analysis of internal threats for the Czech military, and developing an intelligent logging server for correlating heterogeneous data from their NetFlow probes.

Wilfried Wöber asked whether they were undertaking any profiling of the hosts using NAT. Jan replied they were really just trying to get an idea of numbers at the present time.

Maurizio Molina then asked why they were correlating information from different sources, and was anyone using this information. Jan replied this was to build up as complete a picture as they could, in the hope that trends and attacks could be more easily identified.

5. Raiffeisen Informatik CERT presentation

Christian Proschinger gave a presentation about the Raiffeisen Informatik CERT (see <http://www.terena.org/activities/tf-csirt/meeting28/proschinger-ri-cert.pdf>). This was one of the largest IT services and data centre providers in Austria, which included providing security services to financial institutions.

6. Cooperative Cyber Defence Centre of Excellence

Kenneth Geers gave a talk about the Cooperative Cyber Defence Centre of Excellence. This was established in May 2008 in order to improve cooperation and knowledge of electronic warfare amongst NATO nations and their partners, whilst developing their capabilities to defend against such attacks. It currently involves Estonia, Germany, Italy, Latvia, Lithuania, Slovakia, Spain and the United States, and is based in Tallinn where it employs 30 people.

They were specifically interested in military computing and how to protect against 'digital Pearl Harbor' scenarios, but military computers were subject to many of the same problems as civilian computers. They therefore envisaged the involvement of CSIRTs in their programme of work, and were keen to establish relationships with organisations such as TF-CSIRT.

Andrew Cormack asked whether information published by CCDCoE would be publicly available. Kenneth replied this still needed to be determined, but to date his papers had been made public, and he envisaged that an open source academic style would continue in future.

7. RIPE Community Developments

Wilfried Wöber mentioned there had been discussions at the last RIPE meeting as to how to improve communication between the RIPE and law enforcement communities. One of the ideas was to establish a task force to discuss the issues and decide to proceed, and a kickoff meeting had been organised Amsterdam earlier in the week. This would also be discussed further at the next RIPE meeting in Lisbon, and he would report on the outcome at the next TF-CSIRT meeting.

Wilfried also reminded participants about the activities of the RIPE Anti-Abuse Working Group, and pointed to the mailing list discussions that were archived at <http://www.ripe.net/ripe/maillists/archives/anti-abuse-wg/2009/index-thread.html>. It was possible to participate in the discussions without being a member of the mailing list, although postings from non-members first went to a moderator for approval.

8. TRANSITS update

Don Stikvoort provided a short update on the latest TRANSITS developments (see <http://www.terena.org/activities/tf-csirt/meeting28/stikvoort-transits.pdf>). Fifteen of the TRANSITS trainers had met two days earlier in Tallinn, in order to discuss future directions. The plan was to develop a number of advanced TRANSITS modules (e.g. forensics) in order to supplement the existing courses, although the focus of these still needed to be discussed.

9. A brainstorming on security fire drills

Maurizio Molina provided some ideas for security fire drills in the context of the GN3 project SA3/T4 activity (see <http://www.terena.org/activities/tf-csirt/meeting28/molina-fire-drills.pdf>). This activity had started in April 2009 and was focusing on providing security for the multi-domain services in GN3. These required a lot of coding and deployment that needed to be tested for security flaws, and it would be useful to involve groups that already had experience of this.

At the present time though, they were trying to determine the tests and resources needed, but also the criteria for determining successful tests. These meant reviewing the list of proposed tests, excluding those that were unfeasible, and prioritising others. This could be done in consultation with TF-CSIRT and possibly ENISA, who might themselves be able to benefit from the results.

Peter Haag thought such drills required a lot of effort and should be done in a closed environment. However, they can be valuable as they expose weaknesses and shortcomings.

There was the comment there needed to be separation between those devising the drills and those doing the securing, otherwise there was a danger that the drills would not discover previously unknown vulnerabilities.

