Praha 15. 2. 2017

Úřad vlády České republiky
nábřeží Edvarda Beneše 4
118 01 Praha 1 – Malá Strana

na vědomí

Ing. Miloš Zeman
prezident republiky
Hrad I. nádvoří č. p. 1
119 08 Praha 1 – Hradčany

Poslanecká sněmovna Parlamentu
České republiky
Sněmovní 4
118 26 Praha 1 – Malá Strana

Senát Parlamentu České republiky
Valdštejnské nám. 17/4
118 01 Praha 1 – Malá Strana

Česká strana sociálně demokratická
Lidový dům
Hybernská 1033/7
110 00 Praha 1

ANO 2011
Babická 2329/2
149 00 Praha 4

Komunistická strana Čech a Moravy
Politických vězňů 9
111 21 Praha 1

TOP 09
Michnův palác, budova č. 2
Újezd 450/40
118 00 Praha 1 – Malá Strana

Občanská demokratická strana
Truhlářská 1106/9
110 00 Praha 1

Křesťanská a demokratická unie -
Československá strana lidová
Palác Charitas, Karlovo nám. 5
128 00 Praha 2

Úsvit - Národní Koalice
Sněmovní 1
118 26 Praha 1 – Malá Strana

Ministerstvo financí
Letenská 525/15
118 10 Praha 1 – Malá Strana

Ministerstvo financí
Ing. Andrej Babiš
Letenská 525/15
118 10 Praha 1 – Malá Strana

Bezpečnostní informační služba
P. O. BOX 1
150 07 Praha 57

Ministerstvo vnitra
Centrum proti terorismu a hybridním hrozbám
Nad štolou 3
P. O. BOX 21
170 34 Praha 7

Ivo Valenta
Senát Parlamentu České republiky
senátor
Valdštejnské nám. 17/4
118 01 Praha 1 – Malá Strana

Asociace malých a středních podniků
a živnostníků ČR
METEOR Centre Office Park B
Sokolovská 100/94
186 00 Praha 8 – Karlín

Asociace podnikatelů a manažerů
Dělnická 213/12
170 00 Praha 7 – Holešovice

Radostné Česko bez EET
mail@stop-eet.info

Sdružení podnikatelů a živnostníků ČR
Marie Cibulkové 394/19
140 00 Praha 4

Strana soukromníků České republiky
T. G. Masaryka 24
534 01 Holice

Strana svobodných občanů
Perucká 2196/14
120 00 Praha 2

Okresní hospodářská komora
v Jablonci nad Nisou
Jiráskova 9
466 01 Jablonec nad Nisou

Česká tisková kancelář
Opletalova 5/7
111 44 Praha 1

Česká televize
Kavčí hory
140 70 Praha 4

Česká televize
168 hodin
Kavčí hory
140 70 Praha 4

Česká televize
Reportéři ČT
Kavčí hory
140 70 Praha 4

Echo Media a.s.
Malostranské nám. 203/14
118 00 Praha 1 – Malá Strana

CET 21 spol. s r.o.
Kříženeckého nám. 1078/5
152 00 Praha 5

FTV Prima, spol. s r. o.
Na Žertvách 24/132
180 00 Praha 8 – Libeň

Barrandov Televizní Studio, a.s.
Kříženeckého nám. 322
152 00 Praha 5

Futura, a.s.
Politických vězňů 9
111 21 Praha 1

CZECH NEWS CENTER a. s.
Komunardů 1584/42
17000 Praha 7

Economia, a.s.
Pernerova 673/47
186 00 Praha 8

RF HOBBY, s. r. o.
Bohdalecká 6/1420
101 00 Praha 10 – Michle

Tlačová agentúra Slovenskej republiky
Dúbravská cesta 14
841 04 Bratislava

Rozhlas a televízia Slovenska
Mlynská dolina
845 45 Bratislava

PETIT PRESS, a. s.
Lazaretská 12
811 08 Bratislava

MAFRA Slovakia, a. s.
Nobelova 34
836 05 Bratislava 3

Zoznam s.r.o.
Viedenská cesta 3-7
851 01 Bratislava

Vážení,

dovoluji si Vás upozornit na dvě závažná ohrožení občanů a firem v České republice včetně upozornění na zavádějící až zcela mylné informace, které byly a jsou veřejně sdělovány ze strany některých státních orgánů a jejich zástupců. Jedná se o rizika spojená s elektronickou evidencí tržeb (EET) a kontrolním hlášením a dále rizika spojená s auty a jejich počítačovým řízením. Tato vozidla již začínají jezdit i v České republice.

