A navigation authority’s measures for cybersecurity
- The example of Germany

Alan Jacobsen
Dipl.-Ing., MBA
IT-Security Officer

Federal Waterways and Shipping Administration
Germany
Overview inland waterways and technology

- along main waterways there are a **variety of techniques, systems and sensors** of traffic technology

- used for traffic information and traffic advice and thus indirectly support the **safety and efficiency of shipping**

- to ensure the safety of shipping, it is necessary to **implement appropriate cybersecurity measures**
Overview inland waterways and technology

- **in focus is traffic technology:**
  - AIS
  - RIS
  - radar
  - light signals
  - reporting and information system inland navigation
  - river headquarters
Requirements

- **governmental and legal requirements** (in Germany)
  - (e. g. IT-Security-Act in connection with regulations for critical infrastructures + supported acts (from NIS Directive and General Data Protection Regulation)

- method as governmental administration: **BSI-standards** from Federal Office for Information Security (BSI)

- focus is information security
  - **comprehensive approach** with technology, organization and infrastructure
  - aim is to **secure information**

- cybersecurity **is a part of information security**
Threats

- no isolated systems
  - connection to several systems in a **complex network**
  - interfaces to **internet** (third party support, data exchange etc.)

- **digitalization** with **increasing data** in shipping
  - autonomous vessels
  - logistics and transport chains
  - traffic management

- **motives** for attacks: terrorism, extortion (money), rivalry etc.

- **effects** on: traffic, environment, supply, single persons etc.
Threats for inland navigation

(concrete examples)

- carelessness
- internet / mail
- mobile devices
- criminals
- inconsistently / outdated documentation
- fire, water, storm, cold, heat
- gateways and external users
- unclear change management
- cleaning personnel and service provider
- permissions
Measures

- depending on the **criticality**

- **basis and standard** measures for normal protection level

- when protection level is high → **risk analysis**

- example with **security modules**: server in AIS system with virtualization and web platform for monitoring
  - general server (for host and virtual machine)
  - server under Linux (for host and virtual machine)
  - virtualization
  - web server
Measures

- single measures for AIS and reporting and information system inland navigation:
  - external access (network)
  - update management
  - permission management
  - change management
  - firewalls / security gateways
  - separation
  - logging
Measures

- single measures for AIS and reporting and information system inland navigation:
  - only allow as little as possible (USB, microphone, devices, functions, communication)
  - tests and checks (e.g. penetration test)
  - hardening of systems (services, programs, scripts etc.)
  - documentation (for operation and analysis of security incidents etc.)
  - maintenance → product selection
    - avoid potential errors
  - no information leaks (e.g. error messages with version numbers etc.)
Thank you for your attention!