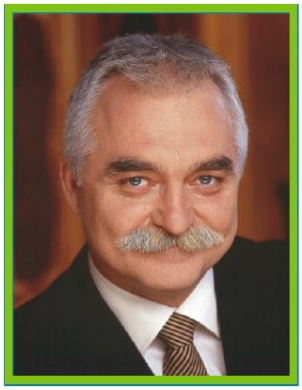

TECHNOLOGICKÁ PLATFORMA
ENERGETICKÁ BEZPEČNOST ČR

MINISTERSTVO
PRŮMYSLU A OBCHODU

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OPPI

Vystoupení předsedy správní rady TPEB ČR ing. Milana URBANA
Na kulatém stole projektu „Energetická a kybernetická bezpečnost“
dne 26.září 2013

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.. Důvodem může být, kromě jiného příprava jednotlivých členských států na prosazení vlastních metodik, postupů, standardů a návazných technologií což 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. To vidíme jako příležitost pro český průmysl i stát.

Kybernetická bezpečnost je fenomén, který má ve vztahu ke státu 4 základní roviny: národní obranu (řeší AČR), národní bezpečnost (řeší NBÚ), veřejný pořádek (řeší PČR) a zpravodajství (řeší BIS, ÚZSI, VOZ). Právní regulace kybernetické bezpečnosti je technicky i organizačně vysoce problematická – důvodem je skutečnost, že dominantní část informační sítě má soukromé vlastníky nebo provozovatele, že stát nemá technické kapacity ani kompetence k faktické kontrole informační sítě a že síť má mezinárodní charakter (tj. nelze pracovat se standardně pojímanou státní jurisdikcí).

Kybernetická bezpečnost ve smyslu národní bezpečnosti je předmětem návrhu zákona o kybernetické bezpečnosti. Přestože mají nová právní úprava a činnost vládního a národního dohledového pracoviště přinést podnikům nové typy povinností, nejedná se o kontroverzní otázku – při práci na návrhu zákona se ukázalo, že podniky naopak tuto iniciativu podporují, neboť jejím cílem je bezpečně fungující česká a evropská informační společnost (i podnikatelé navíc dospívají k závěru, že je tento cíl nedosažitelný bez účasti státu).

Ukazuje se, že české podniky jsou na nové bezpečnostní požadavky poměrně dobře připraveny a nebude tedy na jejich straně třeba žádných zásadních investic – naproti tomu úroveň státních a místních informačních systémů mnohdy neodpovídá bezpečnostním požadavkům.

Návrh zákona prozatím nepočítá se státem garantovanými certifikačními procesy. Naproti tomu ale zákon předpokládá existenci bezpečnostních standardů (tzv. bezpečnostních opatření), které budou u určitých typů soukromoprávních i veřejnoprávních subjektů mandatorní (typicky pro subjekty působící v energetice). Na straně středních a velkých podniků se bude jednat o otázku tzv. compliance procedur a vznikne tak poptávka po procesech předběžného posouzení konformity místního bezpečnostního řešení se zákonnými požadavky. Není-li taková procedura zákonem stanovena, bude její potřeba logicky vykryta soukromým sektorem – z toho však plyne nebezpečí její problematické kvality. Absence státní ingerence navíc může vést k vytvoření subversivního potenciálu generujícího v technologicky extrémně náročném prostředí bezprostřední bezpečnostní rizika. Je tedy nutno řešit formy zapojení státu do tvorby, unifikace a implementace soukromých certifikačních procedur.

Procesy zadávání veřejných zakázek významně znesnadňují aplikaci bezpečnostních kritérií pro nákup ICT od úrovně jednotlivých zařízení až po velké investiční celky. Je tedy třeba vytvořit důvěryhodný systém národní certifikace nejen shora uvedených bezpečnostních řešení (tj. např. metodik, postupů apod.) ale též konkrétních bezpečnostních technologií tak, aby technologie používané v bezpečnostně exponovaných aplikacích nepředstavovaly riziko pro národní kybernetickou bezpečnost. Specifickou pozornost vyžadují v tomto směru technologie pro delokalizované ukládání a zpracování dat (tzv. technologie cloud computing).

České univerzity a podniky zabývající se vývojem a provozem bezpečnostních řešení jsou i přes velmi malou podporu ze strany státu na světové úrovni. Česká republika je rovněž jedním z prvních států EU, které představily návrh zvláštního zákona upravujícího problematiku národní kybernetické bezpečnosti (to rovněž při vynaložení jen naprosto minimálních investic). Při důsledné politické podpoře se může Česká republika díky existujícímu know-how relativně snadno dlouhodobě prosadit do skupiny států určujících průmyslové, politické a právní trendy v této oblasti.

Kybernetické útoky mají sice obvykle původ ve vyspělých zemích, k jejich provádění je však často zneužívána infrastruktura rozvojových států. I malý rozsah rozvojových investic do zabezpečení infrastruktury v rozvojových státech tedy může přinést výrazné zlepšení české a evropské bezpečnostní situace. Může rovněž výrazně podpořit vývoj českých komerčních bezpečnostních řešení a jejich prosazení na mezinárodním trhu. Tento typ rozvojové pomoci je navíc prozatím mimo hlavní pozornost světových mocností, takže může včasné uchopení této problematiky vést k založení významného postavení ČR v mezinárodních organizacích i při řádově nízké nominální hodnotě investic.

Z výše uvedeného plynou následující doporučení k podpoře českého průmyslu (tj. k podpoře technologických odvětví jakožto dodavatelů i ostatních odvětví jakožto uživatelů 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 (tato pracoviště již nyní zčásti existují – např. TPEB, C4E aj.)
- Posílit preferenci kybernetické bezpečnosti ve vztahu k využití veřejných prostředků na vědu a výzkum (TAČR, GAČR, Bezpečnostní výzkum MVČR, rezortní výzkumné zdroje apod.)
- Zaměřit českou rozvojovou pomoc do sektoru kybernetické bezpečnosti, aktivně pracovat s tématem rozvojové agendy v oboru kybernetické bezpečnosti na mezinárodně-politické úrovni a aktivně se účastnit práce mezivládních organizací, do jejichž kompetence spadá nebo může spadat oblast kybernetické bezpečnosti.