38th TF-CSIRT Meeting
Monday 28th January 2013
Lisbon, Portugal. The meeting was hosted by CERT-PT/FCCN.

1. Approval of Minutes

The minutes of the last meeting held on 27 & 28 September 2012 were approved.

2. Actions from last meeting

37.1 Andrea Dufkova to ask Marco Thorbrugge about the current status of CHIHT.
Done.

37.2 Lionel Ferette to continue discussion about TF-CSIRT activities on the mailing list.
Done.

3. RESTENA-CSIRT

Cynthia Wagner, RESTENA provided an update of RESTENA-CSIRT (see http://www.terena.org/activities/tf-csirt/meeting38/wagner-restena.pdf).

The 5 member team of RESTENA-CSIRT is part of the Luxembourg NREN which also provides networking services public/private institutions for research, education and culture; operate the .LU top-level domain; Is the member of TERENA, GN3 Project, GÉANT network and collaborates with other peer organisations. An array of statistics is available in the presentation.

4. CERT Austria Team update

Aaron Kaplan, CERT Austria provided an updating including an introduction of new colleagues and focusing the special interest groups that CERT.at actively participate including a call for wider participation at a meeting to be held on Wednesday morning. (see http://www.terena.org/activities/tf-csirt/meeting38/kaplan-certat.pdf).

5. Local Security Unit MEF/Consip: a brief presentation of the team

Matteo Cavallini provided an update on the internal CERT team from the Italian Ministry of Economy and Consip (see http://www.terena.org/activities/tf-csirt/meeting38/cavallini-consip.pdf).

The presentation focused on two research projects which resulted in MoTo (Monitoring Tool) and FoTo (Forensic Tool) to provide monitoring of "pastes" publishing sites on recent attacks and easy data acquisition from compromised machines for forensic analysis.

6. NREN & ISP Security Working

Wayne Routly from DANTE covered the security audits of the GÉANT network (see http://www.terena.org/activities/tf-csirt/meeting38/routly-dante.pdf).

The audits were performed by InfoLab21 in 2011 and 2012 which resulted in 40 and 42 actionable recommendations. A summary of outcomes and the composition of a working group to act as an external review committee was covered.

7. Another perspective to IP-darkspace analysis

Cynthia Wagner, RESTENA-CSIRT - Alexandre Dulaunoy and Gérard Wagener, CIRCL provided an analysis of traffic sent to mistyped private address space (RFC1918) equivalent to local darkspace (see http://www.terena.org/activities/tf-csirt/meeting38/restena-circl.pdf).

Many transposition errors of private address space (192.168.0.0/16, 10.0.0.0/8 and 172.16.0.0/12) leads to darkspace covered by these teams. The constant pattern of the traffic leads to the belief that it is mistyped configured devices producing the traffic.

8. Breach Notification and Incident

Andrew Cormack, Janet provided an update on current breach notification processes and current gaps (see http://www.terena.org/activities/tf-csirt/meeting38/cormack-janet.pdf).

The rumoured Cybersecurity Directive is expected to cover "internet companies" but telcos are already covered. The *draft* Data Protection Directive removes the legitimate interest of the recipient in information sharing. Andrew concluded with some thoughts that team should raise with their respective legislators and regulators.

9. ENISA Updates

Andrea Dufkova, ENISA provided an update on CERT relations (see http://www.terena.org/activities/tf-csirt/meeting38/dufkova-enisa.pdf).

A refresh of the existing published material and easier navigation to find documents was presented along with some statistics from the 2012 Status Report and an expansion of CERT Exercises material for training. The TRANSITS courses are rated highly in comparison with comparative courses.

10. RTIR Development Update

Kevin Falcone and Keri Shaughnessy of Best Practical the developers of RTIR and RT provided a roadmap on the development of the tool and efforts to ensure that the best of both products are merged into the base or module to ensure longer term maintainability of the code. (see: http://www.terena.org/activities/tf-csirt/meeting38/falcone-rtir.pdf)

11. Date of Next Meeting

The next TF-CSIRT meeting has been scheduled for 23rd – 24th May 2013, Bucharest, Romania.

12. AOB and Close

No other business was raised. Lionel Ferette thanked CERT-PT and FCCN for hosting the meeting. The meeting closed at 17:45 on Monday 28th January 2013.

Open Actions

No open actions.

