TECHNOLOGICKÁ PLATFORMA
ENERGETICKÁ BEZPEČNOST ČR

Ochrana kritické infrastruktury v oblasti energetiky

JUDr. Richard Hlavatý
Předseda výkonného výboru

Technologická platforma energetická bezpečnost ČR
V Holešovičkách 1443/4, 180 00 Praha 8
richard.hlavaty@tpeb.cz

MINISTERSTVO PRŮMYSLU A OBCHODU
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
OPPI

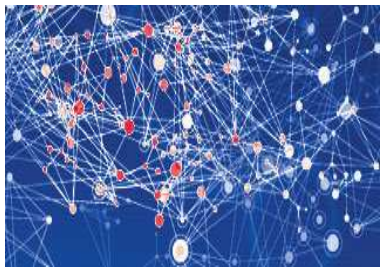
TPEB ČR - vznik a cíle

TECHNOLOGICKÁ PLATFORMA ENERGETICKÁ BEZPEČNOST ČR

- **Byla založena z iniciativy HV PSP ČR a MPO ČR na konci roku 2011** jako projekt Partnerství veřejného a soukromého sektoru (PPP projekt). Podobný projekt PPP není ani v ČR ani v EU. Instituce EK a průmyslová uskupení EK jej a vnímají pozitivně z hlediska důvěryhodnosti pro spolupráci a současně jej vidí jako možný precedent pro ostatní členské státy EU.

- Je sdružením právnických osob, veřejného i soukromého sektoru zaměřených na problematiku energetické a kybernetické bezpečnosti a související ochrany kritické infrastruktury.

- **TPEB nabízí** svým členům:
  - ✓ Silné partnerství a přístup k nejnovějším trendům v oboru
  - ✓ Přístup do procesu standardizace v evropských organizacích
  - ✓ Aktivní prosazovaní zájmů členů v ČR a v EU
  - ✓ Účinnou spolupráci při zavadění preventivních opatření vedoucích k zajištění fyzické a kybernetické bezpečnosti
  - ✓ Strategie pro zapojení do mezinárodních inovačních konsorcií
  - ✓ Propojení společností působících v oblasti utilit



- Cílem je zlepšení zabezpečení kritické infrastruktury a přenesení těchto zkušeností, jako referenčních standardů na úroveň evropskou a mezinárodní.

TPEB ČR v zahraničí

TECHNOLOGICKÁ PLATFORMA
ENERGETICKÁ BEZPEČNOST ČR

- TPEB je aktivní členem řady programů EU zaměřených na zajištění bezpečnosti kritické infrastruktury:

  - **ERNCIP** - Platforma je spolu s HZS ČR (řádný člen platformy) ve společném projektu EK DJ JRC ERNCIP- Referenční síť evropských laboratoří, který analyzuje evropské laboratoře a zkušebny a doporučuje jejich využívání pro nové technologie z oblasti Ochrany kritické infrastruktury.

  - **Cyber Security Coordination Group** - Platforma se spolu s ÚNMZ při MPO (Úřad pro technickou normalizaci, metrologii a státní zkušebnictví) angažuje v projektu EK, řízeným evropským standardizačním orgánem CEN/CENELEC zaměřeným na Kybernetickou bezpečnost, jejímž cílem bude návrh nové legislativy a standardů.

  - **Smart Grid Task Force - EG2 Deliverable -** zaměřený na problematiku SmartGrids v energetice, jehož výstupem je příslušná metodologie, standardizace a certifikace

  - **European Organisation for Security –** nadnárodní zájmové sdružení firem v oblasti bezpečnostního průmyslu

Evropské trendy

TECHNOLOGICKÁ PLATFORMA ENERGETICKÁ BEZPEČNOST ČR

- V posledním roce se aktivity standardizace v oblasti kybernetické bezpečnosti v EU velmi utlumily, ať se jedná o aktivity institucí ENISA, CEN – CENELEC, DG HOME apod.
- Jedním z důvodů je příprava jednotlivých členských států na prosazení vlastních metodik, postupů, standardů a návazných technologií
- Vyžaduje určitý čas pro „vnitřní vyjednávání“
- Evropa naopak vehementně vybízí členské státy k předložení „best practices“ , které se mohou stát základem pro zajištění této problematiky, jak legislativně, tak i procesně a technologicky.

EU trendy = příležitosti pro český průmysl

TECHNOLOGICKÁ PLATFORMA ENERGETICKÁ BEZPEČNOST ČR

Podpora technologických odvětví jakožto dodavatelů pro uživatele bezpečnostních řešení:

- Podporovat spolupráci s průmyslovými sdruženími a akademických sektorem na vytvoření doporučených postupů (best practices) a certifikačních standardů pro plnění zákonných požadavků na systematické řešení kybernetické bezpečnosti (to se týká též např. certifikovaného vzdělávání odpovědných osob).

