Minutes of the 41st TF-CSIRT Meeting
10th February 2014
Zurich, Switzerland
This meeting was hosted by SWITCH

Table of Contents

1. Welcome and Apologies

Lionel Ferette welcomed attendees to the meeting. No apologies were received for this meeting.

2. Minutes of Last Meeting and Update of Action List

- Minutes

The minutes of the meeting were accepted as an accurate record of the meeting.

- Actions from Previous Meetings

There were no open actions from the previous meeting.

3. Trusted Introducer Update

Klaus Peter Kossakowski gave an overview of the new CERTS that have joined Trusted Introducer since the last meeting. There has been significant growth in commercial and government CERTS, whereas research and education CERTS are plateauing – as should be expected.

UNINETT CERT has now been accepted as a certified CERT and 5 CERTS are now candidates for certification.

Trusted Introducer is now offering information on the public web page in multiple languages. This is based on a fixed template, translated and reviewed by 2 native speakers.

Tomas Lima and Aaron Kaplan are chairing a working group looking at APIs for the Trusted Introducer information and ways to make this information more useful.

4. TRANSITS Update

Don Stikvoort gave an update on progress with TRANSTS training. Don started by recommending the ENISA exercises that are available on the ENISA website as a great starting place for anyone looking for training.

TRANSITS is looking at a more flexible model to allow different formats to be introduced depending on the requirements of attendees (e.g. adding 'capture the flag'). In 2015, TRANSITS options may be added to TF-CSIRT or FIRST meetings to support this flexibility.

The TRANSITS I technical module is being renewed in 2013, and is looking for funded volunteers to help renew this material.

TRANSITS I will next be run on 7/8 April 2014 and 20/21 November 2014 in Prague. TRANSITS II will be in Autumn 2104 in the Netherlands. Don invited anyone who is interested in becoming a TRANSITS Trainer to attend the workshop on Wednesday 12th February at the event.

Don reminded people of the new TERENA / FIRST MoU for use of TRANSITS outside of Europe. CERTS should approach FIRST if they interested in TRANSITS training outside of Europe.

4. Supertel

Supertel (Superintendencia de Telecomunicaciones de Ecuador) from Ecuador introduced themselves to the community. They described some of the issues faced by the team and their interest in the TF-CSIRT community; the team is already using RTIR. Supertel are currently supporting the government and telecommunications sectors but hope to expand to support all citizens in the future.

5. CERT-GOV-GE

CET-GOVE-GE gave an update on activities and international partnerships in Georgia. They work with information reporting over 15,000 affected IP addresses a day – to support this they have introduced a 'check my IP' service. One of their recent concerns was a report placing Georgia eighth on a list of 'most infected nations' in 2013.

Attendees expressed interest in the 'check my IP' software and ask if the CERT-GOV-GE team could make this available.

6. GEANT AND DANCERT Security Changes

Wayne Routly gave an update on changes at GEANT and DANCERT in terms of security practices. GEANT objectives in terms of security are: anomaly objectives, reporting mechanisms, incident handling and security audits.

Current system changes include EOL for Netreflex in 2014 and the introduction of an new anomaly detection system and introducing a new ticketing system. A full review of workstations is being undertaken, as well as a review of VPN access and processes.

The Security Team has bee restructured and GEANT are seeking secondees to GEANT for a 6-8 months in Cambridge to lead security policy implementation and enforcement.

Challenges in 2013 included CYNET DDoS and the "Snowdon" effect.

In response to the question of the GEANT Virtual Security Team, Wayne explained that this was part of the GEANT project looking at specific multi-domain issues and wasn't part of the core backbone support GEANT. The Virtual Security Team produced projects such as Perfsonar but was ended in GEANT2.

Wayne spoke briefly about the challenges for GEANT in supporting multiple countries across the EU in terms of attacks that may be perceived to be coming from government agencies.

7. Network Security Monitoring Working Group Presentations

Six short reports from the Network Security Monitoring Working Group were presented at the meeting.

- Jan Vykopal – summary of anomaly survey

TF-CSIRTs were invited to participate in an anomaly survey at the September 2013 meeting. Jan reported on the outcomes of this survey. 42 people responded to the survey. The survey looked at how people define 'anomalies' , how many people are dedicated to handling reports and how many reports are made.

- Wim Biemolt - Monitoring at Surfnet

Wim gave an update on monitoring practices at Surfnet.

- Pavel Kacha – CESNET Security Tools

Pavel described the following tools used by CESNET: Network Probes on CESNET perimeter, FTAS (continuous monitonring of IP traffic based on collecting netflow), G3, IDS systems, honeypots and systems for sharing correlating data (Warden and Mentat).

