25th January 2016

Reference/Subject: Minutes: 47th TF-CSIRT Meeting

Amsterdam Office
Singel 468 D
1017 AW Amsterdam
The Netherlands
+31 (0) 20 5304488

www.geant.org
info@geant.org

Minutes of the 47th TF-CSIRT Meeting

25th January 2016
Prague, Czech Republic. Hosted by CZ.NIC.

Table of Contents

1. Welcome and AOB 1
2. Minutes of the Last Meeting 1
3. TI Team Update – Antonio Liu 1
4. TRANSITS Update – *Nicole Harris and Irina Mikhailava* 2
5. CSIRT Maturity and TI Certification – *Baiba Kaskina and Andrea Dufkova* 2
6. About Vulnerability Disclosure – *Cosmin Ciobanu* 3
7. BT Team Update – Daniel Porter and Graham Austin, BT 3
8. To share or not to share, that's just one question - *Jean-Paul Weber, GOVCERT.LU* 3
9. CSIRT.CZ from 2011 to 2016 – Zuzana Duračinská 4

1. Welcome and AOB

Baiba Kaskina welcomed attendees to the meeting and thanked the host for this meeting – cz.nic.

There was no AOB proposed.

2. Minutes of the Last Meeting

The minutes of the 46th Meeting were accepted as an accurate record of the meeting.

3. TI Team Update – Antonio Liu

Antonio Liu gave an update from the TI team.

There are 12 new listed teams within TI for this period, 8 of which are commercial teams. This continues the trend of commercial teams being the main new parties within TI. There are 6 new accreditation candidates, 5 of which are commercial. CERT BWI became a certified team.

As reported in the closed meeting, the second response test has been successfully carried out. A TI Out-of-Band Alerting test was also successfully carried out. Teams were reminded to ensure that there are TWO team representatives in the TI database to ensure continuity.

The team has also introduced a self-service interface for managing teams and candidate proposals and this has been well received.

TI is introducing user certificates for listed teams. TI is in the process of asking listed teams to name individuals to receive the certificates via PGP signed emails. TI is also working to implement registration via TI certificates for GÉANT events.

The full slides from the presentation can be found at: https://www.terena.org/activities/tf-csirt/meeting47/A.Liu-TI-update-public.pdf.

4. TRANSITS Update – *Nicole Harris and Irina Mikhailava*

Nicole Harris updated members on the upcoming TRANSITS I training, to be held 13th – 14th April 2016 in the Netherlands. Nicole introduced Irina Mikhailava to the community. Irina will be leading TRANSITS training coordination moving forward.

Full details of the next TRANSITS I training can be found at: https://www.terena.org/activities/transits/transits-i/egmond/april-2016/.

5. CSIRT Maturity and TI Certification – *Baiba Kaskina and Andrea Dufkova*

ENISA presented their previous work on CSIRT maturity that moved from TIER 1 (fundamental), to TIER 2 (baseline), to TIER 3 (Advanced) and compared this to the SIM3 model and its use for TI certification.

This is the first document that really discusses the TI certification process and it provides a useful introduction to any team considering certification. The focus of the work to date was on government and national CSIRTS but the work is reusable. The CSIRT Maturity Kit by NCSC-NL is also a useful document.

Members asked how we measure the effectiveness of teams as well as maturity.

The full slides from the presentation can be found at: https://www.terena.org/activities/tf-csirt/meeting47/A.Dufkova-B.Kaskina-CSIRT-maturity.pptx.

6. About Vulnerability Disclosure – *Cosmin Ciobanu*

Cosmin Ciobanu gave an overview of the ENISA study on disclosure. The incentive for the study was to examine the way the disclosure of vulnerabilities was handled (either by researchers or vendors) in the light of a string of security issues (e.g. heartbleed, shellshock, sandworm etc.).

The ENISA study was supported by RAND Europe to provide an overview of the current situation for the vulnerability disclosure scene. Cosmin presented the attempt to break a Chubb Detector lock in 1853 as the first vulnerability disclosure… this is comparable to teams nowadays showing issues with security locks online.

For sometime, full disclosure was championed as the only true way to manage information sharing. This has changed with increasingly complex regulations, legal challenges / prosecutions, lack of vendor maturity and lack of researcher maturity. Thought needs to be given to the impact of all disclosure.

The study sets out the challenges of disclosure and defines a series of good practice approaches in this space. This moves towards responsible disclosure rather than full disclosure.

The full slides from the presentation can be found at: https://www.terena.org/activities/tf-csirt/meeting47/C.Ciobanu-Vulnerability-disclosure.pptx.

7. BT Team Update – Daniel Porter and Graham Austin, BT

Daniel Porter and Graham Austin gave a general team update from BT.

BT identified the major challenge as recruiting the right staff, which can be difficult to find. Work has included significant training and building a dedicated team for incident response and management.

Slides from this presentation are not currently available.

8. To share or not to share, that's just one question - *Jean-Paul Weber, GOVCERT.LU*

Jean-Paul presented on a range of practical issues faced by GOVCERT.LU in managing information sharing. This covered the range of audiences, terminology, groupings and workflow. The

connotation of each individual event can also change the focus of the definition. Jean-Paul asked for contributions from those facing similar issues.

The full slides from the presentation can be found at: https://www.terena.org/activities/tf-csirt/meeting47/J.P.Weber-GOVCERT.LU.pdf.

9. CSIRT.CZ from 2011 to 2016 – Zuzana Duračinská

Zuzana gave an overview of CSIRT.CZ and how the team has grown in the past five years of operations. The team as originally established with CESNET in 1998 and moved to CZ.NIC in 2010. The team became accredited in 2011. The team has focused on active project work to support incident response, security and information sharing – including the development of Malicious Domain Manager, Turris, PROKI and Web Scanner.

The full slides from the presentation can be found at: https://www.terena.org/activities/tf-csirt/meeting47/Z.Duracinska-csirt.cz.pdf.