I. Elektronická evidence tržeb a kontrolní hlášení

Upozorňuji Vás na skutečnost, že jste Ministerstvem financí zřejmě byli záměrně uvedeni v omyl v záležitosti elektronické evidence tržeb a kontrolního hlášení.

V prosinci 2016 jsem za kolektiv na Ministerstvo financí odeslal dopis [příloha č. 1], ve kterém jsem mimo jiné žádal o zaslání odborné studie, která byla podkladem pro rozhodování o výhodnosti a výnosnosti elektronické evidence tržeb. Ohledně reklamy na EET nazvané *etržby - Férově pro všechny* [1] jsem chtěl získat podrobné výpočty, které sloužily jako podklad pro čísla uveřejněná v této reklamě.

Od Ministerstva financí jsem v lednu obdržel dopis s odpovědí. [přílohy č. 2 a 3] V dopise bylo i CD, na kterém byly tři studie, které Ministerstvu financí sloužily jako podklady pro rozhodování o výhodnosti a výnosnosti EET. Tyto studie jsou rovněž zveřejněny na webových stránkách Ministerstva financí. [2–4] Na většinu mých dotazů byla odpověď zamítavá a na dotaz týkající se reklamy na EET byla vyhýbavá.

Po prostudování dodaných materiálů jsme zjistili, že se v nich vyskytují významné nedostatky. Chybí v nich informace o možných dopadech případného úniku dat, což se nám jeví jako zcela zásadní problém (podrobněji se tomu věnujeme níže). Dále se jedná o nekvalitní citace použitých zdrojů, protože z uvedených bibliografických citací v podstatě není možné jednoznačně dohledat zdrojové informace.

Vhledem k tomu, že dvě ze studií poukazují na slovenský způsob řešení elektronické evidence tržeb, jsme považovali za vhodné tento dopis poslat i na Slovensko, protože tam není problém s jazykovou bariérou.

Iluze zabezpečení dat na počítačích

V dnešní informační společnosti představují úniky dat stále větší a větší hrozbu a nelze jim zcela zabránit. Velké úniky dat jsou poměrně časté. [5–12] Ani sebelépe zabezpečený počítač neznamená plnou záruku, že data v něm uložená jsou v bezpečí. Dokonce ani počítače trvale odpojené od internetu nejsou za určitých okolností zárukou 100% zabezpečení dat, a to ani v případě, kdy se k nim fyzicky nedostane nikdo „nepovolaný“, aby je nakopíroval na CD apod. [13–15]

Data z elektronické evidence tržeb a kontrolního hlášení lze zařadit mezi velmi nebezpečná. Jejich případný únik může vést k vážnému ohrožení řady firem i občanů České republiky. Jakmile se taková data jednou zveřejní a dostanou do nepovolaných rukou, bude velmi obtížné až téměř nemožné zabránit jejich zneužití a šíření. Kdo tvrdí, že data z EET a kontrolního hlášení jsou plně zabezpečená proti úniku, ať již zvenku, nebo zevnitř, ten o počítačové bezpečnosti prakticky neví vůbec nic. Je tedy s podivem, že v žádné ze zmíněných studií se neřeší dopady případného úniku dat sesbíraných z EET pro firmy a obyvatele v České republice. Protože o problémech spojených s případným únikem dat z databází museli autoři studií dobře vědět, je vysoce pravděpodobné, že někdo, například z vedení Ministerstva financí, musel dát pokyn k tomu, aby se tato hrozba ve studiích záměrně neřešila.