Participants

Dirk Ableiter	Germany	CERTBw
Shin Adachi	Japan	NTT
Steve Adegbite	United States	Lockheed Martin
Shehzad Ahmad	Denmark	DK-CERT
Juan Leandro Berlanga Fuentes	Spain	UPC
Willem Biemolt	The Netherlands	SURFnet
Vladimir Bobor	Sweden	TS-CERT
Matej Breznik	Slovenia	SI-CERT
Jagor Cakmak	Hungary	CARNet
Jorge de Carvalho	Portugal	FCCN
Matteo Cavallini	Italy	MEF
Bente Christine Aasgaard	Norway	UiO-CERT
Johannes Clos	Germany	CERT-Bund
João Colier de Mendonça	Germany	Deutsche Telekom AG
Ian Cook	United Kingdom	Team Cymru
Andrew Cormack	United Kingdom	Janet
Goran Culjak	Hungary	ZSIS
Vincent Danjean	-	INTERPOL
James Davis	United Kingdom	Janet CSIRT
Freddy Dezeure	-	-
Serge Droz	Switzerland	SWITCH
Andrea Dufkova	-	ENISA
Nora Duhig	-	NeuStar
Alexandre Dulaunoy	Luxembourg	CIRCL
Jacqueline Dulmaine	Belgium	CERT.be
David Durvaux	Belgium	BELNET
Lionel Ferette	Belgium	-
David Ford	United Kingdom	University of Oxford
Sven Gabriel	The Netherlands	Nikhef/EGI CSIRT
Chris Gibson	-	FIRST

Jaap van Ginkel	The Netherlands	SURFcert
Tor Gjerde	Norway	UNINETT CERT
Katarzyna Gorzelak	Poland	CERT Polska (NASK)
John Green	United Kingdom	STFC
Espen Grondahl	Norway	UiO-CERT
Peter Haag	Switzerland	SWITCH
Martin Hathaway	United Kingdom	BT CERT
Arjan van Hattum	The Netherlands	XS4ALL
Cristine Hoepers	Brazil	CERT.br
Paweł Jacewicz	Poland	CERT PL
Przemek Jaroszewski	Poland	CERT Polska (NASK)
Robert Jonsson	Sweden	CERT-SE
Sigitas Jurkevicius	Lithuania	-
Bob van der Kamp	The Netherlands	Nationaal Cyber Security Centrum
Leon Aaron Kaplan	Austria	CERT.at
Hideo Kinoshita	Japan	Mitsubishi Financial Group
Vytautas Krakauskas	Lithuania	Litnet
Ossi Kuosmanen	Finland	Funet CERT
Franz Lantenhammer	Germany	CERTBw
Toomas Lepikq	Estonia	CERT-EE
Tomás Lima	Portugal	FCCN
Hikohiro Yen P Lin	Japan	Panasonic
Tony Lindberg	Sweden	SUNET/CERT
Antonio Liu	Germany	DFN-CERT
Norihiko Maeda	Japan	Kaspersky
Gints Malkalnietis	Latvia	CERT.LV
Yoshinobu Matsuzaki	Japan	Internet Initiative Japan
Detlev Matthies	Germany	DFN-CERT
Ilkka Mattila	Finland	CERT-FI
James McLoughlin	United Kingdom	Janet CSIRT
Barbulescu Mihai	Romania	RoEduNet
Maciej Milostan	Poland	POZNAN
Dave Monnier	United States	Team Cymru
Gustavo Neves	Portugal	FCCN
André Oosterwijk	The Netherlands	Nationaal Cyber Security Centrum
Martin Paljak	Estonia	CERT-EE
Patrick Pichler	Austria	ACOnet-CERT
Javier Pieternella	The Netherlands	Nationaal Cyber Security Centrum
Timo Porjamo	Finland	Funet CERT
Margrete Raaum	Norway	UiO-CERT
Gaus Rajnovic	-	Panasonic
Stephan Richter	Austria	CERT.at
Wayne Routly	United Kingdom	DANTE
Axel Sanner	Norway	UiO-CERT
Lino Santos	Portugal	FCCN

Robert Schischka	Austria	CERT.at
Derrick Scholl	-	-
Andreas Schuster	Germany	Deutsche Telekom AG
Jacques Schuurman	The Netherlands	XS4ALL
Udo Schweigert	Germany	Siemens
Mauro Silva	Portugal	FCCN
Adam Smutnicki	Poland	Wrocławskie Centrum Sieciowo-Superkomputerowe
Klaus Steding-Jessen	Brazil	CERT.br
Marc Stiefer	Luxembourg	RESTENA-CSIRT
Erika Stockinger	Sweden	CERT-SE
Yoshiki Sugiura	Japan	NTT CERT
Hiroshi Suzuki	Japan	Internet Initiative Japan
Rune Sydskjør	Norway	UNINETT CERT
Alexander Talos-Zens	Austria	ACOnet-CERT
Masato Terada	Japan	Hitachi
David Tresgots	France	Cert-IST
Marius Urkis	Lithuania	Litnet
Anto Veldre	Estonia	CERT-EE
Dimitra Vitsa	Greece	FORTH-ISC
Torsten Voss	Germany	DFN-CERT
Valeriu Vraciu	Romania	RoEduNet
Jan Vykopal	Czech Republic	CSIRT-MU
Gerard Wagener	Luxembourg	CIRCL
Cynthia Wagner	Luxembourg	RESTENA-CSIRT
Torbjörn Wictoin	Sweden	SUNET/CERT
Mirko Wollenberg	Germany	PRESECURE
Ken van Wyk	-	KRvW
Suguru Yamaguchi	Japan	JPCERT-CC
Jyrki Yli-Paavola	Sweden	TS-CERT
Alexandros Zaharis	Greece	GRNET