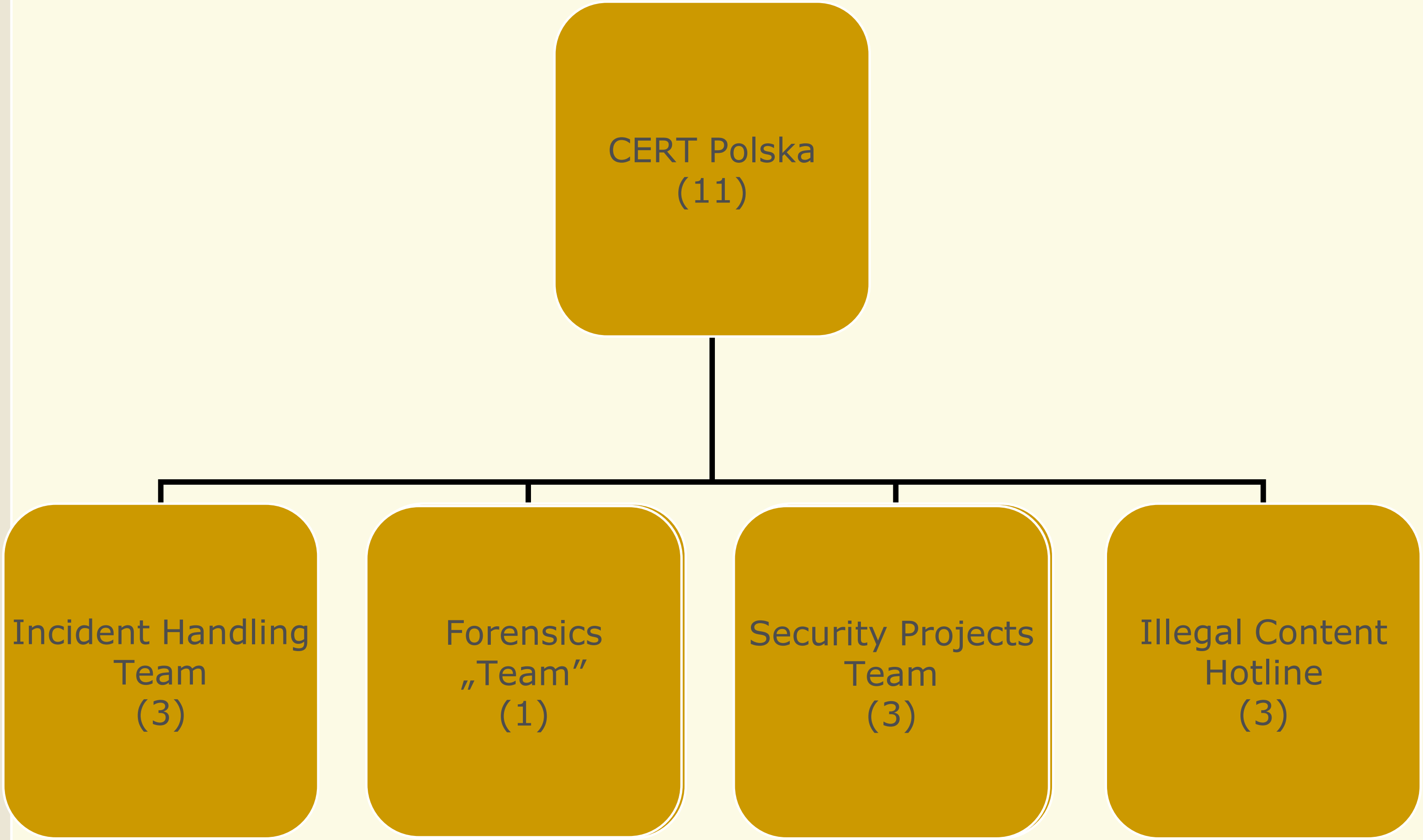
CERT Polska

expiriences in running national CSIRT

Some history

- 1996 – establishing CERT NASK
  - Visit to DFN-CERT to learn best practices
- 1997 – joining FIRST (sponsored by DFN-CERT)
- 2000 – extending the formula of our IRT
  - new roadmap to introduce new project for polish constituency
  - Changing the name to CERT Polska
- 2001 – joining TERENA TF CSIRT
- 2002 – Trusted Introducer Accredited Team

CERT Polska within NASK



CERT Polska
(11)

Incident Handling Team
(3)

Forensics „Team”
(1)

Security Projects Team
(3)

Illegal Content Hotline
(3)

International activities

1996

- Team established

- FIRST (Forum of Incident Response and Security Teams)

http://www.first.org/

- TERENA TF-CSIRT (Trans European Research and Academic Networks Association – Task Force Computer Security Incident Response Teams)

http://www.terena.nl/tech/task-forces/tf-csirt/

- Trusted Introducer (Accredited Team)

http://www.ti.terena.nl/

CERT Polska activities

- Incident handling (constituency: .pl)
- Content illegal incident handling
- (inter)National level security projects
- Assistance in establishing new CSIRT
- National cooperation of CSIRT
- Awareness building
- Working with LEA

