36th TF-CSIRT meeting
10 May 2012
Wetenschappelijk Centrum Watergraafsmeer, Amsterdam, The Netherlands

Please note that a seminar was held the following day. The presentations can be found at http://www.terena.org/tf-csirt/meeting36/

1. Approval of Minutes

The minutes of the last meeting held on 30 January 2012 were approved.

2. Actions from last meeting

32.2 Marco Thorbrügge to send pointer to information about Article 13a to the mailing list.
Done.

35.1 Kevin Meynell to discuss meeting between TF-CSIRT and Spamhaus.
Done.

35.2 Kevin Meynell to draft new TF-CSIRT Terms of Reference.
Done.

3. CSIRT-IE presentation

Cormac Doherty gave a presentation about the new Irish National Cyber Security Centre (see http://www.terena.org/tf-csirt/meeting36/). This built on existing emergency planning and was focusing on protecting the energy, communications and finance sectors. INCSC was itself divided into three sections covering computer security (CSG), critical national infrastructure (CNIPF), and incident response (CSIRT-IE).

CSIRT-IE would focus on helping government departments to provide their ICT infrastructure and data against attack and misuse, whilst CSG would assist by providing training and would liaise with law enforcement. INCSC was the responsibility of the Department of Communications, Energy and National Resources, but was operationally independent and would have its own dedicated infrastructure. As well as government, the initiative involved academia, law enforcement, the military and industry (e.g. Microsoft and Symantec).

One of the initiatives was the 'MakeITSecure' website (http://www.makeitsecure.ie/) that make available to the public information on computer security, identity theft, phishing and other risks Another website was the Irish Botnet Initiative (http://www.botfree.ie/) that allowed users to check for malware and provided advice on disinfecting their machines.

The question was asked whether the BotFree website was inspired by the similar Anti-Botnet project run by the German Internet Industry Association. Cormac replied it was very much based on it.

4. CERT-RO presentation

Dan Tofan gave a presentation about CERT-RO (see http://www.terena.org/tf-csirt/meeting36/tofan-cert-ro.pdf). This was established in response to the EU action calling for national CSIRTs to be established in all member countries, and was created by a law passed by the Romanian Parliament in May 2011.

The goals of CERT-RO are to analyse and respond to cyber-security incidents in Romania, along with developing national IT security policies and strategies in conjunction with other public bodies. It also acts as a national contact point for the international community.

CERT-RO is currently comprised of 20 staff, including 9 in the technical department. It is coordinated by representatives of the Ministry of Communication and Information Society, the Ministry of National Defence, the Ministry of Administration and Interior, the Romanian Intelligence Service, the Foreign Intelligence Service, the Special Telecommunications Service, the Protection and Guard Service, the National Registry Office for Classified Information, and the National Authority for Management and Regulations in Communications. There are several other recognised CSIRTs within the CERT-RO community including CorisSTS, RoCSIRT and CertMil, but it is planned to develop better cooperation with the private sector.

As well as the normal portfolio of proactive, reactive and training and awareness raising activities, future plans also include a national early warning system, a cybersecurity training centre, and the development of public security standards.

Lionel Ferette asked whether the organisation was currently fully staffed. Dan replied there were still 11 unfilled vacancies as it was it difficult to find suitable people.

5. CSIRT.SK presentation

Tomas Kokolevsky gave a presentation about CSIRT.SK (see http://www.terena.org/tf-csirt/meeting36/kololevsky-csirt-sk.pdf). This is the Slovakian national and governmental CSIRT that was established in July 2009 in response to increasing threats to critical infrastructures, and is operated as an independent department of DataCentrum under contract to the Ministry of Finance.

There is no legally defined constituency yet, but CSIRT.SK is supporting the government and certain public services in Slovakia. It is also promoting IT security incident handling, whilst providing the national point of contact for the international community.

CSIRT.SK handled around 3000 incidents during 2011, of which 70 were considered critical. The most common were web attacks (41%), with phishing (17%), malicious code (17%), system penetration attempts (16%) and botnets (9%) the next most common. They were using THEMIS as an early warning system that also offered information sharing through secure channels.

