

Approved Minutes of the 24th TF-CSIRT Meeting 14 May 2008 – Oslo, Norway

Please note that a seminar was held the previous day. The presentations can be found at <http://www.terena.org/activities/tf-csirt/meeting24/>

1. Approval of Minutes

The minutes of the last meeting held on 28 January 2008 were approved.

2. Actions from last meeting

- 23.1 All to think about the type of activities that TF-CSIRT should work on.
- Done. The new Terms of Reference were discussed later in the meeting.

- 22.2 Jacques Schuurman to check with AuCERT (and perhaps JPCERT) who was already involved in the out-of-band communications project and what would be required from potential volunteer European teams.
- Ongoing. Jacques was not present at the meeting.

3. TF-CSIRT Delegation to Russia

Gorazd Božič reported that the proposed TF-CSIRT meeting in Russia unfortunately had to be dropped for logistical reasons. However, a TF-CSIRT delegation (led by himself) would instead visit Moscow in early-October to discuss CSIRT activities with the various stakeholders.

4. UiO CERT Presentation

Margrete Raaum gave a presentation about the UiO CERT (see <http://www.terena.org/activities/tf-csirt/meeting24/raaum-uio-cert.pdf>). This covers the University of Oslo and cooperating partners/groups, and is comprised of 10 members representing different aspects of the organisation.

UiO mainly deals with vulnerability watch, intrusion detection, and other incident handling and coordination activities. However, it also disseminates information about security issues in the form of talks, articles, and campaigns. An important role is coordinating with the operational side of the university networking services, to ensure that all team members are up-to-date with the issues, and to ensure that incidents are handled properly when they occur.

On a wider scale, UiO CERT closely cooperates with Uninett CERT (as Uninett provides Internet services to the University of Oslo), and with NorCERT (the Norwegian Government CERT) where appropriate. Usually though, they directly

contact other security groups as necessary, and to this end they are applying for FIRST membership.

5. UNINETT CERT Presentation

Per Arne Enstad gave a presentation about UNINETT CERT (see <http://www.terena.org/activities/tf-csirt/meeting24/enstad-uninett-cert.pdf>). UNINETT is the Norwegian NREN that serves more than 75 institutions and approximately 400,000 end-users.

The UNINETT CERT was established in 1995 and covers all customers within the UNINETT address space. It is a virtual team comprised of 4 persons working in the NOC, who take it in turns to handle incidents. They have been a member of FIRST since 2000, and have been TI Accredited since 2001.

Most of the activities focus on incident prevention and handling, and whilst much of this takes the form of coordination, they are still a number of hands-on cases to deal with. As of 2008, the team dealt with around 5,000 incidents per year.

Their current development work was focused on extending the RTIR software, undertaking passive monitoring, developing flow visualisation tools, and looking at ways to improve anomaly detection. They were also implementing the Child Abuse Anti-Distribution Filter.

6. NorCERT Presentation

Einar Oftedal gave a presentation about NorCERT. This was part of the Norwegian National Security Authority (NSM), and is responsible for coordinating responses against attacks on vital IT infrastructure in the country. It also gathers information related to security incidents, and identifies vulnerabilities in important IT systems. Another role is to act as Norway's point of contact for similar organisations abroad.

7. CERT NIC.LV Presentation

Kristians Melinš gave a presentation about CERT NIC.LV (see <http://www.terena.org/activities/tf-csirt/meeting24/melins-cert-niclv.pdf>). This was formerly known as LATNET CERT, but after the re-organisation that had seen LATNET becoming a fully commercial ISP, the academic services became the responsibility of a renamed organisation called SigmaNet. As a result, the CERT was now under the umbrella of NIC.LV that ran the Latvian ccTLD registry (.lv), which was itself part of the Institute of Mathematics and Computer Science at the University of Latvia.

The constituency of CERT NIC.LV was the SigmaNet and MIL.LV customers, as well as any other Latvian groups willing to cooperate. The team had applied for FIRST membership and was currently a candidate for TI Accreditation.

