32nd TF-CSIRT meeting
1 February 2011
CaixaForum, Barcelona, Spain

Please note that a seminar was held the following day.

1. Approval of Minutes

The minutes of the last meeting held on 16 September 2010 were approved.

2. Actions from last meeting

31.1 TI Review Board to discuss how to deal with Spamhaus problems and what further action to take.
Ongoing.

31.2 CERT NIC.LV to document specific problems they had experienced with Spamhaus.
Ongoing.

3. CERT.LV presentation

Baiba Kaskina gave a presentation about CERT.LV (see http://www.terena.org/tf-csirt/meeting32/kaskina-cert.lv.pdf). A new law passed by the Latvian Parliament in October 2010 decided to merge the government CSIRT (DDIRV) with the academic and commercial CSIRT (CERT NIC.LV) under the auspices of the Institute of Mathematics and Computer Science at the University of Latvia. The new entity came into effect on 1 February 2011 and would be known as CERT.LV.

This decision had been somewhat unexpected, but it allowed for the pooling of resources to improve IT security in the country. It would be government funded and could call upon ten staff (4.5 FTEs). The focus would be on incident response, the raising of security awareness, security research, and cooperation with other CSIRTs. There were also plans to conduct exercises and firedrills with state and municipal organisations.

4. GOVCERT.NL presentation

André Oosterwijk gave a presentation about GOVCERT.NL. This was the Dutch government CSIRT that had been founded in 2002 under the auspices of the Ministry of Internal Affairs. It was currently comprised of 15 internal employees, with a similar number of external employees working on supporting activities.

There were three departments focusing on incident handling and response, knowledge dissemination, and service development. They had developed several incident and intrusion detection monitoring systems in collaboration with SURFnet and NASK, and were developing a CERT Academy in collaboration with KPN-CERT to raise awareness and train CSIRT staff in the Netherlands.

They were also involved in the development of a national cybersecurity strategy to consolidate the responsibilities of different departments under the Department of Safety and Justice.

Marco Thorbrügge commented that he thought GOVCERT.NL already performed the functions of a national CSIRT. André replied this was not currently an official role.

Kauto Huopio asked whether the CERT Academy materials could be made available to other CSIRTs. André said he didn't know what the use policy was, but he would find out.

Action 32.1 - André Oosterwijk to check whether CERT Academy materials could be made available to other CSIRTs.

5. CESICAT-CERT presentation

Carlos Fragoso gave a presentation about CESICAT-CERT (see http://www.terena.org/tf-csirt/meeting32/fragoso-cesicat.pdf). This was a part of CESICAT which was a foundation set up by the Catalan government to support information security in the region. In addition to the Catalan government, there were also a number of other sponsors and stakeholders including local authorities, universities, the Catalan Chamber of Commerce, and banks.

The constituency served included public bodies, higher education and research institutes, small and medium sized enterprises, as well as private citizens. As well as providing incident response, it also aimed to actively reduce vulnerabilities, promote security awareness and provide consultancy in collaboration with other parties.

In conjunction with this, they collaborated closely with the Catalan police service and currently had a police officer working with them. This provided a direct line of communication to law enforcement agencies, whilst familiarising their officials with network security issues.

Marco Thorbrügge asked whether the police officer was on a permanent detachment to CESICAT. Carlos replied that he was, although he also had other police duties so was not available full time.

6. ENISA update

Marco Thorbrügge gave an overview of the work that ENISA was planning in 2011 (see http://www.terena.org/tf-csirt/meeting32/thorbruegge-enisa.pdf). This included the reprising the pan-European drill exercises, facilitating the transposition of Article 13a of the EU's common regulatory framework into national laws, and undertaking a cost benefit analysis of implementing security measures.

Another goal was to reinforce national and government CSIRTs by encouraging proactive detection of incidents as well as better cooperation with law enforcement agencies. They also aimed to address the legal aspects of cross-border information sharing, to determine how this could be improved.

Kauto Huopio? asked about the latest status of Article 13a. Marco replied there was some information on the ENISA and he'd send a pointer to the mailing list.