CSIRT.SK had also participated in two international critical infrastructure exercises – CyberEurope 2010 and CyberAtlantic 2011, as well as the national SISE 2011 (Slovak Information Security Exercise) that had international participation. As part of the plan to raise information security awareness, a hardware and software forensics lab would be held in August 2012.

Lionel Ferette asked why CSIRT.SK came under the Ministry of Finance as this was a different arrangement to many other countries. Tomas replied this was unclear and was presumably a political decision.

6. EGI-CSIRT presentation

Adam Smutnicki gave a presentation about EGI-CSIRT (see http://www.terena.org/tf-csirt/meeting36/smutnicki-egi-csirt.pdf). This was a distributed CSIRT that provided incident handling and coordination for the European Grid Infrastructure; a federation of 350+ resources centres in 50+ countries.

EGI-CSIRT had been operational since May 2010 and was comprised of representatives of National Grid Initiatives (NGIs). It was itself divided into four teams.

The Incident Response Task Force (IRTF) deals with incident handling, coordination, vulnerability assessment, and forensics. The Security Management Group (SMG) provides system level monitoring and notifications using various tools. The Security Drill Group (SDG) organises non-intrusive security exercises in order to ensure responses and handling were adequate and to identity areas that could be improved. Finally, the Training and Dissemination Group (TDG) provides security training and information for Grid operatives.

Adam went on to outline the operational actions and procedures of the IRTF in which 14 NGIs actively participated. There had been 18 incidents since 2010, most of which had been confined to single sites. However, it was also important to have good relationships with NREN CSIRTs as incidents can spread quickly in grid infrastructures across different networks with different administrations.

7. Redesigning CERT.at's incident handling capabilities

Aaron Kaplan discussed the improvements to the incident handling capabilities of CERT.at that are being undertaken (see http://www.terena.org/tf-csirt/meeting36/kaplan-cherrypicking.pdf). With the number of incidents ever increasing, it is becoming ever more urgent to improve automated handling capabilities, as well as reliably categorise incidents so that resources can be focused more effectively.

CERT.at is currently processing feeds from several sources, but does not have good trending and statistics generating capabilities and there were concerns with how this would scale in future with more feeds. They had a requirement for uniform processing of mass-log events, the ability to integrate new feeds quickly, closer integration with RTIR, a standardised output format, and a feedback mechanism for report recipients.

AbuseHelper and Megatron were existing solutions that attempted to address these requirements. Whilst they had their strengths, they also had limitations and some effort should be put into synthesising an improved solution from the best aspects of both. To this end, a small team from CERT.at and CERT.be had been put together with the aim of improving AbuseHelpers' batch capabilities and event logging through regular Hackathons. They also had a request for the TI database so that the information could be easily imported for contact purposes.

8. Blocking access to phishing websites

Alexander Talos-Zens talked about the issues surrounding the blocking of phishing sites (see http://www.terena.org/tf-csirt/meeting36/zen-talos-phishing.pdf). Phishing was increasing and becoming ever more sophisticated, but there were questions over the legality of blocking sites where this was occurring, especially as the site owners were often innocent victims themselves. Whilst users were generally supportive of action being taken, in some cases blocking caused significant inconvenience and sometimes financial

losses.

The effectiveness of blocking websites was also questionable as phishing was most effective when users responded within an hour or two before sites could be blocked. Moreover, phishers often targeted users at weekends or during holiday periods when response times were generally slower. In other cases, users had used their mobile phones or home networks to access sites when they found them to be blocked on their institutional network, which rather defeated the purpose of blocking them in the first place.

Derek Simpson (?) felt the role of a CSIRT was primarily to protect the network(s) of its own constituency, and whilst protections may cause collateral damage or be circumvented, that should only be a secondary consideration.

Andrew Cormack suggested that when sites were blocked, users could be redirected to a 'landing' page that explained the reasons why this had been done (e.g. http://education.apwg.org/r/about.html). That might help prevent users trying to reach the sites through other networks, and Kauto Huopio further suggested that a community phishing service might be established to provide filtering information to network providers.

