



SUBJECT

Approved minutes of the 27th TF-CSIRT meeting
19 May 2009, León, Spain

Page 1/7

27th TF-CSIRT meeting

19 May 2009
INTECO, León, Spain

Please note that a seminar was held the previous day. The presentations can be found at <http://www.terena.org/activities/tf-csirt/meeting27/>

1. Approval of Minutes

The minutes of the last meeting held on 19 January 2009 were approved.

2. Actions from last meeting

- 26.1 Lionel Ferette to investigate how to establish liaison with ISO 27035 drafting process.
Done, but a formal letter needs to be drafted and discussed by the ISO Working Group.
- 26.2 Lionel Ferette to speak to Wilfried Wöber about organising tutorial on IRT objects at a future TF-CSIRT meeting.
Done, the tutorial will be held at the next meeting.
- 26.3 Lionel Ferette to start discussion on the mailing list about potential drill exercises.
Done.
- 26.4 Lionel Ferette to start discussion on the mailing list about which incident handling tools to evaluate.
Done, but there had been little feedback so far.
- 24.2 Marco Thorbrügge to present new proposal for CHIHT at the 25th TF-CSIRT meeting.
Done, the proposal was presented during the current meeting.

3. CERT.PT Presentation

Lino Santos gave a presentation about CERT.PT (see <http://www.terena.org/activities/tf-csirt/meeting27/santos-cert-pt.pdf>). This is operated by the Portuguese National Foundation for Scientific Computing (FCCN), which manages the Portuguese NREN, the .pt ccTLD registry, and the Portuguese Internet Exchange. It is responsible for more than 100 higher education and research institutes, 8,000 public schools, and a number of other organizations.

The goals of CERT.PT are to gather and disseminate information about incidents, vulnerabilities, and malicious activities, and provide technical support in resolving these to uses within its constituency. It also raises awareness of security issues, advises on best practice, and promotes the creation of new CSIRTs in Portugal.

CERT.PT has four staff members, and is currently recruiting a fifth. Its constituency is the

IP address blocks issued by the RIPE NCC to FCCN, which includes the NREN, schools network, and the FCCN corporate network. It has relationships with the Portuguese criminal investigation body, armed forces, and other security agencies, and provides specialised training to these organizations. Other activities include participation in the Portuguese Emergency Preparedness Council (CNPCE), and representation on the ENISA Management Board.

Marco Thorbrügge asked whether the CNPCE is running any national exercises? Lino replied that he wasn't aware of them doing this, but they did participate in wider NATO exercises.

Lionel Ferette asked how critical infrastructure was identified. Lino replied they just sat down and drew up a list for FCCN, but questionnaires were sent to other sectors. A publication about this was available.

4. BELNET CERT Presentation

Lionel Ferette gave a presentation about BELNET CERT (see <http://www.terena.org/activities/tf-csirt/meeting27/ferette-belnet-cert.pdf>). This is the CSIRT of the Belgian research and education network, but also covers the Belgian Federal Government and the Belgian National Internet Exchange (BNIX). It was established in 2004 in response to user concerns, as BELNET was at the time one of the few NRENs without a CSIRT.

At the present time, the CSIRT has 2.5 FTEs, and offers incident and vulnerability handling, alerting and warning, and building awareness of security issues. In the five years of operation, they had seen an overall increase in incidents, although those within BELNET had remained relatively static over the past three years. Equally the number of security advisories issued had fallen, perhaps reflecting the success of the CSIRT.

Nevertheless, Belgium still remained a black spot within Europe as it did not have any governmental or military CSIRTs, far less a national coordinating body. These competencies fell within the remit of the telecom regulator, but they had been slow on the uptake in this respect. As a result, BELNET CERT had effectively become the de-facto national CSIRT.

As a result, BELNET had recently been asked to make a proposal for a national CSIRT (CERT.be). The contract still had to be formally agreed, but envisaged a project that funded more effort, with services rolled-out to government agencies, telecoms operators and the public over the next four years. This would involve some recruitment challenges, and the relationship with telecoms regulator needed to be clarified, but it was a positive reflection on BELNET CERT's stature within the Belgian networking community.