EET – hrozba pro firmy a občany

Jak se dají data z EET zneužít? Kromě DIČ (obsahující rodné číslo podnikající fyzické osoby) na účtenkách mohou být data využita ke zjištění denních hotovostních tržeb v jednotlivých prodejnách. Je potom velmi snadné vysledovat, kolik peněz případně zůstává ve firmě do další přepravy peněz do banky, kolik peněz se bude převážet do banky apod. V tomto ohledu by tyto informace představovaly „zlatý důl“ pro kriminální živly, kterým by stačilo jen malé krátkodobé sledování pohybu zaměstnanců při odchodu z určité firmy, pokud peníze nejsou odváženy bezpečnostní agenturou. Tato data jsou mnohem přesnější než nejpodrobnější marketingový průzkum. Dají se z nich dobře zjistit nadstandardní příjmy konkurence v dané oblasti, a tedy je možné poblíž umístit svoji pobočku, čímž by se poškodila, nebo dokonce zničila konkurence.

Kdo se navíc dokáže dostat k datům mobilních operátorů, kteří zaznamenávají i údaje o přibližných polohách mobilních telefonů, které se při datové nebo hlasové komunikaci hlásí do sítě, může získat velmi dobrý přehled nad lidmi. Přibližnou polohu lidí v době, kdy nevolají nebo jejich telefony se nepřipojují na internet, lze docela snadno dopočítat. [16] Na sledování polohy telefonu stačí případně znát jen telefonní číslo. [17–18] Díky boji proti tzv. terorismu se v rámci údajné větší bezpečnosti lidí přistupuje k jejich větší kontrole.

Především různé zpravodajské služby mohou zkombinovat data z EET se sledováním výskytu občanů. Pokud k tomu přidají data z bank, nic jim nebrání, aby u většiny lidí dokázaly s velmi vysokou pravděpodobností určit jejich každodenní chování. Šlo by určit, kdy daný člověk nakupuje, jestli kupuje dražší věci, kolik peněz má zřejmě doma, jaké má vybavení domácnosti a mnoho dalších podrobností. Sběr těchto dat je časovanou bombou a lidé by měli mít možnost se rozhodnout v referendu, jestli toto riziko chtějí podstoupit. Vláda nemá a neměla od lidí svolení na sbírání takto citlivých dat a ani žádná politická strana neměla sběr citlivých dat od občanů a firem ve volebním programu.

S ohledem na zmíněné skutečnosti je možné, že hlavním důvodem pro zavedení EET mohla být snaha o tiché získání téměř plné kontroly nad většinou obyvatel ČR a že získání několika miliard korun (pokud vůbec) ročně navíc do státního rozpočtu může být jen pouhou záminkou. Několikanásobně více peněz se dá snadno ušetřit bez propuštění státních zaměstnanců a bez snižování jejich platů. Podrobnosti jsou popsány v dopise, který byl v červenci 2016 zaslán na Úřad vlády České republiky. [příloha č. 4] Protože Úřad vlády České republiky neprojevil zájem o to, kde by se dalo každoročně získat až 100 miliard korun, ale řeší několik teoretických miliard korun z EET a kontrolního hlášení, je na místě si položit otázku, jestli je „narovnání“ podnikatelského prostředí a vybrání pár možných miliard tím pravým důvodem. Z Úřadu vlády České republiky přišlo pouze standardní potvrzení o přijetí dopisu. Dopis zřejmě zaujal pouze pana JUDr. Vojtěcha Filipa, předsedu KSČM, který písemně odpověděl.

O tom, že EET je možná jen záminka pro získání plné kontroly nad občany ČR, svědčí i následující skutečnosti. V říjnu 2016, během bouřlivých debat o blížícím se prosincovém spuštění EET [19], byla ministrem obrany, panem MgA. Martinem Stropnickým (z ANO 2011), v tichosti předložena k projednání novela zákona o vojenském zpravodajství. [příloha č. 6], [20] Po několika kolech připomínek je projednání této novely zákona naplánováno na 21. 2. 2017. Tato aktualizace zákona by tajné službě umožňovala sběr metadat, tedy obdoba toho, co údajně sbírá Americká bezpečnostní agentura (NSA). Metadata sice netvoří samotný obsah sdělení, ale dá se z nich většinou odvodit mnohem více, než kdyby se „pouze“ zjistil obsah sdělení. Z metadat se zjistí odesílatel a příjemce, jejich poloha, datum a čas komunikace, velikost zprávy, u mobilního telefonu kromě telefonního čísla i výrobní číslo, navštívené stránky, stažené soubory, … [21–22] Z metadat se určí pohyb, zájmy a částečně i některé plány „libovolného“ člověka, tedy téměř vše. Ve spojení s EET a kontrolním hlášením se podchytí i nákupní zvyklosti, majetek všech lidí včetně jejich plánů do budoucna a životní úrovně. Sběr metadat může být velmi nebezpečný i pro zdroje novinářů, a dokonce i pro samotné novináře. Je téměř jisté, že by ohrozil svobodu tisku a demokratické hodnoty, na kterých si náš stát tolik zakládá. Vzhledem k tomu, že exis-

