



SUBJECT

Approved minutes of the 29th TF-CSIRT meeting
25 January 2010, Hamburg, Germany

Page 1/8

29th TF-CSIRT meeting

25 January 2010

Grand Elysee Hotel, Hamburg, Germany

Please note that a seminar was held the following day.

1. Approval of Minutes

The minutes of the last meeting held on 25 September 2009 were approved.

2. Actions from last meeting

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

28.1 Lionel Ferette to ask TERENA whether they can apply to be a ISO 27035 liaison member.
Done, an application was currently being discussed.

3. CZ.NIC and CZ.NIC-CSIRT Presentation

Martin Peterka gave a presentation about CZ.NIC and its associated CSIRT (see <http://www.terena.org/activities/tf-csirt/meeting29/peterka-cznic.pdf>). CZ.NIC is a special interest association founded in 1998 by a number of leading ISPs to operate the Czech (.cz) ccTLD registry. It currently comprises 65 members and 40 employees, and through an MoU with the Czech government is considered a critical part of the state infrastructure. The main activities are to operate the ccTLD and ENUM registries, to develop and support registry software, to train and educate, and to operate a CSIRT.

The CZ.NIC-CSIRT is responsible for incident handling within the AS25192 address space, and with respect to the name servers for .cz and 0.2.4.e164.arpa. They also handle complaints related to phishing and malware associated with .cz domain names, and work in cooperation with CSIRT.CZ on these issues.

From the 1st of January 2010, they also have the legal power to deactivate a domain if it is used in a fashion that endangers computer security. Deactivation can be for up to one month at the decision of CZ.NIC-CSIRT, but further suspensions can be enabled if abuses continue.

CZ.NIC-CSIRT plans to apply for TI accredited status.

Andrew Cormack asked whether there was a published procedure for deciding when to suspend domains, and what happens after they have been suspended. Martin replied there was an internal process that was followed, particularly with respect as to who was informed, but this was not published.

Lionel asked how many domains had been suspended so far. Martin replied none had actually been suspended to date, although domains had been cancelled in the past.

4. CIRCL Presentation

Pascal Steichen have a presentation about CIRCL (see <http://www.terena.org/activities/tf-csirt/meeting29/steichen-circl.pdf>). This was the government CSIRT for Luxembourg, which provided incident handling for government departments, municipalities, and other public organisations. It also supported critical infrastructures in sectors such as banking and ICT that were important to national interests. The team had recently become a member of FIRST, and was now also TI accredited.

CIRCL took a three way approach to security – responding to incidents and distributing alerts and warnings, taking a proactive approach by following trends and circulating advisories, and finally providing security training and consultancy. This included development of the LEWIS project (Luxembourg Early Warning and Information Sharing System) which was based on locating sensors at strategic network points to provide active and passive intrusion detection, as well as honeypot facilities for capturing and analysing malware. This facilitated correlation and exchange of information, which was provided to members of the project in a standardised format.

Another initiative was SMILE (Security Made In Letzebuerg) which was a publicly funded private agency with eight employees that had been established to advise less technically knowledgeable organisations about security. This would start in Spring 2010 and would focus on schools, municipalities, and small/medium enterprises.

5. Delivering services in a user-focused way

Marcus Pattloch gave a presentation about the new DFN-CERT portal that aimed to improve handling of incident warnings and alerts (see <http://www.terena.org/activities/tf-csirt/meeting29/pattloch-dfncert-portal.pdf>). The issue was that the DFN-CERT had seen ever increasing numbers of vulnerabilities over the years, and had been circulating more and more information in an attempt to raise awareness of these. However, not everything was useful to every site, and this had led to information overload that decreased the effectiveness of what was trying to be achieved.

As a result, the DFN-CERT portal (<https://portal.cert.dfn.de/>) aimed to provide information that was only relevant to individual sites, as identified by their site certificates. For example, only advisories related to platforms operated by a particular site, or incident warnings affecting particular networks would be received. In addition, the portal would shortly offer network scanning for IP address ranges in order to show open ports, services being advertised, and potential system vulnerabilities.

The portal was not intended to replace directly replace incident response operators, but to improve distribution of information, identify potential problems in advance, and ensure the right people were aware of issues when they did arise.

Benôit Moreau asked how they knew who was responsible for IP address ranges when a check was requested. Marcus replied that DFN maintained site contact information for all addresses under its authority.