CERT NIC.LV was comprised of a team leader, three technical experts, a legal expert, and a communications manager. Other personnel could also be called upon

from NIC.LV and SigmaNet as necessary. The team dealt with around 15-20 incidents per day; 80% of which were spam reports, with the remainder largely concerned with port scanning, phishing, botnets and copyright infringements.

The main plans for the future involved the extension of CERT services in Latvia through the LV-CERT initiative. This aimed to foster and strengthen cooperation with other CERTs from other agencies, through exchange of contacts and experiences, as well as improved incident coordination. However, NIC.LV was also planning to set-up a number of network sensors and honeypots to improve its monitoring capabilities.

8. OIC-CERT Update

Kevin Meynell gave an overview of the OIC-CERT Task Force meeting he had attended on 1-2 April in Tunis, Tunisia (see <http://www.terena.org/activities/tf-csirt/meeting24/meynell-oic-cert.pdf>). This had been established under the auspices of the Organisation of the Islamic Conference (OIC), an international organisation of 57 countries, with funding coming from the Islamic Development Bank.

The OIC-CERT Task Force was formed in 2005 with the aim of improving cooperation between existing CERTs in its constituency, and promoting the establishment of CERTs in countries without them. At the present time, it appeared to be primarily targeted at North Africa and the Middle East, although there was active involvement from MyCERT (Malaysia). The group met at least once a year, although was mostly concerned with information sharing and establishing contacts at this stage.

The meeting in Tunis involved four established CERTs, namely CERT-TCC (Tunisia), Cybersecurity/MyCERT (Malaysia), TR-CERT (Turkey) and CERT-SA (Saudi Arabia). There were also representatives from other regulatory and security-related organisations in Libya, Pakistan, Morocco and Nigeria that were in the process of establishing CERT-type activities.

9. APCERT Update

Megat Muazzam provided an update on APCERT (see <http://www.terena.org/activities/tf-csirt/meeting24/muazzam-apcert.pdf>), which had recently met on 10-12 March 2008 in Hong Kong. The group now comprised 21 teams from 15 countries and territories, and had an active programme of collaborative activities and assistance to new teams.

Perhaps the most significant activity was the APCERT Drill Exercise held in November 2007 to prepare for potential cyberattacks related to the Beijing Olympics (which was also covered in more detail during the TF-CSIRT seminar). This was used to reinforce the communication and collaboration between APCERT teams, and would be repeated towards the end of 2008.

APCERT also continued to support the development of new teams in the Asia-Pacific region, including an initiative to develop CERT capabilities in the Pacific Islands. In

addition, coordination meetings were organised with other regions at APEC TEL 36 in Chile, and with the Organisation of American States (OAS) in the United States.

10. RIPE Database Activities

Wilfried Wöber provided an update on the RIPE database (see <http://www.terena.org/activities/tf-csirt/meeting24/woeber-ripedb.pdf>).

IRT deployment was growing, albeit at a slower rate than new address space was being distributed. In addition, the Database Policy Task Force had recommended changes to the RIPE Database Terms and Conditions and Acceptable Use Policy, in order to better define expected behaviour and access limits. This would include a documented removal procedure for personal data, although this should not be construed as a way to anonymise resource holdings.

The Resource Certification programme would also require resource holder information to be digitally signed as a foundation for secure routing mechanisms, and potentially for managed transfers of usage rights when the free pool of IPv4 addresses is depleted. Another proposal was to mandate contractual relationships between resource holders, Local Internet Registries (LIRs) and the RIPE NCC.

Gilles Massen asked whether the other Regional Internet Registries (RIRs) would handle things in a similar fashion. Wilfried replied this would likely be the case.

11. Update on TRANSITS Training Courses

Karel Vietsch reported on TRANSITS training courses. (see <http://www.terena.org/activities/tf-csirt/meeting24/vietsch-transits.pdf>).

The most recent workshop had been held on 24-25 April 2008 in Egmond-aan-Zee, The Netherlands. This was organised by TERENA, with sponsorship from ENISA and GOVCERT.NL.