tují různé smlouvy o spolupráci mezi některými zeměmi, je vysoce pravděpodobné, že by data o občanech České republiky beztrestně proudila do zahraničí. Kdo by chtěl mít trochu soukromí, ten by si asi zřídil e-mail mimo země NATO a jeho spojenců, ideálně v Ruské federaci (e-mail na Yandexu v angličtině [23]), a přemluvil by k tomu i své přátele. Dále by asi použil šifrované připojení k internetu prostřednictvím zpravidla placené virtuální privátní sítě (VPN), která by maskovala jeho IP adresu, což by museli dodržovat i jeho přátelé, a pak by si e-maily posílali v docela slušném soukromí, aniž by potřebovali používat program Tor nebo jeho klony. [24–25] Sběr metadat neochrání stát a občany před teroristy, protože ti dokážou toto opatření snadno obejít použitím prakticky neprolomitelných šifrovacích mřížek (každému známých z letních táborů), klasické neevidované pošty, kurýrních služeb apod., ale slouží pro naprostou kontrolu občanů a případné předávání dat do nepovolaných rukou mimo území České republiky.

Čím déle by trval sběr dat z EET, tím přesnější by bylo přiřazení účtenek ke konkrétním lidem.

Ke sběru dat dochází i při placení platebními kartami, ale tyto informace směřují do jednotlivých bank apod., a jsou proto evidované na mnoha samostatných místech. Kdyby došlo k úniku těchto dílčích dat, byla by obtížně zneužitelná na celonárodní úrovni. Oproti tomu data z EET i kontrolního hlášení jsou shromažďovaná na jednom místě, což rizika zneužití zvyšuje.

Kontrolní hlášení – hrozba pro firmy

U přijatých a vydaných faktur nad 10 000 Kč včetně DPH firmy vyplňují kontrolní hlášení, a to buď měsíčně, nebo čtvrtletně. Kromě problémů, které toto vyplňování formulářů mnoha firmám způsobuje, je zde obdobně jako u EET nebezpečí v podobě úniku dat. Z těchto dat lze snadno získat informace o dodavatelsko-odběratelských vztazích mezi firmami. Po propojení dat z EET a kontrolního hlášení lze u firem jednoduše zjistit například velikost skladových zásob, finanční možnosti jednotlivých firem, jejich zákazníky, jakou jsou schopné dát cenu ve výběrových řízeních, na jakých dodavatelích jsou závislé, jaké přibližné platy mají jejich zaměstnanci, nové levnější dodavatele, řadu nových odběratelů a hodně dalších výhod. Jakmile by se nějaká firma s větším kapitálem a špatnými úmysly dostala k těmto datům, může i v rozsahu několika měsíců významně poškodit, nebo dokonce zničit konkurenci. O možném úniku a následném zneužití dat se v takovém případě nikdo nemusí dovědět, a tudíž může být téměř nemožné toto řádně vyšetřovat. V průběhu několika let od úniku mohou za zvláštních okolností krachovat různé firmy. Tato data mohou být lehko zneužita i k vydírání. Taková databáze představuje „zlatý“ důl pro člověka znalého dobývání znalostí z databází. [26]

