Towards secure information society

Epp Maaten
Head of the Cyber Security Domain
e-Governance Academy
eGA’s reach

130+ countries, 200+ organisations
5500+ participants in training events
Estonian e-governance goals since 1998

- Provide information
- Enable electronic communication with the state. Governmental databases have to be accessible for officials and for citizens on-line
- Paperless administration
  Issuing documents and certificates, gathering applications and tax declarations
- Development of e-services for citizens, entrepreneurs and public sector
- Increase efficiency in the public sector

*The development of the information society must not undermine people’s sense of security. The protection of basic rights, personal data and identity must be ensured.*

_Estonian Information Society Strategy, 2006_
Milestones of eGovernment

- 1993: Government web page
- 1998: State portal
- 1999: Registry of registries
- 2001: Data exchange layer – x-road
- 2002: ID-card, PKI
- 2005: Internet voting
- 2007: Mobile ID
- 2007: Reorganisation of legislation
- 2009: Concept of CIIP
All levels of society are affected by IT

- **Targets:**
  - Individuals
  - Businesses
  - Critical Infrastructure
  - Government

- **Actors:**
  - Activists
  - Criminals
  - Organised crime
  - Terrorism
  - Nation states
Cyber Security Principles

- Interdisciplinary approach
- All stakeholders involved
- Public and private sector, Academia
- Coordinated policies and implementation
- Links between regulatory, CERT, law enforcement, intelligence, military
Critical infrastructure sectors
From IT security to cyber security

- 2004 – IT security standard, compulsory for public sector
- 2008 – First Cyber Security Strategy
- 2009 – Emergency Law, concept of CIIP
- 2011 – supervisory tasks to Information System Authority (EISA)
- 2012 – Renewed government regulation for public sector
- 2013 – IT security requirements for vital service providers
- 2018 – Cybersecurity Law, transposition of the EU NIS Directive
  - Cybersecurity requirements for the providers of essential services
  - Additional competences of EISA
New Cybersecurity law 2018

- Cybersecurity policy
- Coordination and cooperation
- Implements the EU NIS Directive
- Consolidates existing norms
- Establishes a clear and solid legal basis for actions
eGA and Cyber Security

- Assessment of state-level or sectorial cyber security capacity
- Development of national/sectorial cyber security strategy and development plan
- Overview of European Union digital and cyber security regulations
- Minimum cyber and information security requirements/standard
- Defense oriented cyber security exercise
- Secure interoperability solution for independent organisations
Global Cybersecurity Index

GCIV2 World Heat Map

Commitment levels
- High
- Medium
- Low
Measures countries’
• cyber security status quo,
• preparedness to prevent cyber threats and
• readiness to manage incidents

Ranks the cyber security capacities of 130 countries.
Visit the NCSI website: ncsi.ega.ee
NCSI indicators

GENERAL CYBER SECURITY INDICATORS
1. Cyber security policy development
2. Cyber threat analysis and information
3. Education and professional development
4. Contribution to global cyber security

BASELINE CYBER SECURITY INDICATORS
5. Protection of digital services
6. Protection of essential services
7. E-identification and trust services
8. Protection of personal data

INCIDENT AND CRISIS MANAGEMENT INDICATORS
9. Cyber incidents response
10. Cyber crisis management
11. Fight against cybercrime
12. Military cyber operations
Thank you!

Follow us online

eGovAcademy
ega.ee