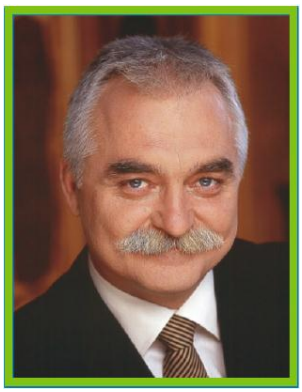

Milan Urban

Vážené dámy, vážení pánové,

pevně věřím, že krásné léto a dovolené Vám pomohly nabrat nových sil. Stejně tak TPEB ČR se v druhé polovině roku chystá na realizaci řady aktivit, které již byly započaty. MPO ČR předložilo Strategickou energetickou koncepci ČR, probíhá posuzování dokumentů ekonomických dlouhodobých přínosů a nákladů pro trh a jednotlivé zákazníky při zavedení inteligentních měřících systémů v elektroenergetice a v plynárenství.

Evropská komise 30. 7. 2012 oznámila přijetí akčního plánu věnovaného na podporu konkurenceschopnosti průmyslu EU v oblasti bezpečnosti – zpráva IP/12/863. Během posledních měsíců roku by měla být přijata směrnice o ochraně kritické infrastruktury, která může významným způsobem ovlivnit i oblast energetické a kybernetické bezpečnosti. Klíčovou úlohu zde hrají procesy připravovaných norem, standardů a certifikací. Zde můžeme říci, že spolupráce zaměřená zejména na tuto problematiku s HZS ČR při MV ČR i ÚNMZ při MPO ČR probíhá velmi dobře a má první výsledky.

IP/12/863
http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/863&format=HTML&aged=0&language=CS&guiLanguage=en

Ing. Milan Urban

Předseda Správní rady Technologické platformy
„Energetická bezpečnost ČR“

Projekty – tuzemské

Bezpečnostní výzkum Ministerstva vnitra ČR

Na základě výzvy třetí veřejné soutěže ve výzkumu, experimentálním vývoji a inovacích PROGRAMU BEZPEČNOSTNÍHO VÝZKUMU ČESKÉ REPUBLIKY V LETECH 2010 – 2015 (BV II/2-VS) iniciovala TPEB ČR přípravu projektů v oblastech komunikačních technologií, kybernetické bezpečnosti a technologií sledování prvků KI v návaznosti na ochranu kritické infrastruktury.

Projekty jsou nyní ve fázi zhodnocení návrhů projektů. Hodnotící lhůta končí vyhlášením výsledků veřejné soutěže dne 28. 1. 2013. Vybrané projekty budou zahájeny 1. 4. 2013 a ukončeny do 31. 12. 2015.

MPO - CzechInvest – Program Spolupráce Technolo-gické platformy

- podána Plná žádost 27. 8. 2012

Dne 4. 10. 2012 byl projekt postoupen k dalšímu hodnocení.

- *realizace projektů do 31. 12. 2014*

Projekty – zahraniční

- V mezinárodním měřítku máme předjednánu účast v pracovních skupinách EK, které se zaměřují na přípravu směrnice EK „Evropský program pro ochranu kritické infrastruktury“ nyní projednávané v Evropském parlamentu, která bude předložena na podzim 2012. V ní jsou obsaženy priority ochrany kritické infrastruktury a návrhy na jejich zabezpečení.

Snahou bude také mezinárodní spolupráce v rámci 7. Rámcového programu „Bezpečnost“ (2007 – 2013), kde bylo alokováno 1,4mld € pro rozvoj vědy a výzkumu v uvedené oblasti, a v návazném programu EK Horizon 2020, který počítá s navýšením částky o 50% na uvedenou problematiku.

Aktivity TPEB budou zaměřeny v rámci výše uvedených programů na harmonizaci legislativy, standardizace a zkušebnictví a dále pak na podporu rozvoje nových technologií a propojování (technologické, komunikační) jednotlivých zmíněných oblastí. Důraz bude položen na aplikovaný výzkum a demonstrační projekty v následujících čtyřech tematických oblastech důležitých z hlediska energetické a kybernetické bezpečnosti a to jak z pohledu legislativy, tak technologií:

- Komunikační technologie
- Kybernetická bezpečnost
- Technologie sledování prvků KI
- Fyzická bezpečnost

● TPEB ČR se přihlásila do tendru v rámci standardních projektů Višegrádského fondu. Předložený projekt byl vypracován ve spolupráci s centrem SIX při VUT v Brně, Elektrotechnickou fakultou Univerizity v Žilině a Fakultou informatiky, elektroniky a telekomunikace Technické univerzity v Krakově. Projekt s názvem Critical Infrastructure Protection: Common Risks and Opportunities by se měl zaměřit na dvě oblasti. V první řadě by se autorský tým měl zabývat výhledem relevantních politik a iniciativ EU s přihlédnutím k zájmům a potřebám středoevropských zemí. Druhou oblastí zájmu by se poté měly stát potenciální přeshraniční /regionální dopady selhání kritických infrastruktur.
V případě úspěchu by projekt měl být naplňován v roce 2013.
Jeho výsledky by měly být prezentovány na veřejné konferenci v Praze na podzim roku 2013. Projekt zároveň má sloužit jako příprava k žádosti o významnější strategický grant Višegrádského fondu, o který se TPEB ČR chce v rámci nově utvořeného konsorcia ucházet na jaře 2013.