Marco Thorbrügge asked whether BELNET CERT had any national drill exercises planned. Lionel replied they didn't have any plans at the present time.

5. Common Browser Hijacking Techniques

David Barroso gave a presentation about common techniques used to hijack web browsers (see <http://www.terena.org/activities/tf-csirt/meeting27/barroso-hijacking.pdf>). This is where the settings of web browsers are modified by malicious code, often for the purposes of collecting user information or redirecting users to fake websites, and frequently targeted at users of banking services. In certain circumstances, the operating system is disabled after the code has run, making analysis of the hijacking and tracing of the perpetrators more difficult.

Browser hijacking is frequently used in fraud schemes, and targets brands around the world. At the present time, only Windows users appear to be affected, but users should be suspicious if their browser starts asking for too much information. Even more so if their computer stops working afterwards.

Lionel Ferette asked whether the analysis was undertaken by S21sec's own researchers. David replied that the malicious code had been evaluated by themselves, but had come from external sources.

6. Incident Handling and Privacy

Andrew Cormack mentioned that at previous TRANSITS courses, the issue of how CSIRTs should act in accordance with the law had been raised. This was unclear as national laws were generally not explicit with respect to sensitive information collected and distributed in pursuit of incident handling, and court cases provided contradictory interpretations. It may be that there also needs to be a distinction made between information collected deliberately, and that which was found accidentally.

In light of this, perhaps CSIRTs should set their own expectations and produce their own industry best practices. Many laws already refer to "industry good practice" as a benchmark, and this might also help lawmakers to avoid laws that conflict with the needs of CSIRTs.

Andrew said he was currently putting together some ideas, and hoped to write-up some draft best practice during the summer. He would therefore welcome input on this.

7. Proposed Liaison with Grid Security

Serge Droz outlined some ideas for liaising with the Grid Security Group (see <http://www.terena.org/activities/tf-csirt/meeting27/droz-grid-sec.pdf>). This had been mentioned at the previous meeting in Riga, and there had subsequently been some discussions between NREN-based CSIRTs and the GRID-SEC activity.

It was clear that Grid sites must collaborate with their own site security operatives in the first instance, and should therefore be integrated into existing CSIRT structures. However, a higher level collaboration between NREN and Grid security personnel was desirable, due to the specific requirements of grids.

The Grid community was currently discussing how to handle cross-grid security incidents, and had invited two representatives from NREN-based CSIRTs to join the Grid Security Group (GRID-SEC). It was therefore proposed that Serge Droz (SWITCH-CERT) and Torsten Voss (DFN-CERT) should be the participants.

There followed a short discussion on this issue, and it was agreed that Serge and Torsten should follow these activities and report back to TF-CSIRT on a periodic basis.

8. GN3 SA3-T4 Security Activities

Wayne Routly gave a presentation on the security activities in the recently started GN3 project (see <http://www.terena.org/activities/tf-csirt/meeting27/routly-gn3-sa2t4.pdf>). This was Task 4 within Service Activity 2, which aimed to deliver security expertise to GN3 participants through deployment of an on-demand consultancy service, whilst

defining and rolling-out appropriate procedures and tools for provisioning multi-domain security.

Lionel Ferette asked about how much time each NREN planned to dedicate to this task. Wayne replied that 14 NRENS were involved, and the total effort was 5.2 FTEs. The bulk of the effort would be provided by DANTE.

9. Anomaly Tool Implementation in GÉANT

Wayne Routly provided an update on the anomaly tool testing activity within the GN2 project (<http://www.terena.org/activities/tf-csirt/meeting27/routly-anomaly-tools.pdf>). Three commercial anomaly detection tools had been tested in the GÉANT network over a two-week period, and the results analysed using nfsen and a custom database.

The tests revealed that Guavus NetReflex was most successful at detecting anomalies. Utilised 1/1000 sampling, and later 1/100 sampling, this picked-up an average of 26 anomalies per day, with just 21% of false positives. The main strengths were in the areas of port scanning and denial-of-service attacks, and identifying the origin of such attacks.