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

Kauto also asked whether ENISA was working with European CSIRTs outside of the EU. Marco replied this was part of the general plan.

7. Malware Domain Notification

Serge Droz gave a presentation on the malware domain notification process in Switzerland.

Most malware reaches users through infected websites, but SWITCH as the national ccTLD registry also knows who the owners of .ch domains are. It should be recognised that website owners are often innocent victims as well, but in 2010 the law was modified to allow domains to be blocked if there is reasonable suspicion that a website is being used to distribute malware or hosts a phishing page.

If SWITCH are informed of potential misuse of a domain, they have the power to block it if there is no response from the owner or technical contact within one day. They are then obliged to notify the authorities as to whether further action should be taken, but must unblock the domain within 5 days unless they hear otherwise.

Since the implementation of the new law, around 1,000 URLs had been referred to them and they had temporarily blocked around 30. Most website owners were quite happy when comprises were pointed out to them, although a few had been difficult. However, the general aim was to improve awareness amongst hosting as to security vulnerabilities.

8. AbuseHelper update

Christian Van Heurck provided an update on the AbuseHelper system (see http://www.terena.org/tf-csirt/meeting32/vanheurck-abusehelper.pdf). This was a framework to automate incident report processing based on a variety of inputs such as blacklists, intrusion detection systems and Whois.

A development plan was currently being formulated based on the requirements of the BELNET CERT and CERT.be constituencies, with input from other CSIRTs as well. This aimed to identify which aspects of the framework needed improving, which tools needed modification, and how the statistical analysis should be implemented.

With this in mind, CERT.be was organising a workshop at the BELNET offices in Brussels on 2-4 May 2011 (see http://abusehelper.eventbrite.com/). This was open and would provide an overview of the system as well as cover technical and legal issues.

9. TRANSITS/TRANSITS2 update

Don Stikvoort gave an update on the recent TRANSITS course and forthcoming TRANSITS II course (see http://www.terena.org/tf-csirt/meeting32/stikvoort-transits.pdf).

The most recent TRANSITS workshop had been held on 25-26 January 2011 in Frankfurt, Germany and had involved around 30 participants. The next workshop would be held in the Autumn 2011, although the host still needed to be confirmed.

After a successful trial workshop in October 2010, it had been decided to hold the first TRANSITS II workshop on 6-8 April 2011 in Zürich, Switzerland. This would consist of advanced topics such as forensics, NetFlow, communications skills and practical exercises.

More information about the workshop could be found at http://www.terena.org/csirt-training/transits-ii/courses/switch/ and the deadline for applications was 18 February 2011.

10. RIPE Database IRT and Abuse Task Force

Wilfried Wöber reported that some policies had been agreed at RIPE 61 to improve the quality of contact data in the RIPE Database, as well as ensure this was regularly updated (see http://www.terena.org/tf-csirt/meeting32/woeber-ripe-tf.pdf). To some extent this was a continuation of the work of the RIPE Data Protection Task Force, but a new task force had been chartered with the aim of holding a kick-off meeting later in the year at RIPE 63 in Vienna. This would therefore be a good opportunity for CSIRTs to get involved.

11. ICANN Review of WHOIS policy (RT4)

Wilfried Wöber reported on ICANN's ongoing review of WHOIS policy. This aimed to assess whether the maintenance of WHOIS data met the needs of law enforcement and commercial competition, whilst conforming with national laws.

The Review Team had adopted an action plan to reach its recommendations, as well as an outreach policy to ensure input could be received from all interested parties. As CSIRTs had an interest in the availability and quality of WHOIS information, they may wish to consider providing input into this process.

12. BGP Ranking Project

Alexandre Dulaunoy gave a presentation on the use of BGP data to supplement the security ranking of ISPs (see http://www.terena.org/tf-csirt/meeting32/dulaunoy-bgpranking.pdf). The use of CIDR blocks or AS numbers can be used to assess threat levels, as well as detect suspicious activities amongst ISPs. This can in turn be used as an additional factor in assessing the trustworthiness of specific ISPs.

