20 May 2015

Reference/Subject: Minutes: 45th 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 45th TF-CSIRT Meeting

21st – 22nd May 2015

This meeting was hosted by Pionier-CERT/PSNC.

Table of Contents

1. TF-CSIRT Open Meeting - Welcome from Chair, *Baiba Kaskina*

Baiba Kaskina welcomed attendees to the meeting and thanked the local host and sponsors. The minutes of the last meeting were accepted as an accurate record of the meeting.

2. Overview of the TI Review Working Group, *Nicole Harris*

Nicole Harris gave an overview of the planned TI Review and the requirements for the working group required to carry out the review. Participants were invited to volunteer to participate in either or both phases of the working group. Attendees pointed out that it would be useful to get inputs on how much certain tools are being used ahead of the WG starting. This should be from TI records and from surveying the community. A full stakeholder analysis will also be useful.

The full presentation can be viewed online at: https://www.terena.org/activities/tf-csirt/meeting45/TI-review-ToR.pptx.

3. Trusted Introducer Update, *Miroslaw Maj*

Miroslaw Maj gave an overview of the current Trusted Introducer service and trends in TI membership. TI has seed a significant rise in the number of teams from the Czech Republic. Three specific sectors are being tracked: Research and Education, Government, National and Military and Commercial. TI has 10 team that are currently certification candidates.

The full presentation can be viewed online at: https://www.terena.org/activities/tf-csirt/meeting45/TI-update-Poznan-public.pdf.

4. CSUC-CSIRT, Jordi Guijarro

Jordi Guijarro gave an presentation on behalf of CSUC-CSIRT. CSUC- CSIRT is a recently accredited team based in Spain. CSUC is the new Catalan Universities services consortium (but includes all research organisations). It acts predominantly as a cloud service but includes all IT services, library services etc.

CSUC-CSIRT use SmartxAC Platofrm for traffic monitoring and analysis. It is netflow focused and a low cost solution.

CSUC-CSIRT is very close to the university and has close links with students studying for a Masters in Security Technologies. They are making efforts to show the daily life of security incident management to the students. Jordi asked what other accredited teams are doing to support students and ensuring that students are have some experience of dealing with real life scenarios.

The full presentation can be viewed online at: https://www.terena.org/activities/tf-csirt/meeting45/CSUC-Poznan.pdf.

5. Impact of ENISA's action with regard to CERTs, *Lionel Ferette*

ENISA contracted Deloitte to wnsure that this was an independent reviw. The review was based firstly on legislative and regulatory issues (EU Cybersecurity Strategy, ENISA Regulation, Work Programmes and proposed NIS Directive) and secondly on operational issues (baseline capabilities, capacity building, support for cooperation with law enforcement agencies).

The main findings for the study was that training was the number one most appreciated service and that stakeholders generally want ENISA to carry on doing what they are currently doing. One area that needs more work is in advertising what is available and to generally make more noise about the services available and the success of these documents.

ENISA has a new project plan for this year, which introduces a new aspect in terms of CyberEurope Exercises. They are also looking for people to participate in an expert group for future reviews.

The full presentation can be viewed online at: https://www.terena.org/activities/tf-csirt/meeting45/20150521-ENISA-Lionel.pdf.

6. Checkpoint, Jaroslaw Prokop

Checkpoint is a commercial company offering security services to the community since 1993. Jaroslaw Prokop gave an overview of the work carried out by Checkpoint to manage DDoS attacks and to support organisations, helping them build security best practice in to daily workflows.

The full presentation can be found online at: https://www.terena.org/activities/tf-csirt/meeting45/TF-CSIRT-Check-Point.pdf.

7. Anomaly detection, graph databases and NetFlows - from SECOR project perspective, *Maciej Milostan*

Maciej Milostan gave a presentation on aomaly detection as part of the SECOR project, which intends to develop methodology allowing the construction of next generation IDS/IPS systems with built-in artificial intelligence, capable of performing signature-less intrusion and anomaly detection. The aim of the project is to raise the level of protection of infrastructure used for science, including a move beyond signature based systems to address threats. PSNC are implementing a SECOR prototype looking at both system level and network level events.

The full presentation can be viewed online at: https://www.terena.org/activities/tf-csirt/meeting45/Milostan-TF-CSIRT.pdf.

