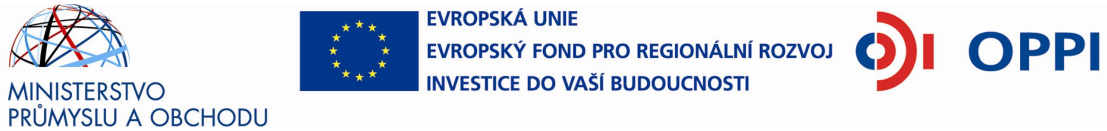
Nikola Schmidt
analytik kybernetické bezpečnosti



Tento projekt je financován z ERDF prostřednictvím OPPI a ze státního rozpočtu ČR.

Kooperace mezi státním, soukromým a akademickým sektorem v kyber-bezpečnostním prostředí

Kooperace mezi státním, akademickým a soukromým sektorem je věčné téma rozpoutávající diskuse. Často se objevuje v momentech, kdy je spolupráce těchto tří zásadních sektorů lidské tvůrčí činnosti nefunkční. Že spolupráce přináší pro všechny zúčastněné přínos a výhody, by mělo být všem zúčastněným jasné. Bohužel tomu tak není a jednotlivé sektory mají tendenci se uzavírat do vlastních. Některé méně, jiný více. K rozlousknutí tohoto problému je nutné nalézt odvážné vizionáře, kteří budou ochotní jít proti rigidnímu systému uvnitř každého ze tří sektorů, dát jim prostor se postavit do vedení, ustát tlak silných mocenských struktur a v závěru pomoci k podání si rukou s ostatními ke spolupráci. Proč tomu dnes tak není?

Ač se to může zdát naprosto zjevné, je vhodné zmínit zásadní motivy zmíněných tří sektorů. Státní instituce jsou motivované politickými a administrativními zájmy, první reprezentují politickou moc, druhé jistou kontinuitu a tedy jistotu udržení si agendy participujících úředníků, což je ve výsledku tichá dohoda na administrativní úrovni reprezentující administrativní moc. Akademický svět objevováním nového a nepoznaného. Soukromý sektor prostými ekonomickými výsledky. Je paradoxem, že tyto tři na hony vzdálené motivy jsou právě tím důvodem, proč by spolu měly všechny tři sektory spolupracovat, aby každý z nich dosahoval co nejlepších výsledků? Nikoli. Akademický sektor naplňuje své poslání rozvojem inovací, nových nápadů, tedy tehdy, přispívá-li k dobré věci výzkumem a inovacemi. Samotná výzkumná soutěž mezi akademiky probíhá ohnivě během samotného zkoumání, nikoli již během implementace registrovaného patentu, protože tou dobu konkurenční týmy opět zaměřují své síly na výzkum nových, a vylepšování starších, nápadů. Snaží se opět přijít s něčím novým. Je-li nápad doveden do použitelné podoby, nastupuje sektor soukromý, tažený ekonomickými zájmy, který patentu vdechne život a věnuje prostor k praktickému rozvoji. Spolupráce akademického a soukromého sektoru se v tomto duchu jeví zjevná a bezproblémová. V tu chvíli nastupuje stát, který by měl v tomto cyklu dobře definovat strategické zájmy státu a tedy i výzkumu tím, že odpovídajícím způsobem ovlivňuje redistribuci finančních prostředků do výzkumných priorit tak, aby závěry co nejlépe reflektovaly strategické zájmy státu. Soukromý sektor by v závěru celého cyklu měl vycítit vůni příležitosti a té se chopit. Pokud se jedná o kriticky důležitou např. bezpečnostní otázku státu, měl by stát v tomto bodě inovaci částečně podpořit, popř. nastavit standardy bezpečnosti tak, aby byly společnosti nucené tyto standardy dodržet nebo se podílet na vývoji odpovídajících prostředků – inovovat. Ačkoliv se to vše může

zdát naprosto zjevné, ne vždy to dokonale funguje. Řekněme si proč a použijme částečně jako referenční rámec realitu kooperace v oboru kybernetické bezpečnosti v České republice.