- Vytautas Krakauskas - Nfsen and Hadoop

Vytautas reported on a project carried out by LITNET to improve Nfsen. The main problems identified with Nfsen were limited storage and the processing time for large data set. The legal requirements to keep a six-month history for incident handling also created a bottleneck.

LITNET aimed to create a distributed programming model for Nfsen to speed up its file-by-file process. By distributing nfcap files between multiple nodes. Hadoop was used for the clustering process.

- Alexandre Dulaunoy – Port Evolution

Alexandre described an approach adopted to help hosting/ ISP companies to spot problematic IP profiles originating from their ASN. This includes anonymisation using cyrptopan.

- Jan Vykopal - Cybernetic Proving Ground

CPF offers simulation of a large network, systems, services and applications. It then monitors network behavior, detection and mitigation. This makes it easier to investigate cyber threats and attacks with automated gathering and processing of data generated during security scenarios.

This is a project recently started and with a planned end date of December 2015.

8. Date of Next Meeting and AOB

No further business was identified. Lionel Ferette confirmed that the next meeting will in Heraklion, Greece on 29th and 30th

List of Participants

Bente Christine Aasgaard	UiO-CERT
Oliver M. Achten	ThyssenKrupp IT Services GmbH
Shin Adachi	NTT-CERT
jordi aguilà	caixabank
Shehzad Ahmad	DKCERT (DTU)
Dominic Alber	Bank Vontobel AG
Joanna Animucka	SG of the Council of the EU, DGA5 Network Defence Capability
ALCIDES ARAUJO	SUPERINTENDENCIA DE TELECOMUNICACIONES
Mihai Barbulescu	Agency ARNIEC/RoEduNet
Pavel Basta	CSIRT.CZ
Javier Berciano	INTECO-CERT
Johan Berggren	Google
Wim Biemolt	SURFnet/SURFcert
Gorazd Božič	SI-CERT, ARNES
Matej Breznik	Arnes SI-CERT
Sven Bruelisauer	Open Systems AG (OS-CIRT FIRST)
Alexander Burchuladze	CERT-GOV-GE
David Byers	Linköping University
Olivier Caleff	ANSSI / CERT-FR
Roberto Cecchini	GARR, Italy
Cosmin Ciobanu	ENISA
Johannes Clos	CERT-Bund / BSI
Andrew Cormack	Jisc Collections and Janet UK
Goran Čuljak	Information System Security Bureau
michelle Danho	cert-renater
Mathieu Delavy	Nagravision - Kudelski Security

Freddy Dezeure	CERT-EU
Ivo Dijkhuis	RIPE NCC
fabien dombard	Deutsche Bank
René Dönni Kuoni	OFCOM Switzerland
Serge Droz	SWITCH
Andreas Dudler	SWITCH
Stephan Dudler	Open Systems AG
Alexandre Dulaunoy	CIRCL Computer Incident Response Center Luxembourg
Zuzana Duracinska	CSIRT.CZ
David Durvaux	Belnet
Tobias Dussa	KIT-CERT
Alexandre EPINAT	BNP PARIBAS
Lionel Ferette	ENISA
Antoni Fertner	Jisc Collections & Janet UK
Christoph Fischer	BFK edv-consulting GmbH
Carlos Fuentes	RedIRIS (Red.es)
Christian Funk	Kaspersky Labs GmbH
Sven Gabriel	EGI/Nikhef
THOMAS GAYET	LEXSI
Delyan Genkov	CERT Bulgaria
Martynas Gintalas	State enterprise "Infostruktura"
Steve GIRAUD	BNP PARIBAS
Tor Gjerde	UNINETT CERT
Oliver Goebel	RUS-CERT
JOSE GOMEZ DE LA TORRE	SUPERINTENDENCIA DE TELECOMUNICACIONES
Abel Gonzalez	INTECO-CERT
Katarzyna Gorzelak	CERT Polska / NASK
Slavo Greminger	SWITCH
Espen Grøndahl	UiO-CERT
Stéphane Grundschober	Swisscom (Schweiz) AG
Irakli Gvenetadze	CERT-GOV-GE
Tamás Gyebrovszki	GovCERT-Hungary
Peter Haag	BFK edv-consulting GmbH
Tilmann Haak	XING AG
Christian Hallqvist	ETH Zurich
Nicole Harris	TERENA
Ryosuke Hatsugai	NCSIRT, NRI SecureTechnologies, Ltd.
Michael Hausding	SWITCH
Frank Herberg	SWITCH
Alban Hessler	XING AG
Lukáš Hlavička	CSIRT.SK (DataCentrum)
Patrick Houtsch	GOVCERT.LU
Roman Huessy	GovCERT.ch
Kauto Huopio	National Cyber Security Centre Finland (NCSC-FI)
Renato Iten	Open Systems
Yurie Ito	JPCERT Coordination Center
Alexander Jäger	BASF Business Services GmbH
Peter Janulf	TeliaSonera Sweden AB
Maik Jöhrisch	CERTBw, Bundeswehr
Robert Jonsson	CERT-SE

