

ENISA

Update December 2012

Supporting the CERT and other operational communities

Contact: opsec@enisa.europa.eu

Supporting the CERT and other operational communities

Supporting the CERT community

ENISA Annual CERT workshops focus on national and governmental CERTs preparedness and response capabilities

Losses comparison

| Parameter | Internet | | | |
|----------------------------------|----------|-------|---------|---------|
| | Spain | Virus | DDoS | Botnet |
| SLE (Single Loss Expectancy) | 21.70 | 62.90 | | |
| ARO (Annual Rate of Occurrence) | 0.2 | 2 | 0.1 | 0.1 |
| ALE (Annualized Loss Expectancy) | 6.471 | 4.750 | 125.979 | 151.363 |
| AEI (Annualized Loss Expectancy) | | | 14.155 | 8.124 |
| TALE (Total ALE) | | | 201 | 122.619 |
| | | | 154.973 | |

New Exercise material 2012

- Technical trainings for CERTs
- Handbook for teachers
- Toolset for students
- SW ready to use from our website: www.enisa.europa.eu/activities/cert/support

FIRST – to improve CERT capabilities

TRANSITS framework: support the basic and advanced training courses for CERTs

Cross-communities Support

INTERPOL Atomic exercise 2012

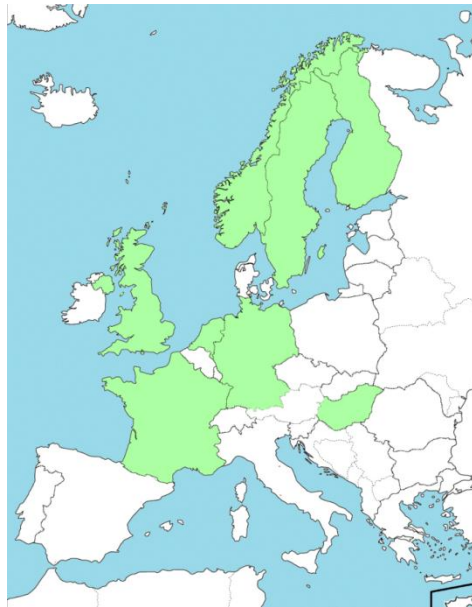
ENISA-EUROPOL joint workshop: “Addressing NIS aspects of cybercrime”

EU FI-ISAC exercise for CERTs, LEA and banks

CEPOL courses: (operational security unit supports cyber workshops for police)

National/governmental CERTs the situation has changed...

in 2005



**ESTABLISHED
IN 2005:**
Finland
France
Germany
Hungary
The Netherlands
Norway
Sweden
UK

in 2012



Baseline capabilities of n/g CERTs

- Initially defined in 2009 (operational aspects)
- In 2010 Policy recommendations drafted
- In 2012 ENISA continues to work on a harmonisation together with MS
- **Status Report 2012**
- National/governmental CERT capabilities – updated recommendations 2012

ENISA's new CERT interactive map:

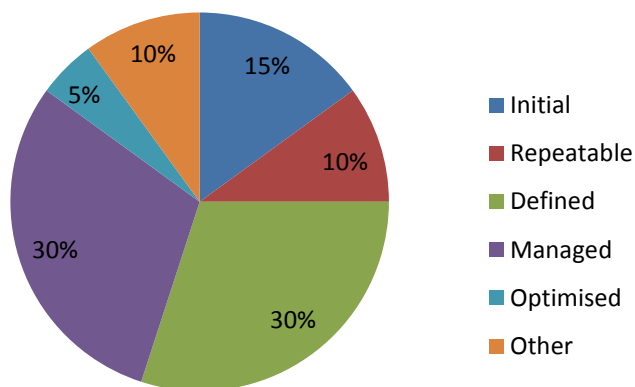
<http://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map>

Status Report 2012

Some initial statistics...

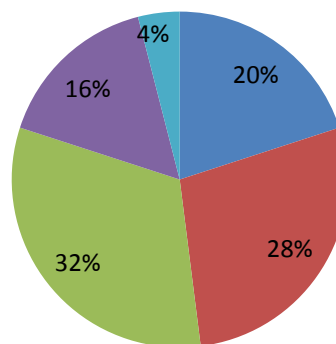
Total: 45 responses to the questionnaire (25 from n/g CERTs; 20 from other CERTs and other stakeholders)