- Podporovat spolupráci s průmyslovými sdruženími a akademických sektorem na vytvoření certifikačních standardů pro konkrétní produkty v oblasti kybernetické bezpečnosti.

- Podporovat ustavení a fungování specializovaných pracovišť zajišťujících koordinaci vývoje a implementace technických řešení průmyslovými podniky, a koordinaci vzdělávání a špičkové vědecké činnosti včetně podpory účasti těchto pracovišť za ČR v mezinárodních organizacích a iniciativách

- Posílit preferenci kybernetické bezpečnosti ve vztahu k využití veřejných prostředků na vědu a výzkum (Horizon 2020, TAČR, Bezpečnostní výzkum MVČR, rezortní výzkumné zdroje apod.)

Projekt TPEB ČR „Energetická a kybernetická bezpečnost“ OPPI CI

- Projekt je strukturován **do čtyř částí**, které spolu vzájemně souvisí a je připravován i s ohledem na trend narůstající potřeby efektivních procesů standardizace a certifikace.

  - Komunikačních technologie
  - Kybernetická bezpečnost
  - Fyzická bezpečnost
  - Technologie sledování prvků kritické infrastruktury

- Jednotlivé studie mají ambici pokrýt technologické oblasti, zmapovat stav v daných segmentech a identifikovat konkrétní priority, jež budou v dalších fázích rozpracovány. Vychází z nových hrozeb a požadavků na nové bezpečnostní a technologické systémy.

EU trendy a projektové příležitosti pro oblast energetiky v období 2014-2020

TECHNOLOGICKÁ PLATFORMA ENERGETICKÁ BEZPEČNOST ČR

- Vytváření jednotného evropského energetického trhu znamená větší propojenost ale i zranitelnost Evropy

- Ochrana kritické infrastruktury (KI) a cyber-security jsou v současnosti významné téma na evropské ale i národní úrovni
  - ✓ vyjednávaní o nových pravidlech pro KI (Networks Codes)
  - ✓ nové EU směrnici o kyber. bezpečnosti (2013/0027 COD)

- Prioritizace těchto oblastí je velice dobře viditelná i v největším evropském programu pro výzkum a inovace **Horizon 2020** (rozpočet 70 mld. € na 2014-20)

Projekty TPEB ČR
v programu Horizon 2020

TECHNOLOGICKÁ PLATFORMA
ENERGETICKÁ BEZPEČNOST ČR

- **CySmart – Adaptive Cyber Security for Low Resource Wireless Communications Systems.** V čele projektového konsorcia stojí University of Sheffield a jeho součástí jsou výzkumné organizace a firmy ze Spojeného království, Německa, Rakouska, Francie a České republiky Cílem projektu je představit adaptivní řešení kybernetické bezpečnosti wireless ICT systémů kombinujících inovativní zabezpečení na úrovni kryptografické bezpečnosti i fyzické bezpečnosti.

- **OPTIMUS – Bringing Order to Chaos during MassiveVictim CBRN Incidents,** směřuje do oblasti ochrany v případě CBRN incident. V kontextu přípravy tohoto projektu TPEB navázala spolupráci s Fakultou vojenského zdravotnictví Univerzity obrany, Vojenským výzkumným ústavem, Centrem biologické ochrany Těchonín a Státním ústavem jaderné, chemické a biologické ochrany. Konsorcium vede řecká odnož britské společnosti EXUS, která má s evropskými projekty velmi bohaté zkušenosti. Cílem projektu je vytvořit UAV/UGV technologii, která by efektivně asistovala záchranným složkám v případech CBRN incidentů.

- **Advanced Wireless Technologies for Clever Engineering (ADWICE)** klade si za cíl vytvořit silné partnerství mezi SIX a TUW. Toto partnerství se stane základem konsorcia firem, veřejných institucí a univerzit, jejichž společným zájmem je výzkum v oblasti chytré techniky, využití výsledků tohoto výzkumu a případně jeho ekonomické zhodnocení. Projekt ADWICE pokrývá oblasti senzorických systémů, zpracování signálů, mobilních komunikací, radiofrekvenčních aplikací a kybernetické bezpečnosti. V širším smyslu se tak jedná o pro TPEB klíčové téma ochrany kritické infrastruktury. TPEB jako součást projektového konsorcia ADWICE přispěje svými zkušenostmi, vybudovanými vazbami a know-how k optimálnímu nastavení obchodního plánu a partnerských vazeb.