JP Velders suggested running multiple drills in parallel as it would provide a more realistic scenario. Maurizio replied this was something to consider.

10. Grid Security update

Serge Droz reported on the liaison with the Grid Security Group (see <http://www.terena.org/activities/tf-csirt/meeting28/droz-gridsec.pdf>). He said that Torsten Voss and himself were on the grid-sec mailing list, which also comprised two representatives from each Grid.

To date, there had been two major grid security incidents, but no specific Grid exploits had yet been seen. However, the one thing to realise is that the Grid works differently to the NREN/ISP world. For example, every Grid job runs under a User ID which if compromised, can cause problems for all Grid nodes that allow access to this. It is therefore necessary to block User IDs rather than IP addresses, which is further

complicated by the fact that Virtual Organisations (VOs) rather than host organisations are responsible for any given ID. Furthermore, forensics are complicated by the fact that Grid jobs typically use a toolkit that adds an additional layer. This requires that CSIRTs become more familiar with Grid procedures and terminology.

Andrew Cormack mentioned that he'd written a guide on supporting grids which was available at <http://www.ja.net/documents/publications/technical-guides/grid-support-web.pdf>.

JP Velders added that many smaller Grids had also started popping up, which didn't appear to give security issues a high priority. He therefore wondered whether anything could be done to encourage them to get more involved in security issues.

11. DNS White Lists

JP Velders gave a presentation about DNS white lists (see <http://www.terena.org/activities/tf-csirt/meeting28/velders-dns-whitelists.pdf>). DNS black lists were commonly used for filtering spam, but the academic world in particular has a need for widespread e-mail contacts and cannot really block domains en-bloc. SURFnet were therefore looking into setting up a white listing infrastructure whereby lists of legitimate servers could be used to reduce the chances of false positives when spam filtering. However, they needed input and feedback, so they were therefore looking for other organisations interested in participating in the trial.

12. Date of next meeting

The next meeting will be held on 25-26 January 2010 in Hamburg, Germany (hosted by DFN-CERT). This would be in conjunction with the FIRST Symposium.

Till Döriges added that the 1st European Workshop on Internet Early Warning and Network Intelligence (EWNI 2010) would also be held adjacent to the next meeting on 27 January 2010. This was being supported by ENISA and PRESENSE, and aimed to bring together those involved in early warning initiatives. The Call for Papers would be sent out shortly.

13. Any other business

Ian Bryant raised the issue of whether TF-CSIRT should become a liaison member in the ISO 27010 information security management drafting process. Lionel replied that it would formally have to be TERENA as TF-CSIRT wasn't a legal entity, but polled the meeting participants as whether they thought this was a good idea.

There was some support for the idea and no objections, so Lionel resolved to ask TERENA whether they could make an application to become a liaison member.

Action 28.1 – Lionel Ferette to ask TERENA whether they can apply to be a ISO 27010 liaison member.

Open Actions

- 28.1 Lionel Ferette to ask TERENA whether they can apply to be a ISO 27035 liaison member.
- 27.3 Lionel Ferette to circulate some ideas about drill exercises on the mailing list.