The dates and venue of the next workshop still had to be determined, but it would probably be held in early-October 2008 near Prague in the Czech Republic. The sponsors would be CESNET and CSIRT.CZ.

12. GN2 Security Activity Update

Christoph Graf provided an update on JRA2, the security activity within the GN2 project (see <http://www.terena.org/activities/tf-csirt/meeting24/graf-jra2.pdf>).

A new version of the NetFlow exporting appliance was now being shipped to project participants by INVEA-TECH (a CESNET spin-off). This supported 1 Gbps, with an upgrade to 10 Gbps expected later. Netreflex, a NetFlow anomaly detection system being developed by GUAVUS, was also expected to be delivered during the summer.

The first toolset training workshop was also held on 18-19 March 2008, which provided training on the use of FlowMon and nfsen/nfdump. A second workshop was planned for late-2008 and would be open to NREN staff and possibly others if there was interest.

JRA2 was also helping GN2 member NRENs to establish CERT functions, with a view to making this a pre-requisite for participating in the proposed GN3 project.

13. Update on ENISA

Marco Thorbrügge provided an update on the European Network and Information Security Agency (see <http://www.terena.org/activities/tf-csirt/meeting24/thorbrugge-enisa.pdf>).

ENISA was attempting to quantify how big a problem security was, and was considering ways of collecting data across the EU. They had a three year programme to help provide a better insight into the types of attacks, the scale of these, why they are undertaken, and what the impact was. This information could then be used to help identify technological and regulatory problems, and reduce the incidence of these.

Another area of study was online social networking which had increased rapidly in recent years, but had many consequences for security and privacy. They were therefore developing a position paper based on the principle that social networking should be considered an identity management system.

ENISA was also developing a number of recommendations for comment. These were along the lines of responsible disclosure by vendors, mandatory fast patching, security certification, and notification of security breaches. In addition, they were considering the feasibility of an EU-wide sharing and alert system.

Karel Vietsch asked about the exercises planned for the European CSIRTs. Marco replied these were currently under discussion, but nothing had yet been decided. The initial pilots were expected to take place sometime during 2009.

14. Date of next meeting

The next meeting will be held on 25-26 September 2008 in Vienna, Austria (hosted by CERT.at).

15. Future of TF-CSIRT

Gorazd Božič said the TF-CSIRT mandate expired on 15 May 2008, 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-chartered the group for a further two years 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 as stated.

It was suggested that reporting on progress at TERENA Networking Conferences was no longer relevant, so reference to this should be deleted from the Terms of Reference. However, presentations at TNCs from TF-CSIRT participants should still be encouraged.

The following was agreed with respect to existing activities:

Meetings and Seminars

It was felt useful to continue to organise the half-day seminars attached to TF-CSIRT meetings.

Trusted Introducer Service

This was a well-established and useful service which should continue to be organised through regular meetings of accredited CSIRTs adjacent to TF-CSIRT meetings.

Security Contact Information for Internet Resources

It was agreed that Wilfried Wöber would reformulate this work item in order to make it more general, but still explicitly mentioning IRT objects.

ACTION 24.1 - Wilfried Wöber to draft new text for Work Item C in the TF-CSIRT Activity List.

Clearing House for Incident Handling Tools

Marco Thorbrügge, the maintainer of the clearing house, had moved to a new position within ENISA and there was currently a lack of manpower to undertake this work. However, this problem should be solved by the end of 2008 and the clearing house activity should therefore remain on the list. A more detailed proposal for the clearing house would be presented at the next TF-CSIRT meeting.

ACTION 24.2 – Marco Thorbrügge to present new proposal for CHIHT at the 25th TF-CSIRT meeting.

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. However, training could be provided to all CSIRT staff rather than just new staff, so the text should be revised to reflect this.

Assistance to the establishment of new CSIRTs

This was considered an important ongoing activity. It was currently largely being undertaken by GN2-JRA2, but would likely be continued in the forthcoming GN3 project.

