Cybersecurity risk management – how to strengthen resilience and adapt in 2021

23rd November 2020, web-conference

Dr. Mirjam Fehling-Kaschek, Natalie Miller
Main objective

- Improve risk control and resilience of European current and future critical telecommunication infrastructures against physical, cyber and combined cyber-physical threats
RESISTO platform

- Long term control loop
  - Periodic offline analysis
  - Determination of criticalities and long term strategies

- Short term control loop
  - Runtime component
  - Decision support system

- Knowledge base
  - Storage of data for both loops
  - Connection between the loops
Long Term Control Loop

**Risk and resilience management process:**
- Extension of ISO-31000 for risk management
- Addition of steps relevant for resilience assessment
- RESISTO specifications for all steps

**Input collection:**
- Extended threat list
  - System components
  - System functions
  - Threats
  - Mitigation options

- Network representation
  - Scheme of the testbed network for simulation

- Testbed tools
  - Results provided by operators (e.g. penetration tests, honeypots)

**Supporting tools:**
- Shiny app
  - Browse tables
  - View correlations, e.g. critical combinations
  - Threat ranking

- Network simulators
  - Resilience quantification
  - Evaluate mitigation options
Short Term Control Loop

- collects and detects anomalies (early warnings on security attacks or events adversely impacting security)
- evaluates impact
- supports decision making
- drives reaction and mitigation

**SHORT TERM CONTROL LOOP**

- Cyber/Physical Events Correlator
- Risk (Impact) Predictor
- Mitigation
- Workflow Manager
- Orchestration Controller
- Emergency Warning Communication

**Communication Infrastructure**

- TLC operator PSIM/physical detectors
- Airborne Threats Detector
- Audio/Video Analysis
- Smart Spectrum Surveillance
- IoT based sensors
- OSINT & Machine Learning based Threat Detector
- TLC operator SOC/network monitoring

Physical resources monitoring
Network resources monitoring
Summary

Knowledge Base

Long Term Control Loop

- Resilience quantification
- Performance loss
- Resilience indicators

- Measured KPIs
- Realtime application in testbed
End of Presentation