Minutes of the 43rd TF-CSIRT Meeting
18th – 19th September 2014
Rome, Italy
This meeting was hosted by Poste Italiane

Table of Contents

1. Welcome and Apologies 2
2. Minutes of Last Meeting and Update of Action List 2
- Minutes 2
- Actions from Previous Meetings 2
3. Trusted Introducer Update, Mirko Wollenberg 2
4. TERENA Update, Nicole Harris 2
5. IPv4 Hijacking – Mirjam Kühne and Ivo Dijkhuis, RIPE 2
6. Scanning for Vulnerabilities: is it Lawful? Andrew Cormack, JANET 3
7. Recent developments of tools to monitor attackers, Daniel Kouril and Jan Vykopal 3
8. Nominations 3
9. Data sets and databases for CSIRTS, Aaron Kaplan 3
10. Security Officer: An NREN Secondee Perspective, Jan Kohlrausch, DANTE 3
11. Project Turris: from realization to findings, Zuzana Duracinska , CSIRT.CZ 4
12. EU Project "Enhancing Cyber Security", Besnik Limaj, LogicPlus 4
13. The National CERT in the framework of the Italian Cyber Security Strategy 4
14. Preparations for the EU presidency in Latvia, Baiba Kaskina, CERT.LV 4
15. NREN & ISP Security Working Group 2014 Review. Wayne Routly, DANTE 4
x. Date of Next Meeting and AOB 5
List of Participants 5

1. Welcome and Apologies

Lionel Ferette welcomed attendees to the meeting. The following attendees sent apologies:

Olivier Caleff	CERT-FR
Serge Droz	SWITCH
Przemek Jaroszewski	CERT Polska/NASK
Frederic Le Bastard	CERT La Poste
Miroslaw Maj	Cybersecurity Foundation / TI team
Gustavo Neves	CERT.PT
Juan Quintanilla	DANTE
Christian Van Heurck	CERT.be / Belnet CERT

2. Minutes of Last Meeting and Update of Action List

- Minutes

The minutes of the meeting have not yet been circulated due to staff absence at the last meeting. Minutes will be circulated shortly.

ACTION20140918-01: NH to circulate the minutes of the 42nd meeting as soon as available.

- Actions from Previous Meetings

There were no open actions from the previous meeting.

3. Trusted Introducer Update, Mirko Wollenberg

Mirko Wollenberg gave an update on the TI service and number of teams that are listed, accredited and certified as well as an update on infrastructure changes.

The presentation slides can be found at: https://www.trusted-introducer.org/misc/20140918_TI-update-public.pdf.

4. TERENA Update, Nicole Harris

Nicole Harris gave attendees a brief overview of the work undertaken by TERENA for the security community and introduced the fee review for Trusted Introducer. The possible fee changes will be discussed with the TF-CSIRT SC and a transparent review announced with the aim to present a more detailed approach at the next TF-CSIRT meeting.

The presentation slides can be found at: http://www.terena.org/activities/tf-csirt/meeting43/tf-csirt-43-nh.pdf.

ACTION20140918-02: TF-CSIRT SC to lead a more detailed discussion on TI fees at the 44th TF-CSIRT meeting.

5. IPv4 Hijacking – Mirjam Kühne and Ivo Dijkhuis, RIPE

Mirjam Kühne gave an update on IPv4 hijacking from a RIPE perspective. Typical hijacks are researched, with hijackers reviewing vulnerable IP addresses, re-registering expired domain names to make email changes look legitimate and copying website with identical pages hosted on (almost) identical domains. Forged documentation is also a significant problem.

RIPE are seeking feedback from the CSIRT community as to how information can be shared concerning such hijacks and hijack prevention.

The presentation slides can be found at: http://www.terena.org/activities/tf-csirt/meeting43/TF-CSIRT43-Kuehne.pdf.

6. Scanning for Vulnerabilities: is it Lawful? Andrew Cormack, JANET

Andrew Cormack gave an update on his research into scanning for vulnerabilities. He started by questioning what law might cover scanning. One current problem is that there is no definition of "access without right" so working out the details of a breach is complex. Access can be defined as anything from any approach being access to access only being if you get inside (equivalent to trespass). UK law says access is "anything that causes a computer to perform any function" (e.g. a response), which is a very broad interpretation.

Within the UK, scanning would be considered access. Intention is not relevant, whether this be honest or dishonest. Andrew recommended that countries review the exact situation for their own environment due to considerable differences in local and case law.

The presentation slides can be found at: http://www.terena.org/activities/tf-csirt/meeting43/Scanning%20for%20Vulnerabilities.pdf.

7. Recent developments of tools to monitor attackers, Daniel Kouril and Jan Vykopal

Daniel Kouril presented the C4e project (Czech CyberCrime Centre for Excellence), which is a project to create a single point of contact in the Czech Republic for investigation of Cyber Crime.
The presentation slides can be found at: http://www.terena.org/activities/tf-csirt/meeting43/kouril.pdf.