Christian Van Heurck added that a lack of institutional training had also helped phishers to scam users. In one particular case, a police offcer had advised a user to pay a demand because it appeared to have come from an official police source.

9. AbuseHelper update

Christian Van Heurck provided a progress update on AbuseHelper (see http://www.terena.org/tf-csirt/meeting36/vanheurck-abusehelper.pdf).

The planned production setup involved two nodes replicating data in accordance with a database model developed by CERT.at and CERT.be (specifically Aaron Kaplan). This recorded event types and priority, the event source along with a computed score, and then a link to RTIR by ticket number. The database was intended to be generic and would be open for use by other teams.

A complementary dashboard was currently being designed by Koen Van Impe and whilst it was specifically designed for the needs of the developers, it would also be open and might fit the needs of others. There were also plans for further visualisation of the data based on an open framework, but at the moment this had not yet progressed.

10. Report on RTIR BoF

James Davis gave a short report on the RTIR BoF that had been held after the previous meeting in Rome (http://www.terena.org/tf-csirt/meeting36/davis-rtir.pdf). This had been attended by 15 participants and was called in response to concerns that RTIR needed improvement.

RTIRv3 had been developed with little coordinated input from the CSIRT community, and there was a lack of information about future plans. It was also felt that RTIR was difficult to set up and there was insufficient support and documentation available for new users. It also needed to be better integrated with automated workflows and tools (e.g. AbuseHelper), and some teams remained unhappy with its performance.

It was clear there were some ideas of the things that needed to be improved, but nothing approaching concrete plans. There had been little activity on the mailing list since the last meeting, and without further discussions there was insufficient progress to warrant holding another BoF or asking to meet with Best Practical

Kauto commented that RTIR didn't really fulfil their requirements any more, and given the rising number of incidents it was expected to handle, they had concerns that software simply wouldn't scale in five years. Something therefore needed to be done before this happened.

Lionel added that whilst TF-CSIRT/TERENA was more than willing to coordinate and provide a financial and legal framework for improving RTIR as it had previously, this required teams to come up with a firm list of the things that needed to be done. This could not happen without teams providing input, and being actively involved in drafting a specification.

11. The Clean IT project

But Klassen presented the Clean IT project (see http://www.terena.org/tf-csirt/meeting36/klassen-clean-it.pdf). This is an international project between the Netherlands, Belgium Germany, Spain and the United Kingdom and partly funded by the European Commission, to initiate cooperation between public and private partners to counter use of the Internet by terrorists. This includes targeting of the Internet, using the Internet as a weapon, and also to facilitate dialogue between terrorists themselves.

The aim is to develop a voluntary and cooperative framework supported by industry, through a series of workshops and conferences. It is hoped to present some interim results in June 2012, but it would also be useful if the TF-CSIRT community could provide input to the draft paper.

12. CERT-SE developments

Erika Stockinger announced that CERT-SE would shortly be getting a new Director, and would also be moving to new premises.

13. TRANSITS I & II update

Don Stikvoort gave a short update on the TRANSITS training courses (see http://www.terena.org/tf-csirt/meeting36/stikvoort-transits.pdf). The next TRANSIT-I course would be organised during Autumn 2012, whilst the next TRANSITS-II course would be organised in October 2012 in Utrecht, the Netherlands.

14. Academic CSIRT meeting

Kevin Meynell announced that a meeting for academic CSIRTs was being organised in conjunction with FIRST 24 (see http://www.terena.org/tf-csirt/meeting36/meynell-academic-csirt.pdf). This would be held on Sunday, 17 June 2012 at the Hilton Malta in Portomaso St. Julian's, Malta.

This was a follow on from a similar meeting that had been held at FIRST 23. Some of the topics to be covered were academic security policies, intellectual property theft, trends in security incidents and cloud security.

Those wishing to attend should register at https://www.terena.org/events/details.php?event_id=2253. A fee in the order of EUR 65 (depending on numbers) will be charged to cover costs, although lunch and refreshments will be provided.

