Estonian
Information System's
Authority

The Estonian approach on ICS security assessments

Ragnar Rattas
Cyber Security Expert
CIIP unit

Outline of my talk

- Short background of EISA & CIIP department
  - Why are we doing it?
- ICS/SCADA security assessments
  - How and what are we doing?

EISA and CIIP department

- EISA cyber security areas
  - CIIP, CERT-EE, Supervision, Baseline security standard development (ISKE)

- CIIP Department
  - Arrange CII protection on the national level
  - Risks analysis, guidelines/controls development, community building, consulting etc.
  - **Testing**

CIIP scope

- 43 vital (critical) services
  - …
  - Electricity supply
  - Gas supply
  - Railway transport
  - Water supply, sewerage and district heating for larger towns
  - …

ICS security assessments

- Find out what is the “real” security level of vital service provider
- How potential attacker could disrupt service?
- Based on attack scenarios
- Verified with penetration testing

ICS security assessments: approach

- Voluntary, state sponsored
- Using 3rd party consultants

- White or gray box testing

- Comprehensive assessment of IT systems (including ICS/SCADA)

Typical assessment task list

- Information gathering from public sources
- Network perimeters
- Workstation & servers
- Remote access
- Physical security

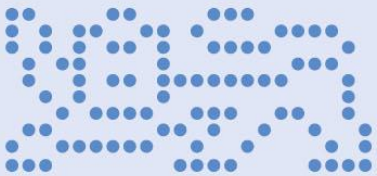
- Disaster recovery plans, architecture, security policies etc.

To sum up

- “Regular” IT is extensively used by ICS
- “quick wins” can be achieved by improving IT security

Thank You!

Ragnar Rattas
ragnar.rattas@ria.ee



Estonian
Information System's
Authority