AS numbers are ranked according to a specific formula, and rankings for individual AS numbers can be queried via a web and DNS interface. The next stage was to improve the query interface, as well as adding a collaborative ranking scheme for CSIRTs.

13. Passive DNS update

Otmar Lendl provided an update on the Passive DNS project (see http://www.terena.org/tf-csirt/meeting32/lendl-dns.pdf). This aims to capture zone information and timestamp it, thus giving CSIRTs the possibility of tracing IP addresses from DNS records.

CERT.at and the University of Vienna had implemented a passive DNS server that could search entire address ranges and could be searched using a web interface. However, they were currently looking to add more sensors to test scalability, especially large recursive DNS sensors at ISPs and universities.

They were quite careful about privacy concerns, with source IP addresses anonymised and the collected data only used for incident handling purposes. The database remained in the EU and it was also be necessary for participants to sign an NDA.

Andrew Cormack commented that although there was considerable uncertainty over how

EU privacy law applied to this kind of information, the approach to handling passive DNS data appeared to address any privacy concerns that might be raised.

14. Date of next meeting

The next meeting will be held on 2-3 June 2011 in Dublin, Ireland (hosted by Jumper CSIRT).

The following meeting will be held on 22-23 September 2011 in Luxembourg City, Luxembourg (hosted by RESTENA-CSIRT and CIRCL).

Open Actions

31.1 TI Review Board to discuss how to deal with Spamhaus problems and what further action to take.

31.2 CERT NIC.LV to document specific problems they had experienced with Spamhaus.

32.1 André Oosterwijk to check whether CERT Academy materials could be made available to other CSIRTs.

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

Participants

Name	*Organisation*	*Country*
Shin Adachi	NTT-CERT	United States
Shehzad Ahmed	DK-CERT (UNI-C)	Denmark
Leonardo Amor	Telefonica	Spain
Jonathan Ashton	OxCERT	United Kingdom
Daniele Barbosa	Motorola	Brazil
Javier Berciano	INTECO-CERT	Spain
Johan Berggren	NORDUnet	-
Wim Biemolt	SURFcert	The Netherlands
Bence Birkás	CERT-Hungary	Hungary
Gorazd Bozic	ARNES	Slovenia
Matej Breznik	ARNES	Slovenia
Nils Byström	SUNET CERT	Sweden
Jagor Cakmak	CARNet	Croatia
Domingo Cardona	TB-Security	Spain
Roberto Cecchini	GARR	Italy
Jorge Chinea	INTECO-CERT	Spain
Ian Cook	Team Cymru	United Kingdom
Andrew Cormack	JANET(UK)	United Kingdom
Michelle Danho	CERT-RENATER	France
James Davies	JANET CSIRT	United Kingdom
Ralf Dörrie	Telekom-CERT	Germany
Serge Droz	SWITCH-CERT	Switzerland
Alexandre Dulaunoy	CIRCL	Luxembourg
Mark Duller	OxCERT	United Kingdom
Øyvind Eilertsen	UNINETT CERT	Norway
Per Arne Enstad	UNINETT CERT	Norway
Lionel Ferette (Chair)	BELNET CERT	Belgium
Antoni Fertner	JANET CSIRT	United Kingdom
Robert Floodeen	CERT/CC	United States
Carlos Fragoso Mariscal	CESICAT-CERT	Spain
Julio Garcia	McAfee	Spain
Manual Garćia-Cervigon	esCERT-UPC	Spain
Natasha Glavor	CARNet	Croatia
Katarzyna Gorzelak	CERT Polska (NASK)	Poland
Chad Greene	eBay	United States
Jordi Guijarro	CESCA	Spain
Peter Haag	SWITCH-CERT	Switzerland
Tilman Haak	DFN-CERT	Germany
John Haller	CERT/CC	United States
Lourdes Herrero Gil	Generalitat Valencia	Spain
Vincent Hinderer	CERT-LEXSI	France
Jose Miguel Holguin Aparicio	Generalitat Valencia	Spain
Nicolas Holin	CERTA	France
Brian Honan	IRISSCERT	Ireland
Kauto Huopio	CERT-FI (FICORA)	Finland
Nino Jogun	CARNet	Croatia
Robert Jonsson	CERT-SE	Sweden
Baiba Kaskina	CERT.LV	Latvia
Piotr Kijewski	CERT Polska (NASK)	Poland
Mark Koek	Fox-IT	The Netherlands
József Komli	CERT-Hungary	Hungary
Klaus-Peter Kossakowski	PRESECURE	Germany
Alex Kouzmine	CERT-LEXSI	Canada