Following the tests, DANTE were now working with the NRENS to rollout a production implementation of NetReflex.

10. Update on CHIHT

Marco Thorbrügge presented the new CHIHT website that had been developed at ENISA (<http://www.terena.org/activities/tf-csirt/meeting27/thorbruegge-chiht.pdf>). This was a proposed collection of tools and guidelines that were useful to incident handling teams, and was intended as a follow-up to the original CHIHT website that was no longer being maintained. However, active involvement from CSIRTs was needed to help update the listings, as they should only include tools that were actively used, rather than those promoted by sales people.

Alexander Talos-Zens volunteered to help Marco update the listings, and they would report back at the next meeting.

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

11. ENISA Exercise Material

Marco Thorbrügge gave an overview of the CSIRT exercise material produced by ENISA (see <http://www.terena.org/activities/tf-csirt/meeting27/thorbruegge-csirt-exercises.pdf>). This came in both a student and teacher's version, and was based on real world examples of security incidents.

The main priority in 2009 was to add case studies, as well as undertake a usability assessment of the current material. Beyond that, it was to provide information on how to establish CSIRT services, and to specify good practice in the provision of CSIRT services.

Two pilot exercise sessions were planned in June. One would be held on 3 June 2009 in conjunction with the CLOSER Coordination Meeting (which was mainly for CSIRTs from the former Soviet Union) in Chisinau, Moldova, and would focus on large-scale incident handling. The other would be held on 30 June 2009 during the FIRST Conference in Kyoto, Japan, and would focus on network forensics.

Chelo Malagón asked about the relationship between the ENISA exercise material and the TRANSITS material. Marco replied there currently wasn't any, but he said there were potential synergies. This could be discussed further at the next TF-CSIRT meetings, after feedback had been received from the initial exercise sessions.

12. TRANSITS Update

Don Stikvoort provided an update on the last TRANSITS training course that had been organised in Dublin, and on future plans (see <http://www.terena.org/activities/tf-csirt/meeting27/stikvoort-transits.pdf>).

The next TRANSITS course would be held in November 2009, although the venue still needed to be confirmed. Further events were planned for Spring and Autumn 2010, and hosts/sponsors were still being sought for these. There were also plans to organise a 'training-the-trainers' type workshop around the September TF-CSIRT in Tallinn.

13. Progressing TF-CSIRT work items

Lionel Ferette reviewed the status of the TF-CSIRT work items that had been added to the Terms of Reference (see <http://www.terena.org/activities/tf-csirt/meeting27/ferette-work-items.pdf>).

There had only been limited feedback on the 'Evaluation of New Tools' item, although this might be linked with the CHIHT activity. There was some idea of organising a workshop to review some of the more complex tools, but given the apparently limited interest, a decision on this should be deferred until the next meeting.

With respect to the drill exercises, there had been much more discussion about this. There were a number of national initiatives being planned within Europe, and there was also provision for these within the GN3 SA2/T4 activity. The Grid community already undertook drills, so this was something that should be considered in more detail. However, it was important to define what should be tested, and what the emphasis should be on.

Lionel Ferette said he would consider this matter in more depth (in consultation with Marco Thorbrügge), and circulate some ideas on the mailing list.

Action 27.2 - Lionel Ferette to circulate some ideas about drill exercises on the mailing list.

14. Date of next meeting

The next meeting will be held on 24-25 September 2009 in Tallinn, Estonia (hosted by CERT-EE).

Toomas Lepik gave a short presentation about the potential venues in Tallinn (see <http://www.terena.org/activities/tf-csirt/meeting27/lepik-tallinn.pdf>), and the unanimous preference of those present was to locate the meeting in the National Library.

The provisional dates for the following meeting are 18-20 January 2010, to be held in Hamburg, Germany (hosted by DFN-CERT).

Open Actions

- 27.1 Marco Thorbrügge and Alexander Talos-Zens to update new CHIHT website.
- 27.2 Lionel Ferette to circulate some ideas about drill exercises on the mailing list.