6. ICANN and DNS Security, Stability and Resiliency Activities

Greg Rattray gave a presentation on DNS security issues (see <http://www.terena.org/activities/tf-csirt/meeting29/rattray-dns-security.pdf>). ICANN was ultimately responsible for the DNS which was critical to the entire Internet infrastructure, so need to take

measures to ensure its security and stability. The DNS root servers were an obvious target for direct attacks, but equally the system could be compromised through poorly run or malicious actors.

The measures being taken included support for DNSSEC through the signing of the root zone by mid-2010, and authenticating communication with TLD managers. In addition, vetting had been implemented to ensure new TLD applicants offered stable operations and proper security controls. This included the Attack and Contingency Response Plan (ACRP) being drawn up in conjunction with ISOC and regional ccTLD associations. In the longer term, there were proposals to disallow wildcards and glue records, and undertake more checks on Whois information.

Another initiative was to provide specific DNS training to CSIRTs, and initial outreach efforts had begun at FIRST 2009 in Kyoto. This would continue at a joint ICANN-FIRST Cybersecurity Workshop that would be held on 5-8 March 2010 in Nairobi, and at FIRST 2010 on 13-18 June 2010 in Miami.

In addition, ICANN proposed to establish a Global DNS CERT to coordinate responses to DNS incidents. This would involve important stakeholders in the DNS community, and would operate in conjunction with the broader cybersecurity community.

Kauto Huopio asked whether ICANN had considered that many national CSIRTs were operated by the same organisation (and in some cases the same people) as the ccTLD registry, and were already involved in DNS activities. Greg replied they were aware of some relationships, but need to investigate this further.

7. Grid Security Developments

Daniel Kouřil gave a presentation on the latest Grid Security developments (see <http://www.terena.org/activities/tf-csirt/meeting29/kouril-gridsec.pdf>). The EGEE project currently coordinated many National Grid Initiatives (NGIs) that involved around 250 sites, 150,000 CPUs and 30 PB of storage, processing thousands of jobs per day. However, EGEE was due to finish in April 2010, and would be replaced by the longer-term European Grid Initiative (EGI).

Operational security was currently coordinated by EGEE CSIRT, in cooperation with individual sites and virtual organisations that remained responsible for their own resources, but signed up to binding policies. NGIs were now establishing their own CSIRTs in response to several incidents that had been experienced, but such incidents were not confined to Grid systems and closer collaboration with NREN CSIRTs was welcomed. With the transition to EGI, utilising the skills and experiences of existing CSIRTs could save a lot of effort.

Marcus Pattloch asked why the Grid community was establishing its own CSIRTs and didn't simply use existing CSIRTs. Daniel replied one problem was that existing CSIRTs were usually nationally-based, whereas Grids often spanned a number of countries. In addition, Grid incidents often had different characteristics, and whilst the processes to handle them were similar, some familiarity with the Grid community was needed.

8. TRANSITS update

Don Stikvoort provided a short update on the latest TRANSITS developments (see <http://www.terena.org/activities/tf-csirt/meeting29/stikvoort-transits.pdf>). The next workshop would be held on 4-5 March 2010 in Uppsala, Sweden, with the deadline for

applications being 8 February 2010. The cost was EUR 500 for participants from not-for-profit organisations, and EUR 750 for participants from commercial companies which included all accommodation and meals.

There were also plans for a TRANSITS-2 workshop later in the year. This would be focused on more advanced topics such as network monitoring and forensics.

9. Trusted Introducer overview

As there were many new people at the meeting, Don Stikvoort gave a short overview of the Trusted Introducer service (see <http://www.terena.org/activities/tf-csirt/meeting29/stikvoort-ti.pdf>). This accredited CSIRTs in Europe and surrounding regions according to established criteria, and maintained a secure database of contacts that were actively checked and updated. It also provided a trusted forum to meet and exchange information, provided supporting services such as out-of-band communication, and worked on issues such as data exchange standardisation and certification.

The first stage towards accreditation was to have one's CSIRT listed. This was free-of-charge and required the support of two accredited teams. A CSIRT could subsequently apply for accreditation, which provided access to the TI services supported by the TI team. More information was available at <http://www.trusted-introducer.org/>

10. GN3 Security Activities

Maurizio Molina and Baiba Kaskina gave a presentation on the latest developments in the GN3-SA2/T4 security activities, in particular the survey on multi-domain anomaly handling in NRENs (see <http://www.terena.org/activities/tf-csirt/meeting29/kaskina-qn3-security.pdf>).

The aim of the survey was to obtain a detailed picture on how multi-domain anomalies were handled. A series of 36 questions were asked about anomaly classification, the tools used for detection, and workflows and procedures. 38 NRENs were contacted and 22 responses were received.

