Zpráva o činnosti a hospodaření v roce 2013 s výhledem na příští období přednesená na Valné hromadě dne 17. prosince 2013

V uplynulém období roku 2013 vyvíjela TPEB ČR celou řadu aktivit v domácím i zahraničním prostředí.

Hlavní pilíř aktivit TPEB ČR představuje projekt Energetická a kybernetická bezpečnost financovaný v rámci programu OPPI MPO ČR. Z technických důvodů, nikoli však na naší straně, byl projekt formálně zahájen 1. dubna 2013. Práce na projektu však již probíhaly od začátku tohoto roku. Projekt je rozfázován do čtyř etap, z nichž první byla zakončena 30.9. Druhá etapa skončí 28.2.2014 a zbývající dvě etapy v intervalech pěti měsíců budou zakončeny 31.12.2014.

Celkové způsobilé výdaje na tento projekt jsou více než 6,5 miliónů Kč. TPEB má smluvně zajištěnu dotaci ve výši 75 % uznatelných nákladů.

Dokument první etapy, který máte před sebou ve finální verzi, měl za cíl zmapovat hlavní národní i nadnárodní politiky a iniciativy v oblasti ochrany kritické infrastruktury a specifikovat a aktualizovat strategickou výzkumnou agendu projektu.

Plánované prioritní oblasti výzkumu byly představeny a prodiskutovány v rámci kulatého stolu, který proběhl 26. září 2013 v hotelu Trója. Setkání se zúčastnili zástupci firem, institucí státní správy a akademických a výzkumných institucí. V návaznosti na kulatý stůl a konzultace v členských firmách byly následně priority upraveny tak, aby rezonovaly se zájmy a potřebami členské základny. Finální zpráva z první etapy byla rozeslána členům a je k dispozici na webu platformy.

Kromě zmíněných vlastních cílů, je smyslem tohoto projektu nastartovat řadu aktivit, konkrétních dílčích projektů v tuzemsku i zahraničí a návazně rozvinout činnosti v oblasti legislativní a normotvorné. V rámci

procesu formování priorit v oblasti kybernetické bezpečnosti se jako všeobecně zajímavý a potenciálně užitečný vyjevil projekt aktivní kybernetické obrany. Nástrojem pro další rozvíjení tématu aktivní kybernetické obrany by se měly stát projektové výzvy Technologické agentury ČR, kde se implicitně počítá s vyvíjením technologických inovací na půdorysu spolupráce mezi firmami a výzkumnými institucemi, což zcela odpovídá poslání a cílům TPEB. Další užitečné alternativy budou představovat výzvy v rámci Bezpečnostního výzkumu MV ČR či programů napojených na Horizont 2020.

Aktivní kybernetickou obranu (ACD) jsme dle mezinárodních zvyklostí a pro vlastní orientaci rozdělili na tři oblasti samotné obrany: detekce, terminace, klam (detection, termination, deception). V rámci každé této oblasti identifikujeme české i mezinárodní experty, expertní týmy či společnosti, které se danou problematikou zabývají. V této souvislosti jsme rozvinuli aktivity na evropské úrovni, kde jsme se zapojili do 3. pracovní skupiny výzkumu a vývoje – WG3 Research & Inovation při NIS platform (Network and Information Security) zřízené v rámci evropské agentury ENISA. Tato skupina má za cíl identifikovat nejbližší budoucí podobu kybernetických hrozeb a na jejím základě zformulovat priority výzkumných cílů dotačního programu Horizon 2020 v podobě doporučení pro Evropskou komisi. Strategické doporučení sice není závazné, nicméně praxe ukázala, že se jím Evropská komise řídí. České firmy s vizí rozvoje aktivních obranných metod, s jimi související technologické inovace a v oboru komunikačních technologií, kybernetické bezpečnosti budou podpořeny z obou stran. Jak na straně EU formulací cílů, které budou v souladu s expertní vizí jejich odborníků, tak velkou šancí získat pro tyto vize prostředky z programu Horizon 2020.

Další významné aktivity TPEB se týkají vstupů platformy do strategických debat a formování klíčových strategických dokumentů v ČR i na úrovni EU. TPEB vstupuje aktivně do legislativního procesu uchopení kybernetické bezpečnosti v ČR a to konkrétně do jejích aktivních součástí spoluprací s renomovaným expertem doc. Radimem Polčákem, který je autorem věcného záměru návrhu Zákona o kybernetické bezpečnosti. Cílem této spolupráce bude v prvním kroku definování právních dilemat, které mohou nastat pro české firmy v oblasti aktivní kybernetické obrany, především v oblasti terminace. Téma je to velmi žhavé, neboť ve světě právě nedávno proběhlo první soudní rozhodnutí o možnosti aktivní destrukce statisícového botnetu Microsoftem. Trend, kdy se firmy budou bránit proti kybernetickým hrozbám samy nejen ochranou, ale i aktivní terminací probíhajícího útoku, je tedy zřejmý, nicméně právně komplikovaný. V dalších fázích spolupráce plánujeme rozvinout standardizační model pro české technologické firmy, jejichž produkty budou aktivní kybernetickou obranu zajišťovat.