15. TF-CSIRT developments

Kevin Meynell gave an update on the latest TF-CSIRT developments (see http://www.terena.org/tf-csirt/meeting36/meynell-tf-csirt.pdf).

A proposal had been circulated in early January and discussed at the previous meeting in Rome (see http://www.terena.org/tf-csirt/publications/restructuring.pdf). This introduced the concept of membership categories, an elected Chair, a Steering Committee with an enhanced role, and TF-CSIRT formally becoming the umbrella for TI, TRANSITS and other security related activities. As a result, the Task Force agreed to draft new Terms of Reference.

The new Terms of Reference are based on four existing documents – the existing TF-CSIRT Terms of Reference, the TI procedures for the Review Board and Meetings, the TI meeting access rules, and the description of work in the TI contract. A first draft had been circulated to the TF-CSIRTng Working Group on 8 March 2012, and there had been several iterations in response to comments received.

Following this, an updated draft was circulated to the whole TF-CSIRT community on 19 April 2012 (see http://www.terena.org/tf-csirt/publications/proposed-ToR.pdf). Some additional comments had already been received, but any further comments should be sent to Kevin Meynell by 3 June 2012 as the Terms of Reference then needed to be submitted to TERENA for approval.

A transitional period for the TI Review Board members had been agreed at the TI Review Board meeting in January 2012, and this was outlined in Article 5 of the proposed Terms of Reference. In addition, a transitional period for the mailing list was envisaged as outlined in Article 8 of the proposed Terms of Reference, with unaffiliated subscribers being encouraged to apply for membership.

Finally, new logos had been designed for TF-CSIRT, TI Certified Teams, and TI Accredited Teams.

16. Date of next meeting

Lionel Ferette thanked NCSC, SURFnet, the University of Amsterdam and XS4ALL/KPN-CERT for hosting the meeting.

The next meeting will be held on 27-28 September 2012 in Ljubljana (hosted by SI-CERT).

Open Actions

No open actions.

Participants

Name	*Organisation*	*Country*
Shehzad Ahmad	DK-CERT (UNI-C)	Denmark
Pascal Arends	Fox-IT	The Netherlands
Jurre van Bergen	NIKHEF	The Netherlands
Wim Biemolt	SURFcert (SURFnet)	The Netherlands
Phons Bloemen	Ziggo	The Netherlands
Ian Cook	Team Cymru	United Kingdom
Andrew Cormack	JANET(UK)	United Kingdom
Jan-Pieter Cornet	XS4ALL	The Netherlands
Michelle Danho	CERT-RENATER	France
Tjerk Datema	XS4ALL	The Netherlands
James Davis	Janet CSIRT	United Kingdom
Dreas van Donselaar	SpamExperts	The Netherlands
Nils Decker	SpamExperts	The Netherlands
Cormac Doherty	CSIRT-IE	Ireland
Andrea Dufkova	ENISA	-
Alexander Dulaunoy	CIRCL	Luxembourg
Leon van der Eijk	DefCERT	The Netherlands
Lionel Ferette (Chair)	-	Belgium
Carlos Fuentes	IRIS-CERT (RedIRIS)	Spain
Sven Gabriel	NIKHEF	The Netherlands
Erik van Garderen	KPN	The Netherlands
Jaap van Ginkel	University of Amsterdam	The Netherlands
Tilmann Haak	DFN-CERT	Germany
Martijn de Hamer	NCSC-NL	The Netherlands
Lucien Hasselbaink	DefCERT	The Netherlands
Martin Hathaway	BT CERT	United Kingdom
Arjun van Hattum	XS4ALL	The Netherlands
Michael Hausing	SWITCH-CERT	Switzerland
Martijn van der Heide	KPN-CERT	The Netherlands
Jesse Helder	KPN-CERT	The Netherlands
Kauto Huopio	CERT-FI (FICORA)	Finland
Yorkvik Jacqmin	CERT.be	Belgium
Xander Jansen	SURFcert	The Netherlands
Przemek Jaroszewski	CERT Polska (NASK)	Poland
Eric de Jong	Fox-IT	The Netherlands
Bob van der Kamp	NCSC-NL	The Netherlands
L. Aaron Kaplan	CERT.at	Austria
Adam Karama	Ziggo	The Netherlands
Mikael Keri	Handelsbanken SIRT	Sweden
But Klassen	Ministry of Security and Justice	The Netherlands
Remon Klein Tank	SURFcert & WUR	The Netherlands
Mark Koek	Fox-IT	The Netherlands
Oscar Koeroo	NIKHEF	The Netherlands
Tomas Kokolevsky	CSIRT-SK	Slovakia
Klaus-Peter Kossakowski	PRESECURE	Germany
Jelle Kroon	KPN	The Netherlands
Andrea Kropacova	CESNET CERTS	Czech Republic
Patrick van de Kuil	XS4ALL	The Netherlands
Ossi Kuosmanen	Funet CERT	Finland
Arien Landgraaf	Bricade	The Netherlands
Antonio Liu	Trusted Introducer	Germany
Kevin Meynell (Secretary)	TERENA	-
Barbulescu Mihai	RoCSIRT	Romania