An average of 26.8 anomalies were seen per day, with malicious code, abusive content, fraud, intrusion detection and information gathering being the most common. The most popular method for detecting and combating these were NetFlow, log analysis and intrusion detection systems. Other methods included honeypots, DNS blackholing, and darkspace detectors.

Prioritisation was usually based on the source of the anomalies, with preference given to one's own network. However, the number of hosts originated and targeted, and whether events were repeated, also influenced these decisions. The methods used to identify the responsible people on other networks/sites, often came down to personal contacts or through CSIRT contact databases. Failing that Whois or even Google were be resorted to.

Baiba thanked those who had participated in the survey, and mentioned there was still time for other NRENs to be involved which would help provide a more comprehensive picture. In addition, there was an idea to extend the survey to other CSIRT teams from outside the NREN community.

11. Date of next meeting

The next meeting will be held on 20-21 May 2010 in Heraklion, Greece (hosted by FORTH CERT).

Lionel Ferette pointed out that as FORTH was located a few kilometres outside of Heraklion, it would be necessary to arrange transportation to take participants from the hotels to the meeting venue. It was therefore important that the local organisers had accurate numbers in good time, and for this reason registration would close two weeks in advance.

12. Any other business

Marco Thorbruegge mentioned that the list of incident handling tools on the CHIHT website had recently been updated following the ACOnet survey. This could be found at <http://www.enisa.europa.eu/act/cert/support/chiht/>

Open Actions

There are currently no open actions.

SUBJECT

Approved minutes of the 29th TF-CSIRT meeting
25 January 2010, Hamburg, Germany

Participants

<i>Name</i>	<i>Organisation</i>	<i>Country</i>
Hillar Aareleid	CERT-EE	Estonia
Bente Christian Åsgård	UiO-CERT	Norway
Jordi Aguila	La Caixa	Spain
Shehzad Ahmed	DK-CERT (UNI-C)	Denmark
Antti Alinen	Ericsson	Finland
Jimmy Arvidsson	TeliaSonera CERT	Sweden
Ioannis Askoxylakis	FORTH CERT	Greece
Javier Berciano	INTECO-CERT	Spain
Wim Biemolt	SURFcert	The Netherlands
Vladimir Bodor	TS-CERT (TeliaSonera)	Sweden
Philippe Bourgeois	CERT-IST	France
Gorazd Bozic	SI-CERT	Slovenia
Matej Breznik	SI-CERT	Slovenia
Martin Camilleri	mtCERT	Malta
Robert Cecchini	GARR-CERT	Italy
Matthew Cook	EMMAN/Loughborough Univ.	United Kingdom
Jorge Chinaea Lopez	INTECO-CERT	Spain
Ian Cook	Team Cymru	United Kingdom
Andrew Cormack	JANET(UK)	United Kingdom
Frederico Costa	RNP	Brazil
Goran Culjak	CERT ZSIS	Croatia
Michelle Danho	CERT-RENATER	France
Jerome Devigne	BELNET CERT	Belgium
Till Dörge	PRE-CERT/PRESENCE	Germany
Ralf Dörrie	Deutsche Telekom	Germany
Serge Droz	SWITCH-CERT	Switzerland
Jussi Eronen	CERT-FI	Finland
Lionel Ferette (Chair)	BELNET CERT	Belgium
Carlos Fuentes	IRIS CERT	Spain
Sven Gabriel	NIKHEF	The Netherlands
Chris Gibson	citi	United Kingdom
Michael Groening	DFN-CERT	Germany
Peter Haag	SWITCH-CERT	Switzerland
Tilmann Haak	DFN-CERT	Germany
Sven Hallberg	PRESENSE	Germany
Anders Hardangen	NorCERT	Norway
Nicolas Holin	CERTA	France
Kauto Huopio	FICORA/CERT-FI	Finland
Yurie Ito	JPCERT/CC	Japan
Pawel Jacewicz	CERT Polska (NASK)	Poland
Thorben Jändling	SWITCH	Switzerland
Xander Jansen	SURFcert	The Netherlands
Nino Jogun	CARNet	Croatia
Baiba Kaskina	SigmaNet	Latvia
Piotr Kijewski	CERT Polska (NASK)	Poland
Georgia Killcrece	CERT/CC	United States
Mark Koek	Fox-IT	The Netherlands
Jan Kohlrausch	DFN-CERT	Germany
József Komli	CERT-Hungary	Hungary
Klaus-Peter Kossakowski	DFN-CERT	Germany
Daniel Kouril	CESNET CERT	Czech Republic
Thorsten Kraft	1&1 Internet	Germany
Andrea Kropacova	CESNET	Czech Republic