Každý sektor je nutné vnímat z několika různých perspektiv, jednou perspektivou je to, jak se daný sektor vnímá a jinou, co od něj očekávají sektory ostatní. Tak např. soukromý sektor bude chtít, aby mu do jeho inovací stát příliš nemluvil, neboť příležitost dodavatelského subjektu je přirozeně povinnost příjemce, tedy toho subjektu, který je povinován inovaci zaplatit. Navíc s diskutabilním smyslem – není zřejmé, že inovace přinese vyšší zisky. Bezpečnost je investice do snížení rizik, pokud jsou měřitelná nebo alespoň odborným úsudkem předpokládatelná. Kybernetické hrozby jsou v České republice stále spíše neexistující problém, takže investice do jejich prevence jsou pro většinu firem nutnými, ale často zbytečně vynaloženými prostředky. Banální útoky se sice odehrávají, proti těm se lze bránit z drtivé většiny dodržováním základních pravidel informační bezpečnosti. Kybernetická bezpečnost ale diskutuje i potenciál dalších, nových, budoucích a především strategicky cílených útoků, které mohou být řízené a podporované jinými státy proti jeho kritické infrastruktuře. Takové útoky přijdou rozhodně dříve, než mezinárodní právo vyřeší své nekonečné dilema, zda útok v kyberprostoru je nebo není použití síly. Je to v současnosti obrovská příležitost jak pro státy, tak pro souboj soukromého sektoru v konkurenčním boji. Máme tak jasnou představu, proč soukromý sektor motivován není: hrozba je nejspíše malá, většinu se podaří odrazit v zárodcích. Na našem území se kromě „cvičení" neznámých hackerů v březnu 2013 vlastně vůbec nikdy nic nestalo. A v neposlední řadě je pro soukromý sektor potřebné být zaměřen na zisk v nejbližším horizontu. Akademici od soukromníků potřebují testovat v praxi inovace a stát by měl podpořit soukromníky v rozvoji jejich byznysu tak, aby reflektoval strategické zájmy státu. Zde už ale, zvláště v naší na korupci tolik citlivé zemi, chodíme po tenkém ledě.

Akademický sektor v takovém prostředí bez jasně definovaných strategických cílů státu může pouze tápat, sledovat výzkum v zahraničí, experimentovat na vlastní půdě a shánět peníze na výzkum z různých zdrojů, které žádnou strategii nereflektují. Výsledky jsou pro soukromý sektor těžko použitelné, jejich testování v praxi je především drahé a navíc s nejistými výsledky. Celé výzkumné aktivity a směry jsou i mezi vědci zpochybňovány a vně vystavovány posměchu z nesmyslného bádání, což obratem demotivuje často talentované výzkumníky k dalšímu konání. Soukromníci ale od akademiků potřebují inovace, protože se potřebují utkat s konkurencí a bez implementace inovací to logicky nejde. Jak už jsme ale podotkli, nebudou investovat do slepých uliček. Je tedy bezpodmínečně nutné zapojit stát.

Tím se dostáváme do toho nejzábavnějšího prostředí. Akademici i soukromníci jednají do jisté míry komerčně ve světě nabídky a poptávky. Bezpečnostní prostředí je ale problematické, protože míru rizika lze úsudkem odhadnout jen těžko, zvlášť riziko kybernetické hrozby ve státě, kde k žádným seriózním útokům nedošlo. Nejsou žádné statistiky a analýzy dopadů, investic do znovuobnovení informačních systémů, výčet ztrát plošného výpadku proudu apod. V jiných státech, především v USA, ale čelí velké společnosti kybernetickým útokům každý den. Nicméně i přesto je nutné, aby náš stát jasně zorganizoval model kooperace mezi všemi třemi sektory a vydefinoval jasné strategické cíle země v oblasti kybernetické bezpečnosti. Na

počátku jsme zmínili, že ve státě se perou různé politické zájmy, to je čistě řečeno souboj o moc. Nejen o politické směřování země, ale též o to, jaké skupiny budou toto směřování řídit. Akademický i soukromý sektor by měl v této věci spolupracovat koordinovaně, protože na rozdíl od státních struktur jsou oba sektory poměrně neměnné co do personálního složení, ale i co do strategického směřování. Je vážně paradoxní, že ten sektor, od kterého se očekává co nejvíce strategický přístup je již z principu velmi málo schopný taková strategická směřování tvořit, natož se podle nich dlouhodobě řídit. Co z toho vyplývá za závěry? Nic objevného, stáčí se podívat do vyspělejší demokracie.

