REVISED HUNGARIAN IT SECURITY POLICY

Anita TIKOS
• Broad objectives

• Generic tasks
  • PPP, education, R&D
  • regulation, international coordination, awareness
  • child protection

• Challenges:
  • No timeline or deadlines
  • No funding
  • Too sophisticated supporting legal framework, and organizations
• ... on the electronic information security of government agencies
  - scopes extends a somewhat further: supply chain, critical infrastructure
  - scope does not include industry, or the general public

• Established framework for cooperation and information exchange
  - structured tasks and responsibilities
  - designated GovCERT as international single point of contact
OLD STRUCTURE (2013-2015)

Prime Minister's Office
National Cybersecurity Coordination Council

Cybercoordinatort
(Secretariat)

Cybersecurity Forum

Incident management working group
Homeland security working group
E-Government working group
Energy working group
Child protection working group

Ministry of Interior
NBSZ GovCERT

Ministry of National Development
NEISA

Ministry of Public Administration and Justice
NBF CDMA

HM CERT
BM CERT
NAV CERT
NMHH CERT
IH CERT
GovCERT: growing spectrum of tasks
  - vulnerability assessment service for gov’t agencies
  - security training for gov’t IT staff

Competent authority (NEISA): relocated near GovCERT

Formation of the National Cyber Security Center
  - Includes GovCERT, NEISA and IT-sec consultancy
  - Support most of the InfoSec life-cycle (technical and compliance)
Professor Zoltán Rajnai (PHD):
Dean of Óbuda University
Head of Security Science Doctoral School

- From February 2016
- Minister of Interior nominated
- Tasks: keep in touch with private sector companies, cooperate between public and private sector (working groups)
- ENISA Management Board Member
- Organise conference in October (cyber security month)
NEW STRUCTURE (2015- )
MILITARY FRAMEWORK

- Development: 2 level
- 1 March 2016
- Military National Security Service - **Cyber Defence Center** as a new element
  - Tasks: Incident handling and military authority functions
  - Cooperation with Hungarian NCSC and NATO
- **Hungarian Defence Forces/ CIRC:**
  - Military network incident handling
<table>
<thead>
<tr>
<th>National Cyber Security Center</th>
<th>Authority (NEISA)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Incident handling (GovCERT)</td>
</tr>
<tr>
<td></td>
<td>INFOSEC management and vulnerability assessment</td>
</tr>
</tbody>
</table>
IT SEC LIFECYCLE

- Planning
- Governmental institutions
- Regulation and creation of protection
- Incident handling
- Maintenance and monitoring
- Raising awareness
- Alarms and trainings
- Incident coordination
- System support
- IT security control
- Governmental institutions control
- Defense exercise
- Vulnerability assessment
• Single Point of Contact designated by law (from 2013)
• mandate extends beyond governmental infrastructure
• 0-24h on-site & on-call duty
• staff: 20 (duty officers, analysts)
• expanding non-CSIRT tasks
  • technical, compliance & legal consultancy
  • threat assessment
INTERNATIONAL COOPERATION

- Regional
  - Central European Cybersecurity Platform (CECSP)

- EU
  - NIS Directive
  - Commission expert groups: EFMS, EP3R, SMART project
  - ENISA, CERT-EU

- Global
  - Common Criteria
  - FIRST, TI, IWWN
  - NATO MISP
• Exercises
  • NATO CMX, CC, Locked Shields
  • CECSP
  • EU Cyber Europe
  • US Cyber Storm
• From January 2016 there is a new electronic identification card
• More than 220 000 people (end of April)
• Elements: electronic signature
• Healthcare data
• Tax identification
• Fingerprint
FUTURE PLANS

• Government early warning system (EWS)
  • EU-funded project starting in 2016
  • automated, correlated intrusion (attempt) detection

• Legal adaptation of the NIS Directive
  • harmonization of INFOSEC, CI, e-communication, e-commerce legislation
  • participation in cooperation groups, CSIRT network

• Exercises, cybersecurity month, training
Thank you for your attention!

Anita Tikos
National Cyber Security Center
anita.tikos@govcert.hu