REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

CIIP approach in Estonia

Urmo Sutermäe
Cyber Security Branch
Head of CIIP Section

07.12.2015

Outline

- What is CI and CII in Estonia?
- Legal Framework
- CII Protection
- Practical Activities
- Information sharing
- Challenges

Critical Infrastructure (CI)

Services which are needed for proper functioning of a country incl.

- Electricity supply
- Water supply and waste water treatment plants
- District heating
- Communication services
- Health care
- Financial services etc…

Vital services in Estonia

43 vital services ~ 160 providers		
imprisonment electricity supply gas supply liquid fuel supply airports air navigation public railway rail transport ice breaking activities ports vessel traffic main and basic roads telephone network mobile network data communication	marine radio cable network broadcasting network postal network uninterrupted comm. public order rescue work air and sea rescue marine monitoring operational radio Parliament, President and Government medical care emergency medical care	air surveillance meteo. monitoring warning of a radiation food safety state payments payment services cash circulation district heating system municipality roads water supply waste management public transport drinking water safety blood service

Critical Information Infrastructure (CII)

- Information and communication systems which are needed for providing vital services.
- We arrange CII protection on a national level and have authority to conduct supervision activities.

Regulation

- Emergency Act

  - Guidelines for resolving an emergency as well as defining vital services

  - Organized by responsible ministries/authorities

  - Prepare a risk assessment and continuous operation plan of the vital service

- Decree for vital service information system safeguards
- Field regulation for ISP’s and banks

CII Protection

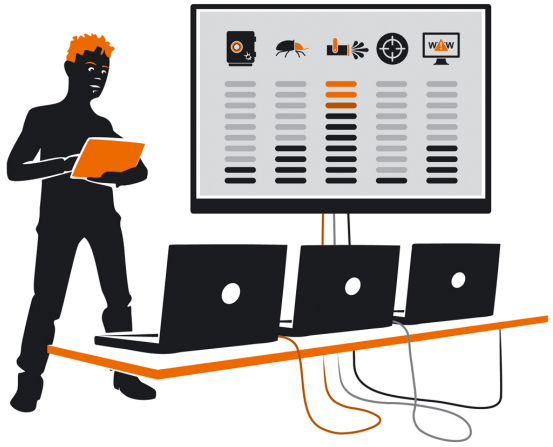
- ISO 27001 / ISKE / best practice
- InfoSec management system
- Guidelines:
  - Requirements for datacenters
  - ICS safeguards
  - Methodology for IT risk assessment
  - Informing of important incident

Practical Activities

- Cyber Security Strategy 2014-2017 activity plan
- National level risk- and vulnerability analysis
- CII dependency analysis
- Development of safeguards and guidelines
- Security assessment and penetration testing
- .ee scanning and website monitoring
- Trainings, Seminars and Cyber Exercises
- Community building

Cyber Exercises in 2015

- Cyber Europe
- Locked Shields
- CONEX
- Baltic Ghost
- Cyber Hedgehog
- Cyber Coalition



Information sharing

- Mandatory reporting of an important incident
- Vital service provider has to inform PoC

  - Mailing list and contact list of vital service providers PoC's
- We will notify the PoC's about important risks and vulnerabilities
- CIIP seminars and workshops
- Usage of eID encryption and TLP

CIIP challenges

- Example IT risk assessment
- New Emergency Act (43➔13+1)
- Technical trainings
- Cyber Exercises for vital service providers
- Penetration tests and follow-up interviews
- Vital service interdependencies and cross-boarder dependencies
- ICS SCADA and Smart grid security
- Product vulnerabilities

Things to remember

- Learn & Teach
- Prevent & Manage
- Risk and Vulnerability Analysis
- Incident Response

REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Thank you!

Urmo Sutermäe
urmos@ria.ee