SUBJECT

Approved minutes of the 29th TF-CSIRT meeting
25 January 2010, Hamburg, Germany

Morten Linneman	DK-CERT (UNI-C)	Denmark
Antonio Liu	PRESECURE	Germany
Stefan Lueders	CERN	-
Scott McIntyre	KPN-CERT	The Netherlands
Stelios Maistros	GRNET-CERT	Greece
Mirosław Maj	CERT Polska (NASK)	Poland
Egil Mannerheim	Swedbank	Sweden
Detlev Matthies	DFN-CERT	Germany
Girts Mažonis	DDIRV	Latvia
Arturs Medenis	CERT NIC.LV	Latvia
Stefan Metzger	DFN-CERT/LRZ	Germany
Kevin Meynell (Secretary)	TERENA	-
Maurizio Molina	DANTE	-
Klaus Möller	DFN-CERT	Germany
Francisco Monserrat	RedIRIS	Spain
Benôit Moreau	CERTA	France
Leif Nixon	National Supercomputer Centre	Sweden
Tomasz Nowocien	PIONIER-CERT/PSNC	Poland
Carol Overes	GOVCERT.NL	The Netherlands
Marcus Pattloch	DFN-CERT	Germany
Darko Perhoc	CARNET National CERT	Croatia
Martin Peterka	CZ.NIC	Czech Republic
Jacomo Piccolini	ESR/RNP	Brazil
Timo Porjamo	FUNET CERT	Finland
Christian Proschinger	Raiffeissen Informatik CERT	Austria
Tomislav Protega	CARNet National CERT	Croatia
Peter Quick	Deutsche Telekom	Germany
Margrete Raaum	UiO-CERT	Norway
Greg Rattray	ICANN	-
Wayne Routly	DANTE	-
Jürgen Sander	PRESENSE	Germany
Lino Santos	CERT.PT	Portugal
Shiori Sato	JPCERT/CC	Japan
Timo Schäpe	DFN-CERT	Germany
Robert Schischka	CERT.at	Austria
Jochen Schoenfelder	DFN-CERT	Germany
Jacques Schuurman	SURFcert	The Netherlands
Udo Schweigert	Siemens CERT	Germany
Hadas Shany	Israel CERT	Israel
Derek Simpson	BT CERT CC	United Kingdom
John Snyder	BT CERT CC	United Kingdom
Liliana Solha	RNP	Brazil
Pascal Steichen	CIRCL	Luxembourg
Don Stikvoort	S-CURE	The Netherlands
Dieter Stolte	DFN-CERT	Germany
Joerg Streckfuss	DFN-CERT	Germany
Egils Stūrmanis	DDIRV	Latvia
Yoshi Sugiura	NTT	Japan
Harri Sylvander	FUNET CERT (CSC)	Finland
Balazs Szekeres	CERT-Hungary	Hungary
Alexander Talos-Zens	ACOnet-CERT	Austria
Axel Theilmann	PRESENSE	Germany
Marco Thorbruegge	ENISA	-
Atanai Ticianelli	RNP	Brazil
Bob van der Kamp	GOVCERT.NL	The Netherlands
Jaap van Ginkel	SURFcert/UvA	The Netherlands

SUBJECTApproved minutes of the 29th TF-CSIRT meeting
25 January 2010, Hamburg, Germany

Anto Veldre	CERT-EE	Estonia
Simona Venuti	GARR-CERT	Italy
Dimitra Vitsa	FORTH CERT	Greece
Torsten Voss	DFN-CERT	Germany
Robert Waldner	NIC.AT	Austria
Torbjörn Wictorin	SUNet CERT	Sweden
Adrian Wiedemann	Karlsruhe Institute of Technology	Germany
Wilfried Wöber	ACOnet IRT	Austria
Christian Wojner	NIC.AT	Austria
Thomas Wolf	1&1 Internet	Germany
Yoshio Yamada	National Police Agency	Japan
Tadashi Yamagishi	IPA Japan	Japan
Jyrki Yli-Paavola	TeliaSonera	Finland
Takahiko Yoshida	NTT	Japan

Apologies were received from:

Przemek Jaroszewski	CERT Polska (NASK)	Poland
Chelo Malagón	IRIS-CERT (RedIRIS)	Spain
Manuel Subredu	RoCSIRT (RoEduNet)	Romania
David Tabatadze	CERT-GE (GRENA)	Georgia