INCIDENT HANDLING

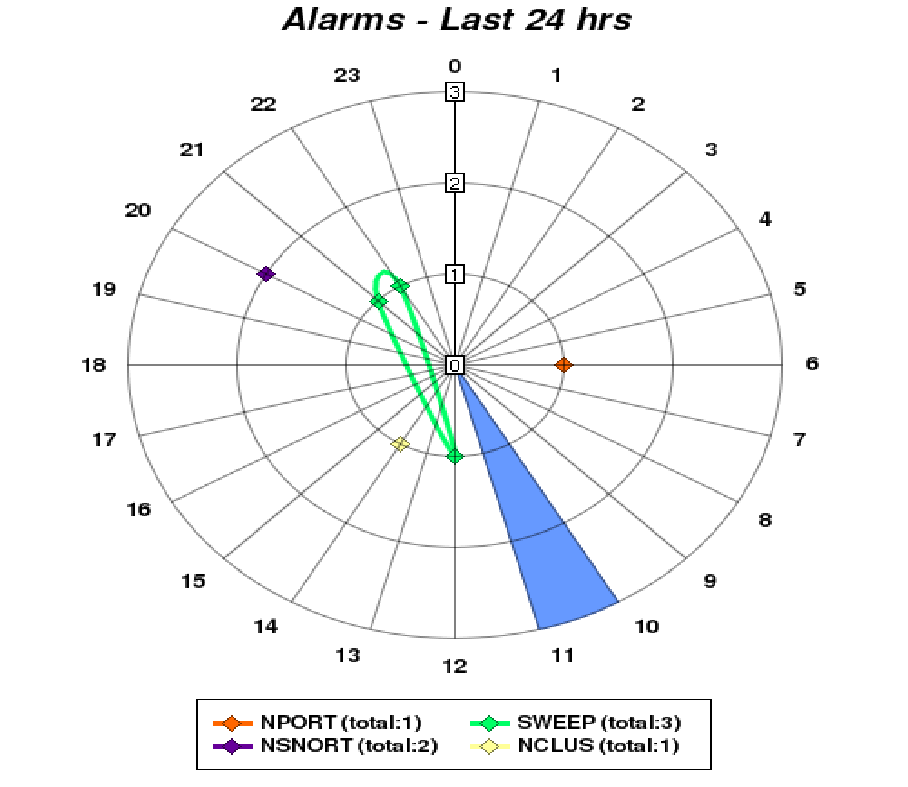
- Contact point for .pl constituency
- Hub for automatic incident handling
  - Technical support
- Representative in many IT foras
  - FIRST
  - ENISA
  - International initiatives (e.g. ASEM cooperation)

ILLEGAL CONTENT INCIDENT HANDLING

- Organization of Dyżurnet.pl hotline
- Technical support for illegal hotline in Poland
  - Incident handling expiriences
    - Polish hotline
    - Internation hotlines (INHOPE)
  - Research on new illegal content techniques
  - Usage for CERT’s communication channels for hotline purposes

Security projects, initiatives

- **ARAKIS** (Distributed Internet Based Early Warning System)
- **HONEYSPIDER** (joint project with GOVCERT.NL and SURFnet-CERT)
- **WOMBAT** (European 7th Framework Programme Project)
- SPOTSPAM (technical support for legal actions against spammers



Security projects, initiatives

- **CLOSER** (establishing and coaching new CSIRT teams in CEE region)
- **ABUSE-FORUM** (cooperation between Polish security teams – ISP representatives)
- Trainings for new teams (Poland)

Assistance in establishing new CSIRT

- Polish Telecom CSIRT (TP CERT)
- Polish military CSIRT (CIRC capability)
- Polish governmental CSIRT (CERT.GOV.PL)
  - Established in 2008
  - Trained by CP
  - Technically based on ARAKIS system

National cooperation of CSIRT

- ABUSE FORUM
  - Established in 2005
  - Based on the international expiriences
  - More then 10 „incident handling capability” teams
  - Regular (3/year) meetings (plus mailing list)
  - Organizational issues and technical „projects”
    - Blackholing
    - Incident distribution

Awareness building

- The oldest IT security conference in Poland – SECURE
- Media expert contact for IT security news commentary
- www.cert.pl serwis (kind of corporate blog starting in June)
- enisa.pl website
- Partner in Safer Internet Action Plan for AWARENODE in Poland

Working with LEA

- Cooperation with Polish Police Academy
- Forensics expert in IT related cases
- IT security consultant

Conclusions

*Whatever you are – governmental CSIRT or national level CSIRT – **be proactive in filling the gaps** on CSIRT services for „national" constituency*

*Find and cooperate with others to **develop better services** and **handing over responsibilites***

Thank you.

Mirek Maj

mirek.maj@cert.pl

info@cert.pl