V USA má výzkum v oboru kybernetické bezpečnosti na starosti DHS – Department of Homeland Security (mimo jiné, centra výzkumu jsou decentralizovaná), který určuje strategické cíle výzkumu v oboru, pomáhá zajistit finance externím subjektům např. i z Evropy nebo rozvíjí strategické směřování firem jako je MITRE, které je financováno přímo DHS nebo Pentagonem. Jsou-li výzkumné experimenty blízko prototypu, zajistí jejich testování v částečně reálném prostředí, které potvrdí rizikovým investorům, že tato technologie stojí za povšimnutí. V USA je to právě stát, který zásadně koordinuje výzkum a motivuje soukromý sektor k investicím tam, kde je to pro stát strategicky zásadní. Je to možné z celé řady důvodů, nicméně schopnost soukromníků a akademiků se zkoordinovat je určitě jedním z nich. Tato koordinace pak může fungovat jako lobbing, který ale reflektuje zájmy státu!

Např. konkrétně v oblasti kybernetické bezpečnosti energetického sektoru došlo v USA k zásadnímu zlomu, kdy úřad pro standardizaci založil v březnu 2009 koordinační skupinu pro kybernetickou bezpečnost (Cyber Security Coordination Task Group – CSCTG), jenž připravila směrnici pro bezpečnost v tzv. Smart Gridech, chytrých distribučních sítích. Poznamenejme, že jejími členy jsou všechny možné soukromé subjekty, od poskytovatelů služeb, přes výrobce po obchodníky, federální agentury, univerzity, laboratoře etc., celkem 475 subjektů obdobného rozměru. Není to tedy stát, kdo definuje konkrétní strategie, ale koordinační skupina složená ze všech sektorů. Stát pouze poukáže na strategické zájmy. V Polsku již kooperace na podobné bázi funguje, celému konceptu se říká PPPP – Public-Privat Partnership Platform (www.ppp.gov.pl). V České republice vzniká spousta malých i větších sdružení, nicméně světlem budiž např. TPEB – Technologická platforma – „energetická bezpečnost“, která je zaměřena pouze na energetický sektor. Nicméně tomuto sdružení se podařilo semknout významné hráče energetického sektoru a nyní připravuje za celek strategickou představu o širším rozvoji dle vzorů ze zahraničí. Stát v USA ve své strategii pouze motivuje obdobné sdružení ke konání jistým směrem – zabezpečit veškerou kapacitou energetický sektor od kybernetických hrozeb. Je-li to nutné, pak prezident USA vydá dekret, kterým umožní všem zúčastněným vyjmout ze všech soutěží čínskou firmu Huawei. Flexibilita tohoto systému je až ohromující a důvod je prostý, stejné cíle všech ve stínu jednoho státu jako ústřední fundamentální hodnota.

Bylo by určitě velmi přínosné, kdyby se Česká republika, tedy stát a jeho úřady, zaměřily na aktualizaci nejzásadnějších strategických dokumentů. Např. v Bezpečnostní strategii ČR z roku 2011 se v bodě 55 uvádí, že proti kybernetickým hrozbám se budeme bránit založením centra reakce na kybernetické incidenty. V kontextu celého problému kybernetické bezpečnosti je to

ohromný redukcionismus. Největší strategie státu by měla obsahovat jasné oblasti zájmu kybernetické bezpečnosti státu, jejich prioritizaci, základní analýzu rizik a definici zájmů státu o stavu blízké a vzdálené budoucnosti, aby ostatní sektory mohly, jak bylo řečeno výše, odpovídajícím způsobem reagovat a zapojit se do mezinárodní spolupráce důstojně a se vztyčenou tváří.