8. Nominations

The following nominations were made for the SC in the meeting:

- Baiba Kaskina was the only nomination for chair and was elected without objection.
- Jacques Schuurman (XS4ALL), nominated by Wilfried Woeber (ACOnet-CERT), seconded by Przemek Jaroszewski (CERT.pl).
- Daniel Röthlisberger (SWITCH), nominated by Wim Biemolt (SURFcert), seconded by seconded by Baiba Kaskina (CERT.lv).
- Jan Vykopal (CSIRT-MU), nominated by Baiba Kaskina (CERT.lv), seconded by Andrea Kropacova (CESNET).
- Vladimir Bobor, nominated by Erika Stockinger (CERT-SE), seconded by Kauto Huopio (NCSC-FI).

Following a voting process inline with the TF-CSIRT ToR Daniel (2 years), Jan (1 year), and Vladimir (2 years) were appointed to the TF-CSIRT SC.

Lionel, Jacques and Erika were thanked for all of their work on the TF-CSIRT SC.

9. Data sets and databases for CSIRTS, Aaron Kaplan

Aaron Kaplan gave an over view of a contact database for datasets listing abuse contacts and CERTS worldwide. The tool is available on github and has a simple markdown list of details to edit and submit. No slides were provided for this presentation.

10. Security Officer: An NREN Secondee Perspective, Jan Kohlrausch, DANTE

Jan was a senior incident handler and researcher with DFN-CERT and moved to a secondment at DANTE as an NREN Security Officer. This has included reviewing new problems such as issues with cloud computing, BYOD and mobile devices. The NREN and ISP Security Working Group has recommended that the role of Security Officer become standardised within companies as a separate function from day-to-day CERT operations.

DANTE CSIRT is working towards ISO 27001 certification.

The presentation slides can be found at: http://www.terena.org/activities/tf-csirt/meeting43/Secondee_Rome.pdf.

11. Project Turris: from realization to findings, Zuzana Duracinska , CSIRT.CZ

Zuzana Duracinska gave an overview of project Turris in the Czech Republic. Turris = latin word for tower and is a service helping to protect a user's home network. It has been established as a not for profit research project. It uses an adaptive firewall based on collected data with regular updates from the project.

The presentation slides can be found at: http://www.terena.org/activities/tf-csirt/meeting43/Turris.pdf.

12. EU Project "Enhancing Cyber Security", Besnik Limaj, LogicPlus

Besnik Limaj gave an overview of an EU funded project to enhance cyber security in Moldova, FYROM and Kosovo. This includes supporting the creation of CERTS and standardizing practice.

The presentation slides can be found at: http://www.terena.org/activities/tf-csirt/meeting43/tf-csirt-43-bl.ppsx.

13. The National CERT in the framework of the Italian Cyber Security Strategy

Rita Forsi and Alessandro Paci gave an overview of the work of the National CERT in Italy. The National CERT is a new initiative and in the process of establishing itself in Italy.

14. Preparations for the EU presidency in Latvia, Baiba Kaskina, CERT.LV

Baiba presented the preparations for the EU presidency in Latvia in 2015, starting by identifying the critical resources for the presidency from government through to media channels and identifying the VIP webpages. The CERT identified around 250 web resources and work started in January 2014. Approximately a third of the identified resources have been pen tested. From these, 80% had critical vulnerabilities. The largest concern is DDoS attacks so the CERT is working closely with ISPs to mitigate this risk.

The presentation slides can be found at: http://www.terena.org/activities/tf-csirt/meeting43/TF-CSIRT_Rome.19092014_PUBLIC.pdf.

15. NREN & ISP Security Working Group 2014 Review. Wayne Routly, DANTE

Wayne gave an overview of the NREN and ISP Security Working Group and the focus on work in 2014, which has included NSHaRP infrastructure, nessus, web cameras in PoPs, firewall on demand and the role of the NREN Security Officer.

The presentation slides can be found at: http://www.terena.org/activities/tf-csirt/meeting43/TF-CSIRT_Rome.19092014_PUBLIC.pdf.

16. Protecting Digital Services - The Role of Cyber Security District. Rocco Mammoliti, Poste Italiane and Francesco Buccafurri, University of Regio Calabria.

Poste Italiane gave an update on the work of the company to support security requirements in Italy and the creation of a "Cyber Security" district by the Italian Ministry for University and Research.

The presentation slides can be found at: http://www.terena.org/activities/tf-csirt/meeting43/TF-CSIRT-ProtectingDigitalServices.pdf.

17. Date of Next Meeting and AOB

No further business was identified. Lionel Ferette confirmed that the next meeting will be in Tenerife, 27th-29th January 2015 followed by Poznan, w/b 18th May 2015.