8. NSHaRP Security Architecture Upgrade, *Wayne Routly*

Wayne Routly from GÉANT gave an update on the NSHaRP Security Architecture Upgrade. GÉANT has recently completed a service upgrade of NSHaRP - Network Security and Response Process. NSHaRP is a GÉANT maintained process that provides a complete security solution. The idea is to provide an extension to the tools used by NREN CERTs to support the GÉANT network. The process now uses OTRS to manage tickets and integrates firewall on demand. Flowmon Is used as the core monitoring tool and has been tested with five European NRENs.

The full presentation can be found online at: https://www.terena.org/activities/tf-csirt/meeting45/TF-CSIRT%20presentation%20NSHaRP_v3.pdf.

9. Evolution of MISP, *Raphael Vinot*

Raphael Vinot gave an update on MISP (Malware Information Sharing Platform) at CIRCL. There are currently around 150,00 attributes in MISP for the private sector from 117 international companies. MISP is available on github: https://github.com/MISP/MISP/issues.

MISP is looking at providing features for community-based sharing of events. CIRCL has provided a version to FIRST that can be accessed and used by FIRST members: https://misp.first.org/users/login.

The full presentation can be found online at: https://www.terena.org/activities/tf-csirt/meeting45/circl-presentation.pdf.

10. intelmq , Aaron Kaplan

Aaron Kaplan gave a demonstration of intelmq. intelmq is a new approach adopted to improve on some of the issues with AbuseHelper. A group of CERTs got together and worked on a "summer of sprint" in 2014 based on a keep it simple approach.

11. IP address certification (RPKI), *Mirjam Kühne and* Ivo Dijkhuis

Mirjam Kühne and Ivo Dijkhuis from RIPE NCC have an update on the RPKI work being carried out by RIPE. At a previous meeting, Mirjam reported that RIPE had seen an increase in IPv4 hijacking. This has now slowed down but the number of IPv4 transfers has significantly increased. RIPE is looking at resource certification to help support this process so that organisations can prove that they are the

legitimate owners of prefixes. The information is stored in the whois database. In order for this to be signed effectively, all certificates and ROAs are published in a repository and available for download. This process has been in production since 2011 and several open source tools are available to validate ROAs.

The full presentation can be found online at: https://www.terena.org/activities/tf-csirt/meeting45/TF-CSIRT45-RPKI-150521.pdf.

12. TF-CSIRT Geographical Scope, *Baiba Kaskina*

Baiba Kaskina gave an overview of proposals from the TF-CSIRT SC regarding the geographical scope of TF-CSIRT. The current Terms of Reference and TI contract do not restrict the scope of operations to Europe. For teams outside of Europe the teams must provide documentation in English and there is a higher charge for accreditation.

Trusted Introducer currently considers three sets of regions:

1. Europe (RIPE NCC Constituency).
2. Countries around the Mediterranean.
3. The rest of the world.

The Steering Committee proposes that we deal with those in Europe (defined as above) as usual and treat regions 2 and 3 alike. Where the team is a member of other existing regional organisations, the TI team will consult with these regional organisations before accepting the team application.

Attendees noted that different membership criteria already exist in different initiatives so this is another good reason to open up TF-CISRT and that we would benefit from strengthening relationships with other regions. It was felt that TI shouldn't actively "poach" other region's members but be willing to engage with teams that approach us. It was also felt important that meetings should stay in Europe and that this should be explicit within the Terms of References. Attendees agreed that managing trust is not related to geographical scope but community size.

ACTION20150521-01 Nicole Harris to review the Terms of Reference in light of these approved changes to the geographical scope.

ACTION20150521-02 TF-CSIRT SC to prepare a document describing the process for accepting non-European CSIRTS that can be shared with other regional organisations.

The full presentation can be found online at: https://www.terena.org/activities/tf-csirt/meeting45/TF-CSIRT-geographical-scope.pptx.

13. Action Summary

ACTION20150521-01	Nicole Harris to review the Terms of Reference in light of these approved changes to the geographical scope.
ACTION20150521-02	TF-CSIRT SC to prepare a document describing the process for accepting non-European CSIRTS that can be shared with other regional organisations.