Praktické zkušenosti z evropských bezpečnostních projektů

TECHNOLOGICKÁ PLATFORMA ENERGETICKÁ BEZPEČNOST ČR

Critical Infrastrucutre Security Analysis

- Cíl projektu: odhalit slabá místa a útoky v prostředí KI pomocí propojení případů zneužití, které jsou typické pro síťovou infrastrukturu: řídicí systémy na bázi SCADA protokolů a infrastruktury Advanced Metering-u
- 2012-2015 | CRISALIS website

CRISALIS SECURING CRITICAL INFRASTRUCTURES

Comprehensive Approach to Cyber roadMap coordination and development

- Cíl projektu: vytvořit komplexní evropskou výzkumnou agendu v oblasti a kyber zločinu a terorismu a zahájit dlouhodobé aktivity, které poskytnou stabilní platformu pro bezpečnostní odborníky
- Projekt navrhne návod, doporučení a komplexní plán pro výzkum týkající se počítačové kriminality a kyberterorismu v EU
- 2014-2016 | CAMINO website

CAMINO

Secure Provisioning of Cloud Services based on SLA management

- Projekt se zaměřuje na rozvoj a implementaci open source rámce a nabízí Security-as-a-Service - bezpečnostní parametry stanovené (SLA)
- Poskytuje techniky k systematickému řízení jejich životního cyklu
- 2014-2016 | SPECS website

SPECS

Praktické zkušenosti z evropských projektů – zapojení aktérů

TECHNOLOGICKÁ PLATFORMA ENERGETICKÁ BEZPEČNOST ČR

Malé a střední technologické firmy

- Benefit účasti na projektu: aplikace (a další vývoj) vlastních inovativních technologií, spolupráce s předními evropskými firmami a institucemi, potenciální přístup k novým trhům, celoevropské PR, přístup k financím
- Typická role v projektu: dodavatel technologických řešení; work package leader / účastník; dotace: 0,2 - 1 M Euro
- Příklad firem: ***Sec-Control Ltd.*** (Finsko), ***Espion Ltd.*** (Irsko), ***CBRNE Ltd.*** (Velká Británie) v projektu CAMINO

Velké firmy (nad 250 zaměstnanců)

- Přínos participace: přístup k nejnovějším evropským výsledkům výzkumu (e.g. v oblasti kyberbezpečnosti kritické infrastruktury) a jejich příprava pro nasazení na trhu; spolupráce se špičkovými evropskými partnery; příspěvek k vytváření evropské strategie v dané oblasti a podpora celoevropské akceptace výsledků
- Typická role v projektu: koordinátor / work-package leader / zákazník projektu; dotace: 0,5 - 2 M Euro
- Příklad společnosti: Symantec (Irsko), ENEL (Itálie), SIEMENS (Německo) v projektu CRISALIS

Výzkumné organizace a jiné instituce (veřejný a mimovládní sektor)

- Benefit účasti na projektu: zapojení do vytváření evropského rámce v dané oblasti; aktivní participace na prosazovaní vlastních preferencí v tomto procesu; podpora sdílení „best practices“ v rámci organizace a partnerských subjektů
- Typická role v projektu: work-package leader / účastník; dotace: 0,2 - 1 M Euro
- Příklad organizace: Cloud Security Alliance (Velká Británie) a její zapojení se do projektu SPECS

Závěr

TPEB organizuje 6.listopadu nejen pro své členy konferenci zaměřenou na bezpečnost v Parlamentu České republiky kde vystoupí mimo jiné:

- Dr. Alois Sieber – poradce EK pro bezpečnost; bývalý ředitel bezpečnostního výzkumu v DG Joint Research Centre ISPRA (SRN)
- Maaike van Tuyll – Head of Unit for Analysis of Natural, Technological and Security Threats; Ministerstvo bezpečnosti a spravedlnosti; Národní koordinátor pro bezpečnost a boj s terorismem(Nl.)
- Dr. Alessandro Lazari – ERNCIP (DG JRC ISPRA) Evropská referenční sít ochrany kritické infrastruktury (It.)
  Directiva 114 na ochranu KI

Děkuji

Kontakt : JUDr. Richard Hlavatý,
předseda výkonného výboru
Technologická platforma energetická bezpečnost ČR
V Holešovičkách 1443/4, 180 00 Praha 8
+420 777 796 963 - richard.hlavaty@tpeb.cz

Co přináší členství v TPEB

TECHNOLOGICKÁ PLATFORMA
ENERGETICKÁ BEZPEČNOST ČR

- ✓ Silné partnerství a přístup k nejnovějším trendům v oboru
- ✓ Přístup do procesu standardizace v evropských organizacích
- ✓ Aktivní prosazovaní zájmů členů v ČR a v EU
- ✓ Účinnou spolupráci při zavadění preventivních opatření vedoucích k zajištění fyzické a kybernetické bezpečnosti
- ✓ Strategie pro zapojení do mezinárodních inovačních konsorcií
- ✓ Propojení společností působících v oblasti utilit

Více informací získáte na http://www.tpeb.cz/