Action Summary

ACTION20140918-01: NH to circulate the minutes of the 42nd meeting as soon as available.
ACTION20140918-02: TF-CSIRT SC to lead a more detailed discussion on TI fees at the 44th TF-CSIRT meeting.

List of Participants

Bente Christine Aasgaard	UiO-CERT
Elena Mena Agresti	Poste Italiane
Shehzad Ahmad	DKCERT (DTU)
Claudio Allocchio	GARR
Mateo Araque	CCN-CERT
Jean-Luc Auboin	EU Council - GSC
Mihai Barbulescu	Agency ARNIEC/RoEduNet
Vladimir Bobor	TS-CERT
Gianluca Bocci	Poste Italiane
Martin Bore	UiO-CERT
Francesco Buccafurri	Università di Reggio Calabria
Emilio Bugli Innocenti	Adetef & CIVIPOL.Conseil
David Byers	LiU IRT
Roberto Cecchini	GARR-CERT
Giantonio Chiarelli	Poste Italiane
Cosmin Ciobanu	ENISA
Alexandru Ciobanu	CERT-EU
Andrew Cormack	Jan
Amy Cox	BT
Ivo Dijkhuis	RIPE NCC
Andrea Dufkova	ENISA
Alexandre Dulaunoy	CIRCL, national CERT of Luxembourg
Zuzana Duracinska	CSIRT.CZ
Lionel Ferette	ENISA
Federico Filipponi	Ministero dello Sviluppo Economico
Rita Forsi	Ministry of Economic Development - National CERT
Sven Gabriel	Nikhef/EGI-CSIRT
Maura Gambassi	MINISTERO DELLO SVILUPPO ECONOMICO
Espen Grøndahl	UiO-CERT
Flavio Guerrieri	ESA
Monica Hargis	Strategy Analytics
Lee Harrigan	Janet CSIRT
Nicole Harris	TERENA

Ulrik Haugen	Linköpings universitet
Kauto Huopio	FICORA/NCSC-FI
Ilir Imeri	RAEPC - Regulatory Authority of Electronic and Postal Communications
Marco Infortuna	Enav SPA
mark johnston	DANTE
Martin Jurcik	CSIRT.SK
L. Aaron Kaplan	CERT.at
Mathias Karlsson	SWITCH
Baiba Kaskina	CERT.LV
Piotr Kijewski	CERT Polska/NASK
Jan Kohlrausch	DANTE
Tunde Kolawole	BT PLC (BT CERT)
Klaus-Peter Kossakowski	PRESECURE Consulting
Daniel Kouril	Masaryk University
Andrea Kropacova	CESNET
Mirjam Kühne	RIPE NCC
Ossi Kuosmanen	CSC/Funet CERT
Sébastien Léonnet	General Secretariat of the Council of the EU
Besnik Limaj	Adetef & CIVIPOL.Conseil
Antonio Liu	The Trusted Introducer Service (DFN-CERT)
Jonny Lundin	NORDUnet
Gints Malkalnietis	CERT.LV
Rocco Mammoliti	Poste Italiane
Dario Marano	NTTDATA
Sandro Mari	Ministry of Economic Development - National CERT
Antonio Merola	Poste Italiane
Francisco Monserrat	RedIRIS
Tomasz Nowocień	Pionier-CERT / PSNC
André Oosterwijk	NCSC-NL
Radim Ostadal	NCSC (cz)
Alessandro Paci	Ministero dello Sviluppo Economico
Sergio Pagnozzi	ESA
Anna Passeggia	MINISTERO DELLO SVILUPPO ECONOMICO
Antonio Piccolo	UNICAL
Tarmo Randel	CERT-EE / EISA
Daniel Roethlisberger	SWITCH
Åsa Roos	CERT-SE
Michelangelo Rosarno	DCS COSENZA
Wayne Routly	DANTE
Jorge Ruão	CSIRT.UPORTO
Luigi Saccà	UNICAL
Tomi Salmi	CSC/Funet CERT
Giampaolo Scafuro	Poste Italiane
Giampaolo Scafuro	Poste Italiane
Dag-Erling Smørgrav	UiO-CERT
Natalia Spinu	CERT-GOV-MD
Erika Stockinger	CERT-SE
Jasmina Stojcheva	AEC - Agency for Electronic Communications
Tamás Szép	GovCERT-Hungary
Alexander Talos-Zens	ACOnet-CERT

Marius Urkis	LITNET CERT
Bob van der Kamp	NCSC-NL
Simona Venuti	GARR-CERT
Andrea Volponi	Poste Italiane
Jan Vykopal	CSIRT-MU
Cynthia Wagner	RESTENA-CSIRT
Dennis Wallberg	NORDUnet
Jean-Paul Weber	Govcert.lu
Wilfried Woeber	ACOnet-CERT
Mirko Wollenberg	TI Team
Alex Zacharis	GRNET-CERT
Martin Zadnik	CESNET