ENISA’s Step-by-Step Guide to Setting up a CERT/CSIRT and its role in Establishing new CSIRTs in CIS Countries

Dr Jacek Gajewski
CEENet, ENISA PSG
What is CEENet?

Central and Eastern European Networking Association (CEENet) is an international association of 25 national academic networks (NRENs) from CEE and CIS countries.
What is CSIRT?

• Computer Security Incident Response Team is the service organization that is responsible for receiving, reviewing, and responding to computer or network security breach.

• Often they are also complete network security service providers, including preventative services such as alerts, security advisories, trainings, awareness raising and security management services.
CSIRT creation project

• In 2007 CEENet started project to create CSIRTs in CIS & CEE
  – AF, AM, AZ, GE, KG, KZ, TJ, TM, UZ
  – BY-MD-UA,
  – AL-BG-MK (just started)
  – JO, EG, TN, AL, MN, MT (planned)
• CSIRTs were usually created as sub-structure of Academic Network (or NGO, e.g. ISOC)
CSIRT creation project

Each newly created CSIRT got free „starting kit”:  

- Equipment bundle:  
  CERT Server with system of incident handling software, Staff working station, router, switch, software, multi-function printer, shredder, manuals)

- Training of 1-3 CERT officers (based on ENISA’s Step-by-Step guide and TRANSITs material)

- Small stipend for CERT officers in initial period of CSIRT operation
ENISA’s Step by Step Guide

- ENISA has created a „A Step-by-Step Guide on how to set up a CSIRT”, which on 85 pages contains detailed instructions how to set up and run CSIRT. This Guide existed in many languages (EN, FR, DE, ES)

- For the usage in CIS countries CEENet has translated this guide to Russian (available from ENISA)
Пошаговое руководство по созданию CSIRT

Включая примеры и контрольные таблицы
в форме проектного плана.

Приложение
A. Список дополнительной литературы
B. Список CSIRT-сервисов
C. Примеры
D. Образцы материалов CSIRT-курсов
Guide in Russian

1. О данном руководстве
2. Правовое уведомление
3. Благодарности
5. Общая стратегия планирования и создания CSIRT
6. Разработка бизнес плана
7. Продвижение бизнес плана
8. Примеры операционных и технических процедур (делопроизводство)
9. Обучение CSIRT
10. Упражнение: создание рекомендаций
11. Заключение
12. Описание Плана Проекта
Current status

Trainings by experienced trainers from CERT-Polska and CERT-Surfnet started in 2006 with English written TRANSITs material;
From 2007 ENISA’s Guide in Russian is used and trainers from AZ and GE are included.
Typically 2-5 CERT officers/NREN have been trained during 5 sessions 2xTbilisi, Vilnius, Warsaw, Skopje)

CERT-Polska is:
- monitoring their activities, on-line support
- introduces them to international fora
Current status

- reports (Web-site set-up, plan of activities, statistics, dissemination, etc.) received from ÂM, BY, MD, AZ, GE, UA, UZ

- problems in AF, KG, KZ, TJ, TM – nature of their problems is being studied
CERT-GE is part of GRENA. As there were no other CERT teams in Georgia, during recent events CERT-GE undertook obligation to operate as national CERT, worked two weeks in 24h mode and coordinated attacks mitigation.

CERT-GE contacted Georgian ISPs and other organizations, created a mailing list in order to facilitate communication and exchange of all needed information.

As this information was huge and geographical distribution of attacks was quite wide, it was impossible to make quick analysis and proper reaction. CERT-GE contacted CERT-Polska (Poland) which offered its help in preventing and filtering attacks; they distributed information on attacks to more than 180 CERT teams and other security related bodies all over the world. Two members of CERT-EE arrived to Tbilisi to help on place.

This example demonstrates that the most important actions for handling incidents are quick information exchange and international cooperation between CERTs and other organizations involved in cyber security.
Contacts to CERT Georgia

• E-mail: cert@cert.ge
• Tel/Fax.: +995 32 251440
• Web-page: http://www.cert.ge

Mailing list was created for GRENA users certusers@cert.ge
To report an incident, you can e-mail us or use the online form.

RFC 2350

Current description of the CERT Georgia team, compliant with RFC 2350 Expectations for Computer Security Incident Response can be found here.

www.cert.ge
Services Provided by CERT Georgia

• Information about new viruses, worms and spams are sent regularly (2 times per week) to GRENA users.
• Monitoring of the traffic by Netflow is conducted and users with traffic problems are informed.
• In case of problems our users are contacting us via e-mail or phone.
Tbilisi State University Downlink

Graph - Zoom Mode - Netflow External TSU Traffic Services [down] - Zoom

Graph showing Netflow External TSU Traffic Services [down]

- Web [INET] Current: 344.59 k Average: 514.53 k Maximum: 2.18 M
- Web [GRENA] Current: 128.59 k Average: 1.06 k Maximum: 6.35 k
- FTP [INET] Current: 0.00 k Average: 13.40 k Maximum: 1.22 k
- Mail [INET] Current: 2.15 k Average: 1.57 k Maximum: 57.73 k
- Mail [GRENA] Current: 2.62 k Average: 2.93 k Maximum: 275.67 k
- Eume [INET] Current: 1.88 k Average: 77.85 k Maximum: 6.60 k
- Eume [GRENA] Current: 11.41 k Average: 8.06 k Maximum: 68.21 k
- Netbios [INET] Current: 0.00 k Average: 0.00 k Maximum: 0.00 k
- Netbios [GRENA] Current: 0.64 k Average: 249.31 k Maximum: 2.78 k
- SSL [INET] Current: 22.28 k Average: 42.10 k Maximum: 251.86 k
- SSL [GRENA] Current: 0.03 k Average: 5.47 k Maximum: 1.36 k
- DNS [INET] Current: 10.95 k Average: 8.35 k Maximum: 23.29 k
- DNS [GRENA] Current: 2.14 k Average: 1.15 k Maximum: 3.25 k
- Other Current: 12.35 k Average: 28.44 k Maximum: 423.95 k
CERT in Turkmenistan

Supreme Council on Science and Technology
under the President of Turkmenistan (SCST)
CERT-TM

• CERT is not separate department.
• (some) Functions of CERT are implemented by local administrators in each universities.
• Technical department of SCST takes care of stability of the network and carried out training of technical university staff.
• SCST technical department helps local administrators to find and manage problems.
• CERT-AM

• CERT-AM (run by ISOC-AM) has wide range of services:
  – Alerts and Warnings
  – Incident Handling
  – Security Audits or Assessments
  – Intrusion Detection Services
  – Security-Related Information Dissemination
  – Disaster Recovery Planning
  – Security Consulting
  – Awareness Building
  – Education/Training

• Memorandum of Understanding was worked out. The memorandum was signed by ISPs and other IT companies, which agreed to cooperate with CERT AM.
• **Host organization**: AzNET Project (School Network)

• **Constituency**: schools and universities (incl. AzRENA) - total 80 clients

• **Services**: incidence handling, incidence response support, incidence response on site, configuration and maintenance of Security, trainings

• **Area**: Baku, Gandja, Mingachevir, Goranboy, Hajigabul

• MinICT has established Internet agency against hackers and requested AzNETs expertise in establishing tracking system for handling incidents

• National level CERT is planned to be started by MinICT
Conclusions

• Starting new CERT needs ca. 2 year „incubation period”
• Training materials should be in local language
• International cooperation of CERTs is the important factor for their effectiveness
• Still many countries without CERT… Task for ITU?
THANK YOU!

Jacek Gajewski
Gajewski (at) CEENet (dot) org