Platforma v oblasti aktivní kybernetické obrany rozvinula na podzim první podobu spolupráce se zahraničními i českým firmami ve věci přípravy na simulaci kybernetického útoků na průmyslové řídící systémy SCADA. Tento projekt je v současnosti v intenzivních přípravách a očekává se, že v průběhu prvního čtvrtletí roku 2014 bude připraveno několik potencionálních scénářů, které pokryjí celou plejádu potenciálních útoků. Od primitivních útoků přetěžující zařízení pro sofistikované zkompromitování průmyslového řídícího systému a převzetí jeho kontroly. TPEB má za cíl do těchto scénářů zapojit všechny své relevantní členy, aby se vyzkoušely nejen kombinace uplatnění různých technologií, např. terminace a její detekce, ale i celkové krizové bezpečnostní opatření. Není úmyslem suplovat schopnosti úřadů a zaměstnanců firem zajišťujících kritickou infrastrukturu, jak je tomu např. při mezinárodním cvičení Cyber Coalition, nýbrž právě uplatnění technologií v praxi a jejich kombinace jak na České, tak mezinárodní úrovni. Tento projekt nám zajistí praktické ukázky uplatnění těch technologií, postupů, best practices etc., ale i úspěšnost jednotlivých opatření, aby ostatní činnosti (legislativní výzkum, standardizace, definice výzkumných cílů) byly v souladu s realitou. Výstupy tohoto projektu budou uplatněny mimo jiné i ve WG3, čímž úspěšné české technologické firmy mohou přímo ovlivnit budoucí vývoj na celoevropské úrovni.


Zástupci platformy i nadále reprezentují ČR v pracovních skupinách v rámci Evropské komise – CEN/CENELEC, Cyber Coordination Group, kde se účastníme formulace několika strategických doporučení pro Evropskou komisi v oblasti standardizace technologií. Dlouhodobější účast v této skupině, i s ohledem na jejím relativně malou velikost a přesto silný poradní hlas, nám zajistí možnost uplatnit standardy vzniklé v ČR včetně konkrétních technologií a trendů jejich vývoji na evropské úrovni.

TPEB také navázala zatím neformální spolupráci s NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), která vzešla z listopadové návštěvy jednoho z řešitelů projektu OPPI v Tallinnu. Cílem této spolupráce bude především konzultace závěrů právní analýzy doc. Polčáka a další možný rozvoj. Centrum CCD COE se v roce 2014 přímo na aktivní kybernetickou obranu zaměřilo včetně jednotného tématu na konferenci CyCon 2014, spolupráce tak lemuje nejen směřování TPEB, ale i celosvětový výzkumný trend.

České technologické firmy i akademická sféra jsou ve světě známí svou vysokou úrovní, nicméně aktivní zastoupení na evropské úrovni, především tam, kde je možné prosadit budoucí směřování výzkumu a vývoje, uplatnit české vynálezy či pomoci identifikovat spolehlivější technologie Česká republika pokulhává. TPEB se podařilo mít silný hlas na několika klíčových místech a začít aktivně upevňovat roli odborné autority. V této věci je spolupráce nejen s doc. Polčákem, ale i odbornými pracovišti jako je NATO CCD COE naprosto klíčová, protože tak TPEB může hrát výraznou roli na poli průmyslového uplatnění v kontextu výrazné české, resp. světové autority v oboru kybernetické bezpečnosti.

Kromě aktivit v projektové oblasti TPEB v uplynulém období nadále rozvíjela myšlenku vytvořit v ČR nejen v evropském kontextu unikátní vzdělávací program zaměřený na bezpečnostní management v oblasti ochrany energetické a kybernetické infrastruktury. V listopadu 2013 došlo k dohodě mezi TPEB a Fakultou podnikatelskou VUT, podle které tento program bude spuštěn jako specializace stávajících manažerských programů akreditovaných ve Velké Británii a USA. Pro tento program TPEB počítá s oslovením předních českých odborníků – teoretiků a praktiků a zároveň chce využít svých evropských kontaktů, které by umožnily funkční internacionalizaci programu.

Činnosti, které TPEB ČR zahájila, je potřebné i nadále rozvíjet jako projekt spolupráce veřejného a soukromého sektoru a v úzké spolupráci s PSP ČR, MPO, MV, MO a dalšími institucemi s ohledem na komplexnost a závažnost této problematiky. Neméně důležitý je zájem o spolupráci a praktickou součinnost s výzkumnou a akademické sférou. Velmi si této spolupráce vážíme a ceníme si operativnost při posuzování a řešení dílčích záležitostí. Jsme jako průmyslová platforma otevřeni spolupráci s dalšími seriózními subjekty, které mají zájem a schopnost se do naší práce a naplňování strategie platformy zapojit na úrovni tuzemské i zahraniční.

Již nyní se potvrzuje, že v dalším horizontu by měla platforma být místem, které svým potenciálem může výrazně napomoci formulování a zejména prosazování společných zájmů v oblasti energetické a kybernetické bezpečnosti, respektive ochrany kritické infrastruktury. Připravenost, jak technologická, tak i normativní výrazně napomůže státu i firmám čelit předpokládaným i jiným hrozbám, které naší společnost čekají. Současně kvalitní příprava na půdorysu klíčových firem, státní správy a výzkumných institucí umožní efektivní vynakládání prostředků s důrazem na podporu českých kapacit a schopností.