Collaboration with FIRST and organisations in other world regions

TF-CSIRT had been closely collaborating with FIRST in recent years, and jointly organised an annual Technical Colloquium with them. In addition, TF-CSIRT had established liaisons with APCERT and OIC-CERT.

Request Tracker for Incident Response

The development of the RTIR software to the original requirements of the participating CERTs had now been completed, but there was still scope to extend it further. It was therefore agreed this activity should be continued, and Robert Morgan would be asked draft some text about it.

ACTION 24.3 – Robert Morgan to draft new text for Work Item H in the TF-CSIRT Activity List.

Wim Biemolt said they were still interested in alternative solutions, and asked whether the scope of this activity could include the development of other software. Karel replied that whilst he did not see any problem with developing other solutions if there was sufficient support for this, it should be listed as separate activity.

Collaboration with Information Security Metadata Activities

There was no longer any interest in this activity, so it was agreed it should be dropped.

Collaboration with the Joint Research Activity "Security" in the GN2 project

Many of the JRA2 participants also participated in TF-CSIRT, and provided regular updates about the activity at the meetings. Although JRA2 was due to finish at the end of 2008, there would likely be a successor activity in the GN3 project.

Liaison with the European Commission

It was considered important to continue to liaise with the European Commission as necessary, even though its research grants did not really support CSIRT goals any more. In addition, a number of TF-CSIRT participants were involved with ENISA.

Liaison with E-CoAT

It was unclear whether E-CoAT still existed, or whether it had been superseded by other initiatives. Kevin Meynell was asked to contact Martijn van der Heide (KPN-CERT) in order to determine whether this activity should be continued or not.

ACTION 24.4 – Kevin Meynell to contact Martijn van der Heide about the current status of E-CoAT.

Incident handling and security guidelines for NREN Grids

Whilst it was felt that coordination with the grid community could be strengthened, practical ways of undertaking this needed to be considered. It was therefore decided this activity should be reformulated to state that TF-CSIRT would monitor and liaise with security developments in the Grid community.

The following new activities were suggested:

Drill Exercises

It was felt that holding practical security exercises could be a good way for teams to identify any problems and weaknesses, whilst helping them improve their incident handling techniques. It was agreed this should be added as a new work item, with further discussions as to what practical steps could be undertaken.

Evaluation of new tools

It was suggested there should be a new activity to evaluate and review software tools that could be used for incident handling purposes. At each TF-CSIRT meeting, a new tool would be presented and discussed, whilst a more in-depth teaching session on using the tool may also be organised.

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 the TERENA Technical Committee for approval.

ACTION 24.5 – Kevin Meynell to draft new Terms of Reference for TF-CSIRT.

16. New Chair

Gorazd Božič had previously announced his intention to stand down as TF-CSIRT Chair after this meeting. Lionel Ferette (BELNET CERT) had therefore been approached to replace him, and had agreed to accept the position for a two-year term.

Kauto Huopio (CERT-FI) would remain as Deputy Chair.

Karel Vietsch called for a vote of thanks for Gorazd who had served as the TF-CSIRT Chair for nearly eight years.

Open Actions

24.1 Wilfried Wöber to draft new text for Work Item C in the TF-CSIRT Activity List.

24.2 Marco Thorbrügge to present new proposal for CHIHT at the 25th TF-CSIRT meeting.

24.3 Robert Morgan to draft new text for Work Item H in the TF-CSIRT Activity List.

24.4 Kevin Meynell to contact Martijn van der Heide about the current status of E-CoAT.

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

22.2 Jacques Schuurman to check with AuCERT (and perhaps JPCERT) who was already involved in the out-of-band communications project and what would be required from potential volunteer European teams.

