Computer Security Incident Response Team Slovakia
Agenda

• Why, Where, What...
  
  – Establishment of CSIRT.SK
  
  – Mission statement and goals
  
  – Projects and Activities
MISSION STATEMENT & GOALS
Provide best in class support for all security related issues.
• Response to the IS incidents

  – cooperation

    • Owners and Providers of impacted parts of CII

    • ISPs & Telecommunication Operators

    • Other public bodies
      – police, investigators, courts
• Raising awareness in the field of IS
  – seminars, trainings
  – best-practices & more

• Cooperation and representation
  – international organizations and peers
• Create a National Point of Contact
  – National and international warnings

• Provide services related to IS
  – Reactive / Proactive

• Cooperation with other CSIRT/CERT teams
• Monitor and Gather Information
  – Level of IS in Slovakia
  – Current threats
  – Vulnerabilities and Risks

• Educate and raise awareness
  – Employees of public administration
  – General public
ESTABLISHING A NATIONAL CSIRT
• Political will

• Legal framework
  – National strategy for Info Sec. under No. 570/2008
    • Information Security stuff
  – CSIRT.SK adopted by Gov. decree No. 479/2009
• Ministry of Finance
  – Provides various types of support to CSIRT.SK

• CSIRT.SK
  – as an independent department of DataCentrum
  – on July, 1\textsuperscript{st} 2009
  – as the first CSIRT/CERT in Slovakia
  – as a \textit{national / governmental} CSIRT
Constituency

- No defined legal framework yet.
Constituency

• CSIRT.SK provides
  – CIIP
  – Services for the Slovak government
  – Particular public services in Slovakia

• Promoting IT security incident reporting.
OUR PROJECTS & ACTIVITIES
Incident handling

• National Point of Contact (POC)

• Incident handling
  – Constituency
  – International institution and counterparts
Incident handling

- Web vulnerabilities
- Phishing
- Defacements
- Penetration testing and vulnerability assessment of web applications
Critical security incidents in 2011

• cca 3000 incident reports

70 critical
Critical security incidents in 2011

- Web attacks: 41%
- Phishing: 17%
- Malicious code: 17%
- System penetration attempts: 16%
- Botnet: 9%
THEMIS

• Early warning
  – SIEM

• Information sharing
  – Secure channels

• Incident handling support
Cooperation

• Various CSIRTs/CERTs

• FIRST
  – Preparation for accreditation in progress

• TERENA
  – TRANSITS training

• ENISA
  – Organizational support for National exercices
• International exercises on CIIP
  – Cyber Europe 2010
  – Cyber Atlantic 2011
  – SISE 2011 (Slovak Information Security Exercise)
    • international participation

• TF-CSIRT
  – Status: “accredited”
    • Since May 2011
Education

• Raising Information Security awareness
  – Courses
  – IS terminology
  – Bulletin
Forensics lab

- Hardware & software lab
  - Due in August 2012