Estonia’s experience

Estonian Information System Authority (RIA)

2016
National Security Council

National Cyber Security Council

- Police
  - Crime Prevention
  - Criminal Investigation

- Internal Security Service
  - Counterintelligence
  - Investigation of national security incidents

- Information System Authority
  - Cyber Security Branch:
    - CERT
    - 24/7 CSOC & Incident Response
    - Risk Control & Advisory
    - R&D

- Defense Forces
  - Military CIRC

- Intelligence Service
  - Classified networks

Cyber Security Framework in Estonia

Estonia - FOR OFFICIAL USE ONLY
Context

- Population: 1,3M / Active eID: 1,2M
  - one unique identifier for all public interactions (since 2002)
- Data exchange of information systems – X-Road
- State Portal eesti.ee,
- I-voting since 2005
- ‘Once only’ principle – data re-use
- Very high penetration rate of public and private e-services,
  - 99,8% of bank transactions
  - 95% of taxes
- Digital signatures: 60+M / year
  - Saving time: 1+ week per capita
We are accustomed to the fact that Estonia's networks and information systems are regularly mapped and measured to obtain information that would be useful for planning any kind of large-scale activities against Estonia.

In cyberspace, it is progressively challenging to differentiate between criminals that are motivated by personal gain and the security services of a neighbouring state that are interested in employing hybrid warfare against Estonia in pursuit of national objectives.
CERT-EE = cleaners

- CERT-EE ([https://www.ria.ee/cert-estonia](https://www.ria.ee/cert-estonia)) includes also GovCERT officer
- Incident Response: triage, coordination & resolution
- Abuse notifications
- ISP “greenwalling” support
- Monitoring (BGP, DNS, etc)
- R&D

- CERT – 24/7, EVERY (incl. false positive) incident “counts”
- CERT is single point of contact (also in international cases)
- Coordination with police and national security agencies etc.
Focus: capability to Prevent, Manage & Learn

Estonian Information System Authority manages large scale cyber incidents on State level:

- **Obligatory reporting** of incidents by
  - Providers of Vital Services
  - Owners of public databases/Government authorities
  - Providers of services of electronic communications

- Management and coordination of State-level emergency situation
- Regulatory supervision and framework of advisory activities
- National level risk / threat assessments
Background: Vital services

- Regulated by Emergency Act from 2009
- 43 Vital Services stated by the law
- Over 98% of service providers admit that they can’t operate without IT
- High level of inter- and cross-border dependency

RIA arranges CII protection on national level
Security measures for vital service information systems and assets

- General requirements for vital service providers to implement security measures:
  - Implement InfoSec management system
  - Prepare information system risk assessment and implement security measures accordingly
  - Constant application of security measures according to ISO 27001, ISKE or best practice
  - Inform RIA of PoC’s and important cyber incidents

Practical Activities (incl. CII)

• National level risk- and vulnerability analysis, security controls & guidelines development, exercises, advisory etc.

• Community building

• Security assessments & testing
Collective brain

- Strong community
- Exercises
- International cooperation
Thank You!

Martin Indrek Miller
Risk Manager @ Risk Control and Advisory
Cyber Security Branch

www.ria.ee
https://www.ria.ee/about-estonian-information-system-authority/