Czech-German Cross-Border Situational Awareness for Critical Infrastructures (PKI)

Introduction of CZ team and its ideas

Jan Voráček

jan.voracek@vspj.cz

Department of Technical Studies
College of Polytechnics Jihlava, CZ

Bayerisch-Tschechische Hochschulagentur
Česko-bavorská vysokoškolská agentura

Vysoká škola polytechnická Jihlava

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Project meeting 1 VŠE Prague 12. 12. 2019

Agenda

Vysoká škola polytechnická Jihlava

1. People
   - Team and expertise
2. Place
   - City and university
3. Project
   - Goals, timetable, results
   - Research strategy and added value
4. Process
   - Agile

Team

Vysoká škola polytechnická Jihlava

- 7 members:
  - 2 academics 0,1 each
  - 2 programmers 30 hours/month
  - 3 students
    - 1 practical placement (12 weeks) and BSc. thesis
    - 2 BSc. thesis

- Expertise
  - Knowledge-based modeling and simulation of complex systems
  - Computer networks, security and QoS
  - Business performance management

Jihlava

College of Polytechnics: 2000s/200e

Vysoká škola polytechnická Jihlava

Project goals

Vysoká škola polytechnická Jihlava

- Introduce joint situational awareness of the stakeholders for critical infrastructures and their cross-border intersections including interdependencies.

- Establishment of a common cyber security (CS) framework for Czech-German cross-border (CB) region.

Phases

- Phase 1: 1.10.2019 – 30.6.2020
  - Analysis of information resources and design of a conceptual model of the security of cross-border critical infrastructures
- Phase 2: 1.7.2020 – 31.3.2021
  - Establishment of shared situational awareness on security of cross-border critical infrastructures
- Phase 3: 1.4.2021 – 31.12.2021
  - Dissemination of results by means of related methodology and shared model for decision support

Timetable and results – see separate file

Strategy

- Collaboration with the key CS players in CZ
  - NUKIB, KYBEZ Platforma kybernetické bezpečnosti
- Identification of stakeholders and their expectations
- Establishment of network
- Continuous delivery of value
- Summarization, modeling and dissemination of results

Stakeholder groups

Vysoká škola polytechnická Jihlava

1. Operators of critical infrastructures

2. Providers of CS technology

3. Governmental institutions

4. Research community

Value for stakeholders

- Networking
  - Exchange of security related knowledge
    - Technology
    - Management
    - Other
- International partnerships
  - Strengthening cross-border cohesion
- Integration of CB CS to business processes
  - Filling the gap between technology and performance
  - Introduction of joint structural metrics

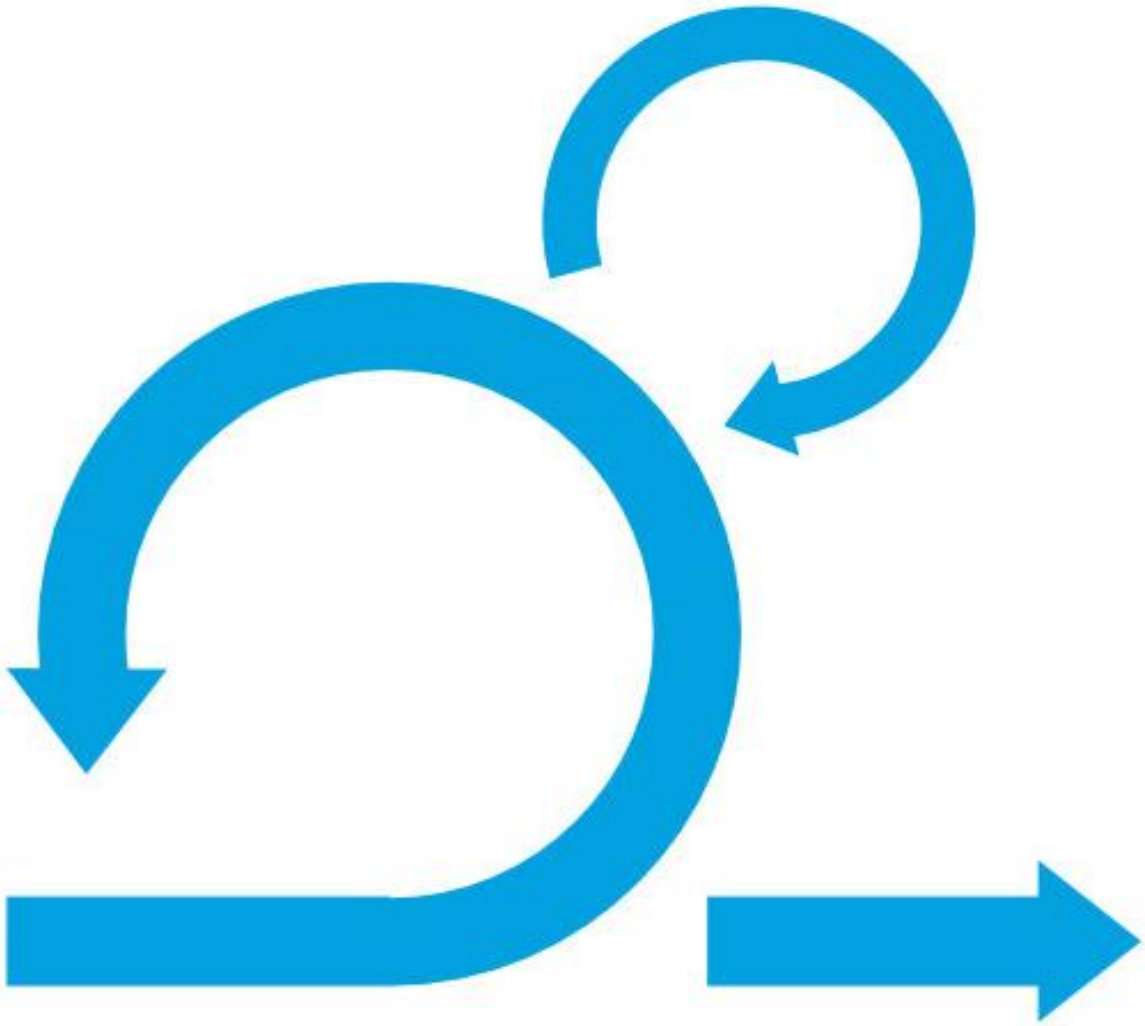
Sample CB-related research questions

- What is the current situation in CS of CB CI?
- How the operators handle both national and international regulations?
- Is it possible to geographically separate CB CI?
- Which specific CB CS arrangements can efficiently localize and minimize impacts of attacks?

Answers must be formulated on the (shared) business level!

- CI must act as supply chain, i.e. adding value to own customers, maximizing performance and preserving desired level of network interoperability

Process: scrum



Thank you!