26 January 2014

Reference/Subject: Minutes: 44th 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 44th TF-CSIRT Meeting

26th January 2014, Las Palmas, Gran Canaria
This meeting was hosted by IRIS-CERT

Table of Contents

1. Introductions, TI-Update and TF-CSIRT Updates

Baiba Kaskina welcomed attendees to the meeting and thanked the local host and sponsors.

Certificates were awarded to 5 teams that have recently been certified: (list). A brief overiew of the status of TI was given and Nicole Harris gave an update on the vote on Trusted Introducer Charging Models undertaken in the Closed Meeting. Accredited Teams voted to approve the fee increase for accredited teams to 1200 euro per annum.

ACTION20150126-01 GÉANT Association to inform members of the price increase via a formal notification.

Nicole Harris also briefly outlined that a full review of the TF-CSIRT portfolio and its current set-up will be undertaken before the next procurement phase. This will look at all elements

of the services offered. Members of the community will be invited to participate in a working group.

ACTION20150126-02 Nicole Harris to invite TF-CSIRT members to participate in a working group looking at the future of TF-CSIRT services.

Nicole Harris reminded participants to sign-up to the TF-CSIRT mailing list at: https://www.terena.org/mailinglists.php?list=tf-csirt@terena.org.

2. Actionable information for security incident response, Cosmin Ciobanu, ENISA

In 2014 ENISA together with CERT Polska undertook a study on actionable information for security incident response with input from a expert group. Cosmin Ciobanu gave an update on this study and the information found in this process.

Further information on the study, its outcomes and the recommendations can be found on the ENISA website: https://www.enisa.europa.eu/activities/cert/support/actionable-information/actionable-information.

Further information can be found in the presentation slides: (https://www.terena.org/activities/tf-csirt/meeting44/Las_palmas_actionable_information.pdf).

3. Turris Outcomes, Zuzana Duracinska, CSIRT.CZ

Zuzana Duracinska gave an update on Project Turris, which was first presented at the 43rd TF-CSIRT meeting. The project started in 2013 and is a project looking at SOHO (small office, home office) routers and improving security in such environments. The project has rolled out approximately 1000 routers with adaptive firewalls and anomaly detection. End goal is to have just over 2000 routers rolled out for the research aspects of the project.

The project is now looking at Turris Lite, taking inspiration from Raspberry Pi – providing a small energy efficient device so in effect a Raspberry Pi for network and server solutions.

Further information can be found in the presentation slides: (https://www.terena.org/activities/tf-csirt/meeting44/Turris_26_01_Las_Palmas.odp).

4. RTIR/Abusehelper, James McLoughlin & Lee Harrigan, JANET

James McLoughlin gave an update on the RTIR Working Group. James is responsible for the CSIRT infrastructure at JANET and any appropriate customization that goes along with that. RTIR 3 was recently released with little fanfare and the RTIR working group has become somewhat inactive. There is still a lot of interest in the area within the community with over 21 teams actively using RTIR. James asked for teams that are interested in reviving the working group to discuss the issue further with him.

Further information about the RTIR group can be found at: https://www.terena.org/activities/tf-csirt/rtir.html.

Lee Harrigan gave an overview of AbuseHelper work at JANET. For JANET this is currently a part manual part automated process. Some of the issues are complicated by the fact that a response is always asked for even when it wasn't needed and the working hours of the JANET CSIRT. A customer survey pointed towards a preference for a change towards automation for some report types.

A meeting on RTIR+ other relevant tools should be coordinated at the next TF-CSIRT meeting.

ACTION20150126-03 Nicole Harris to invite TF-CSIRT members to express their interest in reviving the RTIR working group.

Further information can be found in the presentation slides: (https://www.terena.org/activities/tf-csirt/meeting44/automation-wg_handout.pdf) and (https://www.terena.org/activities/tf-csirt/meeting44/TF-CSIRT%20RTIR%20and%20AbuseHelper.pdf).

5. Firewall on Demand, Evangelos Spatharas, GÉANT Association (Cambridge)

Evangelos Spatharas gave an update on the Firewall on Demand work being addressed by the GÉANT project. The purpose of the work is to address DDoS attacks via a simple to use tool (web GUI). The work is based on standards as specified through RFC5575.

Further information can be found in the presentation slides: (https://www.terena.org/activities/tf-csirt/meeting44/Firewall%20on%20Demand_Las_Palmas.pdf).

6. CyberROAD, Przemek Jaroszewski, CERT Polska/NASK

Prezemek Jaroszewski gave a brief presentation on the FP7 project CyberROAD. It is intended to be a technological, social, economic and political snapshot regarding cyber-crime and cyber-terrorism. This presentation is intended to make all participants aware of the project and Prezemek intends to report on the outcomes at the next TF-CSIRT meeting. Partners from the community are well represented in the project.

Further information can be found in the presentation slides: (https://www.terena.org/activities/tf-csirt/meeting44/20150126_TFCSIRT_CyberROAD.pdf).

7. PSNC and PIONIER: the next TF-CSIRT meeting hosts. NREN, research, applications and security, Tomasz A. Nowocień, Pionier-CERT/PSNC

Tomasz Nowocień gave an update on the work of PSNC and the role of CSIRT activities in the NREN space. Tomasz also welcomed attendees to the next TF-CSIRT meeting, to be held on 21st – 22nd May in Poznan, Poland.

Further information can be found in the presentation slides: (https://www.terena.org/activities/tf-csirt/meeting44/Zaproszenie45TFCSIRT.pdf).

8. Action Summary

ACTION20150126-01	GÉANT Association to inform members of the price increase via a formal notification.
ACTION20150126-02	Nicole Harris to invite TF-CSIRT members to participate in a working group looking at the future of TF-CSIRT services.
ACTION20150126-03	Nicole Harris to invite TF-CSIRT members to express their interest in reviving the RTIR working group.