Participants

<i>Name</i>	<i>Organisation</i>	<i>Country</i>
Shehzad Ahmed	DK-CERT (UNI-C)	Denmark
Mateo Araque	CCN-CERT	Spain
Jimmy Arvidsson	TeliaSonera CERT	Sweden
David Barroso	S21sec	Spain
Javier Berciano	INTECO-CERT	Spain
Wim Biemolt	SURFcert	The Netherlands
Vladimir Bodor	TS-CERT (TeliaSonera)	Sweden
Lasse Trolle Borup	DK-CERT (UNI-C)	Denmark
Jorge Chinaea López	INTECO-CERT	Spain
Andrew Cormack	JANET(UK)	United Kingdom
Michelle Danho	CERT-RENATER	France
James Davis	JANET CSIRT	United Kingdom
Serge Droz	SWITCH-CERT	Switzerland
Andrea Dufkova	ENISA	-
Lionel Ferette (Chair)	BELNET CERT	Belgium
Luis Fernandez	INTECO	Spain
Cyril Gayet	CERTA	France
Stefan Grinneby	SITIC/GOVCERT.SE	Sweden
Peter Haag	SWITCH-CERT	Switzerland
Lourdes Herrero Gil	CSIRT-CV	Spain
Przemek Jaroszewski	CERT Polska (NASK)	Poland
Nino Jogun	CARNet	Croatia
Urpo Kaila	Funet CERT	Finland
L. Aaron Kaplan	CERT.at (NIC.at)	Austria
Daniel Kouril	CESNET	Czech Republic
Susanne Kriszta	IT Security & AConet	Austria
Andrea Kropacova	CESNET	Czech Republic
Huw Langford	BT	United Kingdom
Toomas Lepik	CERT Estonia	Estonia
Antonio Liu	PRESECURE	Germany
Stelios Maistros	GRNET	Greece
Chelo Malagón	IRIS-CERT (RedIRIS)	Spain
Oscar Marin	S21sec	Spain
Manel Medina	esCERT-UPC	Spain
Kevin Meynell (Secretary)	TERENA	-
Francisco Monserrat	RedIRIS	Spain
Carlos Montes Senra	INTECO	Spain
Javier Morant	CSIRT-CV	Spain
Robert Morgan	JANET CSIRT	United Kingdom
Kresimir Neseik	CARNet	Croatia
Thomas Nguyen Van	Jumper Consulting	Ireland
Niclas Olsson	TeliaSonera	Sweden
Marcos Orallo	INTECO	Spain
Timo Porjamo	Funet CERT	Finland
Allan Lynge Rasmussen	DK-CERT (UNI-C)	Denmark
Wayne Routly	DANTE	-

SUBJECTApproved minutes of the 27th TF-CSIRT meeting
19 May 2009, León, Spain

Lino Santos	CERT.PT	Portugal
Marc Stiefer	RESTENA-CSIRT	Luxembourg
Don Stikvoort	S-CURE	The Netherlands
Egils Sturmanis	DDIRV	Latvia
Alexander Talos-Zens	ACOnet CERT	Austria
Marco Thorbruegge	ENISA	-
Marius Urkis	LITNET CERT	Lithuania
Christian Van Heurck	BELNET CERT	Belgium
Anto Veldre	CERT-EE	Estonia
Marc Vilanova	e-la Caixa CSIRT	Spain
Torsten Voss	DFN-CERT	Germany

Apologies were received from:

Gorazd Božič	SI-CERT (ARNES)	Slovenia
Roberto Cecchini	GARR	Italy
Mikhail Ganev	RU-CERT	Russia
Kauto Huopio	CERT-FI (FICORA)	Finland
Baiba Kaskina	CERT NIC.LV	Latvia
Sergey Linde	RU-CERT	Russia
Maciej Milostan	PSNC/PIONIER CERT	Poland
Andre Oosterwijk	GOVCERT.NL	The Netherlands
Carol Overes	GOVCERT.NL	The Netherlands
Margrete Raaum	UiO-CERT	Norway
Jacques Schuurman	SURFcert	The Netherlands
Derek Simpson	BT	United Kingdom
Thomas Stridh	SUNET CERT	Sweden
Wilfried Wöber	ACOnet IRT	Austria