Jonas Juknius	CERT-LT ,Communications Regulatory Authority
Pavel Kácha	CESNET
L. Aaron Kaplan	CERT.at
Baiba Kaskina	CERT.LV
Piotr Kijewski	CERT Polska / NASK
Hideo Kinoshita	MUFG-CERT
Tatsuya Kitao	The Bank of Tokyo-Mitsubishi UFJ
Mark Koek	QCSec
Klaus-Peter Kossakowski	PRESECURE Consulting GmbH
Christos Koutroumpas	CERT-EU
Vytautas Krakauskas	Swedbank
Andrea Kropacova	CESNET
Patrikas Kugrinas	LITNET CERT
Mirjam Kühne	RIPE NCC
Ossi Kuosmanen	CSC/Funet CERT
Antti Kurittu	National Cyber Security Centre Finland (NCSC-FI)
David Kvatadze	CERT-GOV-GE
Franz Lantenhammer	CERTBw, Bundeswehr
Frédéric LE BASTARD	CERT LA POSTE
Toomas Lepik	Estonian Information System Authority (CERT-EE)
Christian Lete	Swisscom
Tomás Lima	CERT.PT
Hikohiro YEN P LIN	Panasonic Corporation
Irakli Lomide	CERT-GOV-GE
Stefan Lueders	CERN
Norihiko Maeda	Kaspersky Lab, Japan
Miroslaw Maj	CERT-GOV-GE
Alejandro Maldonado	SOLUTIONS S.A.
Rocco Mammoliti	Poste Italiane
Jeroen Massar	Ops-Trust
James McLoughlin	Jisc Collections & Janet UK
Antonio Merola	Poste Italiane
Joachim Metz	Google
Maciej Miłostan	PIONIER-CERT/PSNC
Marie Moe	NorCERT
David Monnier	Team Cymru
Arne Nilsson	SUNET CERT
Jakob Nordenlund	Danish GovCERT
André Oosterwijk	NCSC-NL
Héctor Ortiz	Swisscom
Lauri Palkmets	ENISA
Antonio Perret	BCGE
Peter Peters	SURFcert
Timo Porjamo	CSC / Funet CERT
Helmi RAIS	AlliaCERT
Gaus Rajnovic	Panasonic
Ragnar Rattas	Estonian Information System Authority (CERT-EE)
Edwin Reusch	CERT BWI
ALINA RIBEIRO	LEXSI
Lorenzo Riccucci	Swiss Reinsurance Company Ltd.

Daniel Roethlisberger	SWITCH
Wayne Routly	DANTE
Sebastien RUMMELHARDT	Airbus Group CERT
Pierre SARDA	Nagravision
Derrick Scholl	Juniper Networks
Thomas Schreck	Siemens CERT
Christoph Schulthess	University of Berne
Andreas Schuster	Deutsche Telekom AG
Jacques Schuurman	XS4ALL Internet B.V.
Udo Schweigert	Siemens CERT
Remi SEGUY	General Secretariat of the Council of the European Union
Matthias Seitz	SWITCH
Stephen Sheridan	ETH Zurich
Adam Smutnicki	EGI-CSIRT/WCNS
Rolf Sommerhalder	SWITCH
Natalia Spinu	Cyber Security Center CERT-GOV-MD
Marc STIEFER	Fondation RESTENA/ RESTENA-CSIRT
Don Stikvoort	S-CURE bv
Daniel Stirnimann	SWITCH
Erika Stockinger	CERT-SE
Yoshiki Sugiura	NTT-CERT
Tamás Szép	GovCERT-Hungary
Alexander Talos-Zens	ACOnet-CERT
Masato Terada	Hitachi Incident Response Team
Christian Teuschel	RIPE NCC
David TRESGOTS	CERT-IST
Edwin Tump	NCSC-NL
Marius Urkis	LITNET CERT
Bob van der Kamp	NCSC-NL
Aleksejs Veremejenko	CERT.LV
Raphaël Vinot	CIRCL - National CERT Luxembourg
Torsten Voss	DFN-CERT Services GmbH
Valeriu Vraciu	Agency ARNIEC/RoEduNet
Jan Vykopal	Masaryk University, Institute of Computer Science
Jean-Paul Weber	GOVCERT.LU
Wilfried Woeber	ACOnet - CERT
Jyrki Yli-Paavola	TeliaSonera CERT
ALEXANDROS ZACHARIS	GRNET CERT
Stefan Zahnd	University of Bern