Uskutečněná jednání a aktivity

červenec 2012

● Ing. Aleš Špidla a a Ing. Petr Kubeš se stali členy CSCG (Cybers security coordination group) jako zástupci České republiky a zúčastnili se zasedání, které se konalo 31. 8. 2012 v Berlíně.
Vytvoření této skupiny schválil technický výbor CEN (European Committee for Standardization, Comité Européen de Normalisation, Europäisches Komitee für Normung) v únoru roku 2012. CSCG působí jako poradní a koordinační orgán rady CEN v technických, politických a strategických otázkách, týkajících se standardizace kybernetické bezpečnosti.
Cíle CSCG jsou:
- poskytnout strategické poradenství pro technické výbory CEN, CENELEC a ETSI
- provádět analýzu evropských a mezinárodních standardů pro kybernetickou bezpečnost
- definovat společné evropské požadavky pro evropské a mezinárodní standardy kybernetické bezpečnosti
- vytvořit evropský plán na sjednocení kybernetické bezpečnosti
- působit jako kontaktní místo pro všechny instituce EU v otázkách, týkajících se normalizace kybernetické bezpečnosti
- vytvořit návrh společné americké a evropské strategie pro vytvoření rámce mezinárodních standardů v oblasti kybernetické bezpečnosti
- posílit koordinaci evropských aktivit ve výborech ISO a IEC s cílem společné transatlantické strategie
http://www.cen.eu/cen/Sectors/Sectors/Security%20and%20Defence/Security/Pages/CyberSecurityCoordinationGroup.aspx

září 2012

● Ve dnech 4. – 6. září 2012 proběhlo mezinárodní cvičení složek Integrovaného záchranného sboru (IZS) v prostorách elektrické stanice ČEPS, a.s., Nošovice a v blízkosti vedení zvláště vysokého napětí V 404 - Mosty u Jablunkova.
Bezpečnostní cvičení, které bylo pracovně nazváno „HORIZONT 2012“, mělo za cíl prověřit krizovou a havarijní připravenost společnosti ČEPS a součinnost jednotlivých složek IZS. Cvičení proběhlo ve spolupráci s provozovatelem slovenské přenosové soustavy SEPS, a.s., Policií ČR, Hasičským záchranným sborem ČR, Armádou ČR, Českým červeným křížem a Policejním sborem Slovenské republiky.
Cvičení HORIZONT 2012 se uskutečnilo pod záštitou ministra vnitra ČR, ministra průmyslu a obchodu ČR a ministerstva hospodářství SR.
Cvičení se zúčastnili zástupci TPEB ČR.
Více na http://www.ceps.cz/CZE/Media/Tiskove-zpravy/Stranky/horizont.aspx

● Účast na jubilejní XV. Podzimní konferenci, pořádanou AEM (Asociace Energetických Manažerů), která se věnovala aktuálnímu tématu „Blackout v ČR – Strašák nebo faktická hrozba?“. Přednáška JUDr. Richarda Hlavatého byla zaměřena na roli TPEB ČR při přípravě a řešení krizových situací v energetice.
Záznamy i fotogalerie dostupné na www.aem.cz v sekci Akce / 2012.

Plánované akce a konference

říjen 2012

• účast na 4. setkání ERNCIP (European Reference Network for Critical Infrastructure Protection), které se koná 17. 10. 2012 v Amsterdamu. Tématem setkání je ICS a Smart Grids, které je součástí Konference „Building a Resilient Digital Society“

listopad 2012

• setkání s Luigim Rebuffim, výkonným ředitelem EOS (European Organisation for Security) s možností diskutovat aktuální otázky bezpečnostní problematiky a konkrétních zapojení do připravovaných projektů EK.
http://www.eos-eu.com/default.aspx?page=home

Aktuality z oblasti kybernetické bezpečnosti.