Participants

<i>Name</i>	<i>Organisation</i>	<i>Country</i>
Hillar Aareleid	CERT-EE	Estonia
Bente Christian Åsgård	UiO-CERT	Norway
Shehzad Ahmed	DK-CERT (UNI-C)	Denmark
Mateo Araque	CCN-CERT	Spain
Jimmy Arvidsson	TeliaSonera CERT	Sweden
Oscar Berququist	SITIC	Sweden
Wim Biemolt	SURFcert	The Netherlands
Vladimir Bodor	TS-CERT (TeliaSonera)	Sweden
Lasse Trolle Borup	DK-CERT (UNI-C)	Denmark
Ian Bryant	MS3i Project	United Kingdom
Robert Cecchini	GARR-CERT	Italy
Matthew Cook	EMMAN/Loughborough Univ.	United Kingdom
Andrew Cormack	JANET(UK)	United Kingdom
Michelle Danho	CERT-RENATER	France
Serge Droz	SWITCH-CERT	Switzerland
Till Döriges	PRE-CERT/PRESENCE	Germany
Per Arne Enstad	UNINETT CERT	Norway
Lionel Ferette (Chair)	BELNET CERT	Belgium
Thomas Gayet	CERT-LEXSI	France
Peter Haag	SWITCH-CERT	Switzerland
Michael Hausding	SWITCH-CERT	Switzerland
Przemek Jaroszewski	CERT Polska (NASK)	Poland
Nino Jogun	CARNet	Croatia
Urpo Kaila	FUNET CERT	Finland
Baiba Kaskina	SigmaNet	Latvia
Andrea Kropacova	CESNET	Czech Republic
Håvard Kuslid	UNINETT CERT	Norway
Hilar Leoste	Council of the European Union	Belgium
Toomas Lepik	CERT Estonia	Estonia
Antonio Liu	PRESECURE	Germany
Branko Mažar	CARNet	Croatia
Ģirts Mažonis	DDIRV	Latvia
Kevin Meynell (Secretary)	TERENA	-
Maurizio Molina	DANTE	-
Francisco Monserrat	RedIRIS	Spain
Benôit Moreau	CERTA	France
Gustavo Neves	CERT.PT	Portugal
Tomasz Nowocien	PIONIER-CERT/PSNC	Poland
Andre Oosterwijk	GOVCERT.NL	The Netherlands
Karlis Podins	CCDCoE	-
Leila Pohjolainen	FUNET CERT	Finland
Timo Porjamo	FUNET CERT	Finland
Michal Prochazka	CESNET	Czech Republic
Christian Proschinger	Raiffeissen Informatik CERT	Austria
David Pybus	Diageo	United Kingdom

SUBJECT

Approved minutes of the 28th TF-CSIRT meeting
25 September 2009, Tallinn, Estonia

Margrete Raaum	UiO-CERT	Norway
Tarmo Randel	CERT-EE	Estonia
Wayne Routly	DANTE	-
Derek Simpson	BT CERT CC	-
Don Stikvoort	S-CURE	The Netherlands
Erika Stockinger	SITIC	Sweden
Egils Stūrmanis	DDIRV	Latvia
Manuel Subredu	AARNIEC/RoCSIRT	Romania
Harri Sylvander	FUNET CERT	Finland
Varis Teivans	CERT NIC.LV	Latvia
Marco Thorbruegge	ENISA	-
Edwin Trump	GOVCERT.NL	The Netherlands
Koen Van Impe	BELNET CERT	Belgium
JP Velders	SURFcert	The Netherlands
Simona Venuti	GARR-CERT	Italy
Torsten Voss	DFN-CERT	Germany
Jan Vykopal	CSIRT-MU	Czech Republic
Stefan Winter	RESTENA	Luxembourg
Wilfried Wöber	ACOnet IRT	Austria

Apologies were received from:

Javier Berciano	INTECO-CERT	Spain
Gorazd Božič	SI-CERT (ARNES)	Slovenia
Jorge Chinaea Lopez	INTECO-CERT	Spain
Ralf Dörrie	Telekom-CERT	Germany
Carlos Fragoso Mariscal	CESICAT	Spain
Sergey Linde	RU-CERT	Russia
Stelios Maistros	GRNET-CERT	Greece
Chelo Malagón	IRIS-CERT (RedIRIS)	Spain
Milda Mimiene	LITNET CERT	Lithuania
Jacques Schuurman	SURFcert	The Netherlands
Pascal Steichen	CIRCL	Luxembourg
Thomas Stridh	SUNET CERT	Sweden
David Tabatadze	GRENA/CERT-GE	Georgia
Alexander Talos-Zen	ACOnet CERT	Austria