Self-Assessment of the Maturity Status of National / Governmental CERTs



Years of Operation of National / Governmental CERT

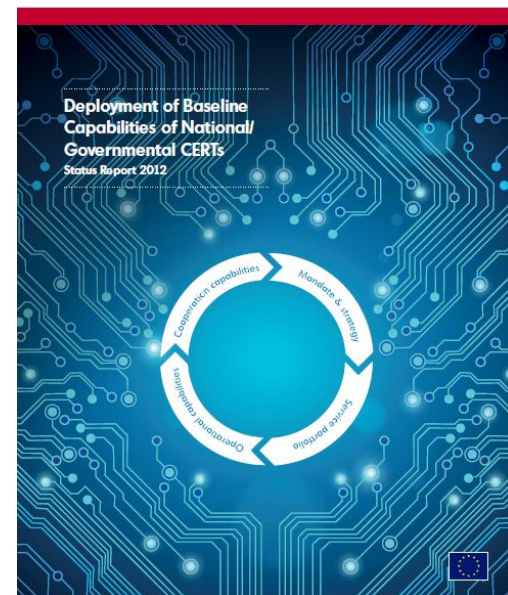
■ Up to one year ■ 1-2 years ■ 3-5 years
■ 6-8 years ■ Over 8 years



Interviewed teams assessed themselves as either governmental or national/governmental CERTs indicated the years of operations between: **4 months and 11 years.**

(France, Germany, Norway, Hungary, Denmark, Sweden, Spain, Ireland, Latvia, Czech Republic, Slovakia, Romania, CERT-EU)

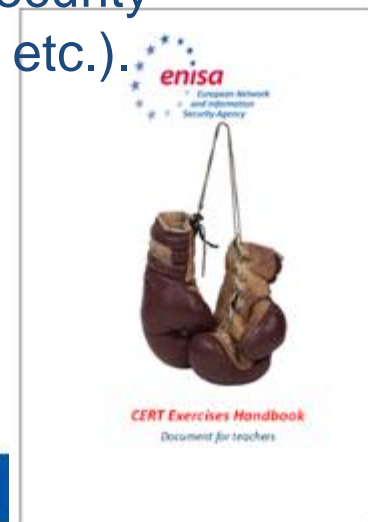
<http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities>



CERT Exercises and training material / news in 2012!

- ENISA CERT training/exercise material, used since 2009, was extended to host 23 different topics and training exercises including:
 - technical aspects (mobile devices forensics based on Android emulator, investigation of DDoS traces, netflow analysis, deployment of Honeypots etc.);
 - organisational aspects (developing CERT infrastructure, establishing external contacts etc.);
 - operational aspects (triage & basic incident handling, automation in incident handling, calculating cost of information security incident and its return on security investment (ROSI) etc.).
- Additionally a Roadmap was created to answer: how could ENISA provide more proactive and efficient CERT training?

<http://www.enisa.europa.eu/activities/cert/support/exercise>



EISAS 2012 – Large scale pilot

- ★ European Information Sharing and Alert System introduced in COM(2006) 251: “Communication on a strategy for a Secure Information Society”
- ★ In 2012: Pilot Project for collaborative Awareness Raising for EU Citizens and SMEs
 - ★ Gathered n/g CERTs, governmental agencies and private companies in 6 different MS
 - ★ Cross-border awareness raising campaign
 - ★ Reached more than 1.700 people in 5 months
 - ★ Social networks involved
- ★ In 2013: EISAS Deployment study

http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder

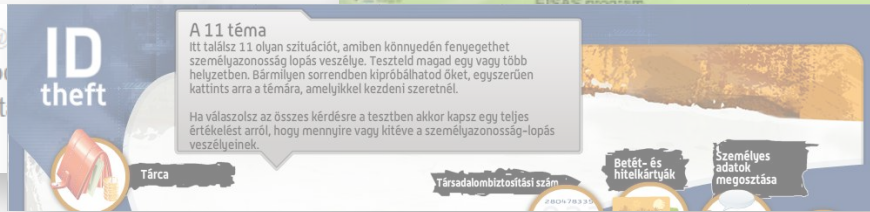
Ostatnio w ramach projektu EISAS ukazał się pakiet materiałów uświadamiających o podstawach bezpieczeństwa w sieci.
Oto pierwszy z nich:



(1/5) "Jak funkcjonuje botnet", "Jak chronić się przed władcami"
www.jak11.knu.edu.pl
Znaczną część komputerów używanych w gospodarstwach domowych jest...
Like Comment Share
Jarek, Dżuk and Karolina Jedralioka-Nemczuk like this.
Write a comment...