• **Industrializace Hackingu - Nová éra v oblasti IT bezpečnosti**

Industrializace Hackingu vytvořila vlnu hrozeb, které jsou stále sofistikovanější. Hacking se stal průmyslovým odvětvím, nástrojem průmyslové špionáže, ale také motorem inovací, které jsou vynuceny stále novými a novými technologiemi útoků. Musíme držet s hackery krok pomocí nových specializovaných bezpečnostních technologií zaměřených na boj proti nejnovějším hrozbám. A to s vědomím dnešní ekonomické reality, omezených zdrojů a rozpočtových škrtů.
http://www.securityweek.com/industrialization-hacking-new-era-it-security

• **Symantec: DDoS útokem hackeři odvrátili pozornost od jejich skutečného cíle**

Důkazem tvrzení, že útoky hackerů jsou stále sofistikovanější je útok na nejmenovanou banku. Hackeři spustili DDoS útok (Distributed Denial of Service), kterým „zaměstnali“ IT specialisty v napadené instituci a zatímco se tito specialisté věnovali řešení DDoS útoku, tak potichu a skrytě hackeři kradli data z bankovních účtů. Dalším znepokojivým momentem, který mně napadá, je to, že hackeři používají pro své útoky válečnou taktiku. Odvést pozornost a síly protivníka jiným směrem a na nechráněném místě zaútočit.
http://www.zdnet.com/symantec-data-stealing-hackers-use-ddos-to-distract-from-attacks-7000005481/

• **Zpráva Kaspersky LAB: Global IT Security Risks: 2012**

V roce 2011 společnost Kaspersky Lab (přední firma v oblasti kybernetické bezpečnosti), ve spolupráci s B2B International, provedla průzkum týkající IT profesionálů pracujících pro velké a střední podniky. Cílem průzkumu bylo zjistit, jaké povědomí mají IT specialisté o firemních bezpečnostních řešeních, zjistit úroveň jejich znalostí o aktuálních hrozbách, jaké jsou problémy, který nejčastěji čelí, jaké jsou jejich schopnosti vyhodnotit rizika spojená s internetovými hrozbami, atd. .

O rok později, obě společnosti provedly podobný průzkum na větší ploše a s větším počtem respondentů. To byla příležitost nejen k posouzení situace v oblasti podnikové bezpečnosti v roce 2012, ale také k porovnání výsledků s výsledky získanými v předcházejícím roce, a zjištění hlavních trendů. Podle poloviny dotázaných, je kyberkriminalita v jejích různých formách druhou největší hrozbou pro podnikání. Navzdory skutečnosti, že tento pohled se změnil jen velmi málo od loňského roku, přičemž opatření podle IT specialistů jsou žalostně nedostatečná - jen o málo více než polovina respondentů věří, že jejich společnosti jsou opravdu bezpečné. Totéž platí i v souvisejících oblastech, jako je porušování práv duševního vlastnictví a průmyslové špionáže.

Více než 3300 senior IT profesionálů z 22 zemí se zúčastnilo tohoto průzkumu. Všichni respondenti měli vliv na IT bezpečnostní politiky, a dobrou znalost IT bezpečnostních otázek a všeobecných obchodních záležitostíá (finance, HR, apod.). Globálně, respondenti pocházeli z firem tří velikostí Small Business (SB, 10-99 uživatelů IT), Medium Business (MB, 100-999 uživatelů IT) a Enterprise organizace (E, 1000 + uživatelů IT).

IT odborníci se podle průzkumu nejčastěji potýkají s malwarem, spamem a neoprávněnými pokusy o proniknutí do systému.

Část průzkumu, který se zabýval bezpečnostními politikami pro mobilní zařízení, ukázal, že třetina společností umožňuje zaměstnancům používat je

s plným přístupem k podnikové síti. Tím vytváří díru v jejich bezpečnosti. Pokud jde o firemní bezpečnostní politiky pro osobní zařízení, zjištění nejsou příliš povzbudivá:
pouze 9% firem plánuje zavést tvrdé omezení.
36% tázaných uvedlo, že jejich firmy schvalují používání osobních zařízení pro pracovní úkoly.
Cílené útoky představují ještě další velkou hrozbu pro firemní infrastruktury. 11% respondentů se domnívá, že tato hrozba bude jejich hlavním zájmem v budoucnu a třetina z odborníků je si jista, že jejich firmy budou napadeny dříve nebo později.
Mnozí IT profesionálové uvádějí jako problém rozpočtová omezení a nedostatek jasného porozumění mezi vysoce postavenými manažery, nemluvě o dostatečném počtu vyškolených pracovníků. Problém je také obecně nízké povědomí uživatelů o kybernetických hrozbách, které lze pozvednout pouze osvětou a vzdělá-váním.

Celá zpráva zde:
http://www.kaspersky.com/downloads/pdf/kaspersky_global_it-security-risks-survey_report_eng_final.pdf