Andrea Kropacova	CZ.NIC	Czech Republic
Rob Kuiters	KPN-CERT	The Netherlands
Olivier Lafon	CERTA	France
Franz Lantenhammer	CERTBw	Germany
Jose Legido	GMV	Spain
Otmar Lendl	CERT.at	Austria
Toomas Lepik	CERT-EE	Estonia
Antonio Liu	Trusted Introducer	Germany
Mario Maawad	la Caixa	Spain
Peter Magula	CSIRT.SK	Slovakia
Stelios Maistros	GRNET-CERT	Greece
Chelo Malagón	RedIRIS	Spain
Ignacio Mancebo	GMV	Spain
Egil Mannerheim	Swedbank SIRT	Sweden
Arturs Medenis	NIC.LV	Latvia
Kevin Meynell (Secretary)	TERENA	-
Francisco Montserrat	RedIRIS	Spain
Lucas Moody	eBay	United States
Luis Morais	CERT.PT (FCCN)	Portugal
Javier Morant	Generalitat Valencia	Spain
Thomas Nguyen-Van	Jumper Consulting	Ireland
Tomasz Nowocień	PIONIER-CERT	Poland
Takayuki Oku	INTERPOL	-
Masashi Omori	IT Promotion Age Japan	Japan
André Oosterwijk	GOVCERT.NL	The Netherlands
Dimos Panagopoulos	FORTH-CERT	Greece
Martin Peterka	CZ.NIC	Czech Republic
Jacomo Piccolini	ESR/RNP	Brazil
Mario Plepelic	CARNet	Croatia
Markellos Potamitis	OCECPR	Cyprus
Margrete Raaum	UiO-CERT	Norway
Allan Rasmussen	DK-CERT (UNI-C)	Denmark
Bart Roos	GOVCERT.NL	The Netherlands
Wayne Routly	DANTE	-
Jorge Ruão	Porto University	Portugal
Ramon Saez	CCN-CERT	Spain
Antonio Sanchez	National Cryptologic Center	Spain
Jürgen Sander	PRE-CERT	Germany
Pekka Savola	FUNET CERT (CSC)	Finland
Robert Schischka	CERT.at	Austria
Andreas Schuster	Deutsche Telekom	Germany
Jacques Schuurman	XS4ALL Internet	The Netherlands
Udo Schweigert	Siemens CERT	Germany
Derek Simpson	BT	United Kingdom
Mark Stiefer	RESTENA-CSIRT	Luxembourg
Don Stikvoort	S-CURE	The Netherlands
Erika Stockinger	Sitic	Sweden
Yoshiki Sugiura	NTT	Japan
Harri Sylvander	FUNET CERT (CSC)	Finland
Dave Tabatadze	CERT-GE (GRENA)	Georgia
Alexander Talos-Zens	ACOnet-CERT	Austria
Marco Thorbrügge	ENISA	-
David Tresgots	Cert-IST	France
Marius Urkis	LITNET CERT	Lithuania
Christian Van Heurck	BELNET CERT	Belgium
Luis Vasquez	Telefonica Peru	Peru

Simona Venuti	GARR-CERT	Italy
Lluis Vera	TB-Security	Spain
Marc Vilanova	la Caixa	Spain
Torsten Voss	DFN-CERT	Germany
Wilfried Wöber	ACOnet-CERT	Austria
Yoshio Yamada	National Police Agency	Japan
Jyrki Yli-Paavola	TS-CERT	Finland
Takahiko Yoshido	NTT	Japan

Apologies were received from:

Przemek Jaroszewski	CERT Polska (NASK)	Poland
Han van Thoor	Jumper CSIRT	Ireland