Participants

<i>Name</i>	<i>Organisation</i>	<i>Country</i>
Claudio Allocchio	GARR	Italy
Mateo Araque	CCN-CERT	Spain
Jimmy Arvidsson	TeliaSonera CERT	Sweden
Wim Biemolt	SURFcert	The Netherlands
Gorazd Božič (Chair)	SI-CERT (ARNES)	Slovenia
Anders Bruvik	UiO CERT	Norway
Andreas Bunten	DFN-CERT	Germany
Sergey Bunyakov	RU-CERT	Russia
Jorge Chinaa López	INTECO-CERT	Spain
Andrew Cormack	JANET(UK)	United Kingdom
Michelle Danho	CERT-RENATER	France
Serge Droz	SWITCH-CERT	Switzerland
Øyvind Eilertsen	Uninett CERT	Norway
Per Arne Enstad	Uninett CERT	Norway
Mikhail Ganev	RU-CERT	Russia
Cyril Gayet	CERTA	France
Christoph Graf	SWITCH-CERT	Switzerland
Espen Grøndahl	UiO CERT	Norway
Peter Haag	SWITCH-CERT	Switzerland
Jamie Hughes	GovCertUK	United Kingdom
Przemek Jaroszewski	CERT Polska (NASK)	Poland
Nino Jogun	CARNet CERT	Croatia
Jonas Juknius	CERT-RRT	Lithuania
Urpo Kaila	FUNET CERT	Finland
Aaron Kaplan	NIC.AT	Austria
Andreas Knudsen	NorCERT	Norway
Morten Knutsen	Uninett CERT	Norway
Klaus-Peter Kossakowski	DFN-CERT Services	Germany
Gina Kramer	DANTE	-
Andrea Kropáčová	CESNET	Czech Republic
Torfrid Leek	UiO CERT	Norway
Toomas Lepik	CERT Estonia	Estonia
Ladislav Lhotka	CESNET	Czech Republic
Sergey Linde	RU-CERT	Russia
Antonio Liu	PRESECURE Consulting	Germany
Chelo Malagón	IRIS-CERT (RedIRIS)	Spain
Frøde Mangseth	NorCERT	Norway
Gilles Massen	RESTENA CSIRT	Luxembourg
Branko Mažar	CARNet	Croatia
Arturs Medenis	CERT NIC.LV	Latvia
Kristians Melins	CERT NIC.LV	Latvia
Kevin Meynell (Secretary)	TERENA	-
Milda Mimiene	LITNET CERT	Lithuania
Maurizio Molina	DANTE	-
Barbara Monticini	GARR-CERT	Italy
Megat Muazzam	MyCERT	Malaysia
Sigurd Mytting	UiO CERT	Norway

Einar Oftedal	NorCERT	Norway
André Oosterwijk	GOVCERT.NL	The Netherlands
João Pagaime	CERT.PT (FCCN)	Portugal
Margrete Raaum	UiO CERT	Norway
Tarmo Randel	CERT-EE	Estonia
Robert Schischka	NIC.AT	Austria
Derek Simpson	BT CERT	United Kingdom
Henrik Skantz	SITIC	Sweden
Pascal Steichen	Ministry of the Economy	Luxembourg
Erika Stockinger	SITIC	Sweden
Elisabeth Høidal Strøm	UiO CERT	Norway
Egils Sturmanis	DDRIV	Latvia
Kenneth Svee	UiO CERT	Norway
Rune Sydskjør	Uninett CERT	Norway
Harri Sylvander	FUNET CERT	Finland
Alexander Talos	ACOnet CERT	Austria
Rafal Tarlowski	CERT Polska (NASK)	Poland
Varis Teivans	Sigmanet	Latvia
Marco Thorbrügge	ENISA	-
Marius Urkis	LITNET CERT	Lithuania
Koen Van Impe	BELNET CERT	Belgium
Simona Venuti	GARR-CERT	Italy
Karel Vietsch	TERENA	-
Torbjörn Victorin	SUNet CERT	Sweden
Wilfried Wöber	ACOnet IRT	Austria
Bente Christine Åsgård	UiO CERT	Norway

Apologies were received from:

Till Dörge	PRESECURE Consulting	Germany
Ralf Dörrie	Telekom-CERT	Germany
Robert Morgan	JANET CSIRT	United Kingdom