Fundació CESICAT @
Al web bit.ly/PAGpo5 p
n'estàs amb la seguretat
Expand

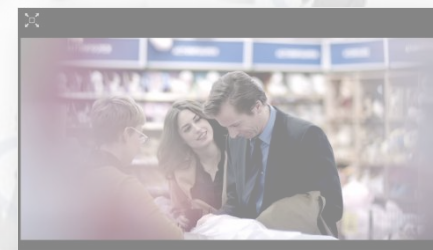


ID theft

A 11 téma
Itt találasz 11 olyan szituációt, amiben könnyedén fenyegethet személyazonosság lopás veszélye. Teszteld magad egy vagy több helyzetben. Bármilyen sorrendben kipróbálhatod őket, egyszerűen kattints arra a témára, amellyel kezdeni szeretnél.

Ha válaszolsz az összes kérdésre a tesztben akkor kapsz egy teljes értékelést arról, hogy mennyire vagy kitéve a személyazonosság-lopás veszélyeinek.

Tárca
Társadalombiztosítási szám
Betét- és hitelkártyák
Személyes adatok megosztása



Cybercrime project 2012

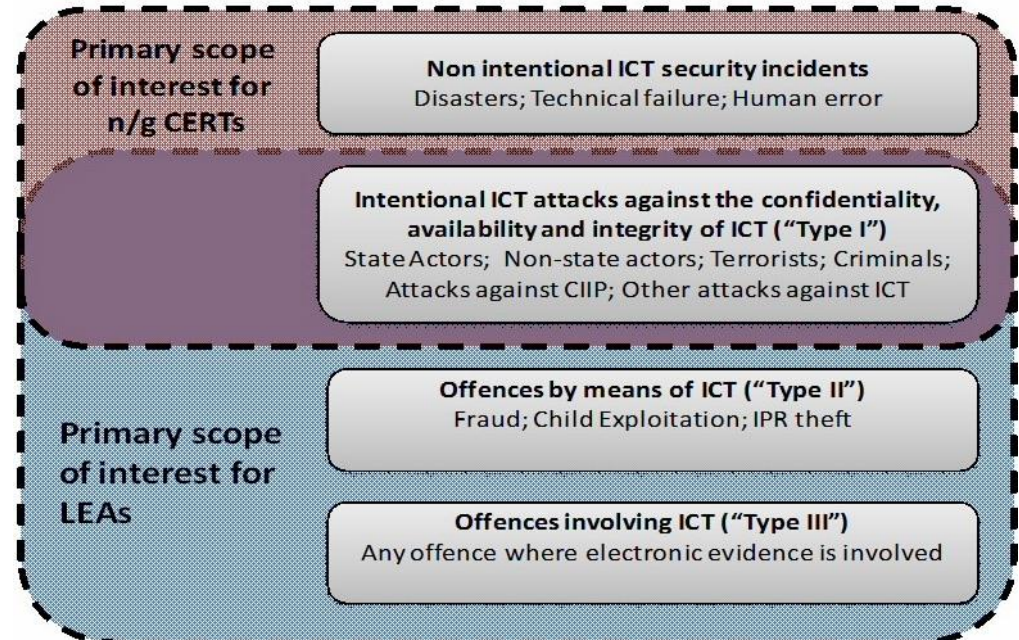
★ Main goals:

- ★ Define key concepts
- ★ Describe the technical and legal/regulatory aspects of the fight against cybercrime
- ★ Compile an inventory of operational, legal/regulatory and procedural barriers and challenges and possible ways to overcome these challenges
- ★ Collect existing good and best practices
- ★ Develop recommendations

★ Focus on CERT-LEA cooperation

★ Differences:

- ★ Definitions cybercrimes/attacks
- ★ Meanings of sharing
- ★ Character of the organizations
- ★ Objectives
- ★ Types of information
- ★ Directions of requests
- ★ ...



ENISA, CERTs and other players in the area of cybercrime prevention

7th ENISA workshop 'CERTs in Europe'

- Part I. - > technical training for n/g CERT experts
 - hands-on training exclusively for the EU national/governmental CERT teams
 - 2 days of deep technical dive into topics like botnets, mobile malware and other interesting topics.
- Part II. - > 2nd time jointly organised with **EUROPOL** on 16/17 October
 - Goal: to facilitate better cooperation between n/g CERTs and LEA in MS.
 - Continuation of the first workshop (6th ENISA workshop in 2011)
 - Interactive sessions – n/g CERTs and LEAs group exercise
 - ***Final report will be published soon!***

<http://www.enisa.europa.eu/activities/cert/events/7th-cert-workshop-partII>

European FI-ISAC (European n/g CERTs, LEA and financial institutions)

- ENISA continuously supports this group since the beginning of its operations in 2008

FIRST/LECC-SIG (global working group; CERTs and LEA)

- ENISA is a member of this WG from 2012