Milda Mimiene	LITNET CERT	Lithuania
Otto Mäkelä	Funet CERT	Finland
Tomas Nowocien	Pionier-CERT	Poland
Luuk Oostenbrink	SURFcert	The Netherlands
André Oosterwijk	NCSC-NL	The Netherlands
Niels den Otter	SURFnet	The Netherlands
Bertwin Oudenampsen	ITQ	The Netherlands
Peter Peters	SURFcert & CERT-UT	The Netherlands
Erik Post	Ziggo	The Netherlands
Wayne Routly	DANTE	-
Jorge Ruão	CSIRT.FEUP	Portugal
Aidan Ryan	CSIRT-IE	Ireland
Mischa Sallé	NIKHEF	The Netherlands
Timo Schulz	DFN-CERT	Germany
Andreas Schuster	Deutsche Telekom	Germany
Hessel Schut	NHTCU	The Netherlands
Jacques Schuurman	XS4ALL	The Netherlands
Derek Simpson	BTCERTCC	United Kingdom
Adam Smutnicki	WCNS	Poland
Wouter Steenbeek	NSCR	The Netherlands
Carel van Straten	Spamhaus	The Netherlands
Don Stikvoort	S-CURE	The Netherlands
Daniel Stirnimann	SWITCH	Switzerland
Erika Stockinger	CERT-SE	Sweden
Manuel Subredu	RoCSIRT	Romania
Tristan Suerink	NIKHEF	The Netherlands
Alexander Talos-Zens	ACOnet-CERT	Austria
Han van Thoor	Jumper CSIRT	Ireland
Dan Tofan	CERT-RO	Romania
Colin Tomlinson	Trusted Introducer	United Kingdom
Marius Urkis	LITNET CERT	Lithuania
Christian Van Heurck	CERT.be	Belgium
JP Velders	SURFcert & UvA	The Netherlands
Rob Vercouteren	KPN-CERT	The Netherlands
Sjoerd Versteeg	ITQ/HITB	The Netherlands
Folkert Visser	KPN-CERT	The Netherlands
Henri Wiering	SpamExperts	The Netherlands
Wilfried Wöber	ACOnet-CERT	Austria
Mirko Wollenberg	PRESECURE	Germany
Dave Woutersen	NCSC-NL	The Netherlands
Peter Zinn	NHTCU	The Netherlands

Apologies were received from:

Matthew Cook	ESISS/Loughborough University	United Kingdom
Peter Dimkov	CERT Bulgaria	Bulgaria
Patrick Houtsch	GOVCERT.LU	Luxembourg
David Landeweer	CSIRT ING Insurance	The Netherlands
Margrete Raaum	UiO-CERT	Norway
Marc Stiefer	RESTENA-CSIRT	Luxembourg
Thomas Stridh	SUNET CERT	Sweden
Marco Thorbruegge	ENISA	-
Georges Toth	GOVCERT.LU	Luxembourg
Jan Vykopal	CSIRT-MU	Czech Republic