Data z kontrolního hlášení se dají zneužít mnoha způsoby. Předpokládejme, že nějaká firma s větším kapitálem a špatnými úmysly se dostane ke všem datům z kontrolního hlášení. U svých konkurentů zjistí jejich dodavatele, odběratele, v jaké výši a jak často mezi nimi probíhají finanční operace, zkrátka má hotový marketingový průzkum trhu. Pak se stačí zaměřit na odběratele konkurence, byť do doby před získáním klíčových dat ještě třeba neznámými, a nabídnout jim nižší cenu, různé doplňkové služby, delší záruku atd. Obdobně lze informace zneužít i na dodavatele konkurence. Je možné klíčového dodavatele koupit či jinak ovlivnit, aby nemohl včas dodat zboží a služby, což se může konkurenci vymstít zejména v případě státních zakázek, kde se za každý den z prodlení může platit značná smluvní pokuta, a tím se konkurenční firma může dostat do vážných problémů. Pokud se tato firma rozhodne pro investice, má jako na dlani celý trh s toky peněz mezi většinou firem. Může tedy koupit takovou firmu, o které přesně ví, jak si stojí na trhu.

Je reálné domnívat se, že pan Ing. Andrej Babiš musel o riziku zneužití těchto dat vědět.

Nedůvěryhodná reklama na EET

V reklamě na EET, nazvané *etržby - Férově pro všechny*, [1] za přibližně 30 000 000 Kč, [příloha č. 2] která proběhla v médiích, Ministerstvo financí možná lhalo celému národu o výhodnosti a výnosnosti EET. V reklamě se tvrdí, že díky EET se vybere až 18 miliard korun, k čemuž lze podotknout, že toto číslo není výslovně uvedeno v žádné ze zmíněných studií. V reklamě se také tvrdí, že za 18 miliard se dá koupit 2700 špičkových hasičských vozidel atd. Když bylo Ministerstvo financí požádáno o zaslání podrobných výpočtů pro ověření těchto čísel, [příloha č. 1] jeho odpověď byla vyhýbavá [příloha č. 2]. Z toho vyplývá, že Ministerstvo financí nemá odpovídající podkladové materiály a že k těmto číslům dospělo metodou, která je neověřitelná. Jelikož se tato reklama udělala za peníze daňových poplatníků a její obsah byl vytvořen zcela neprůhledně, měl by její obsah být prošetřen nezávislým auditem, aby se objasnilo, jestli se Ministerstvo financí nesnažilo účelově manipulovat s veřejným míněním občanů České republiky a jestli nedošlo k naplnění skutkové podstaty některého z trestných činů.

Prosíme Vás o zřízení nezávislé komise, která prošetří obsah zmíněné reklamy, tj. jestli daná čísla nebyla účelově nadhodnocená. Pokud se ukáže, že Ministerstvo financí není schopné doložit daná čísla a že se jednalo o dezinformační kampaň za peníze daňových poplatníků, pak Vás podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, prosíme o zaslání informací, jak byli viníci potrestáni. Rovněž prosíme o zaslání závěrečné zprávy vyšetřovací komise včetně podkladových materiálů, které obdržela od Ministerstva financí. Zprávu s materiály stačí nakopírovat na přiložené DVD.

Návrh řešení k EET a kontrolnímu hlášení

Z výše zmíněných důvodů se jako jediné řešení problémů z EET a kontrolního hlášení jeví zrušení elektronické evidence tržeb a kontrolního hlášení, bezprostřední smazání veškerých sesbíraných dat z těchto evidencí (neobnovitelným způsobem), a to včetně všech záložních kopií či jiných záznamů s tím souvisejících. Pracovně-právní postih těch vedoucích pracovníků, kteří svým jednáním uvedli v omyl zákonodárce a vládu při následném rozhodování o nasazení EET a kontrolního hlášení. Bez zbytečného odkladu uhradit podnikatelům alespoň jejich přímé náklady na zajištění EET a kontrolního hlášení. Zvážit případné trestní stíhání odpovědných osob, pokud se prokáže, že svým jednáním ohrozily občany a stát. V takovém případě by bylo na místě po těchto osobách požadovat plnou úhradu nákladů vzniklých státu se zajištěním provozu EET a kontrolního hlášení.

Místo nebezpečného sběru dat z EET a kontrolního hlášení je vhodnější posílit finanční kontroly a vydávání daňových dokladů ponechat pouze na papírovou podobu.

Pokud vládě tvořené především členy ČSSD a ANO záleží na bezpečnosti lidí a firem, zajistí bezodkladné zrušení EET a kontrolního hlášení včetně smazání všech shromážděných dat.

II. Nová auta s počítačovým ovládáním řízení

Vývoj v oblasti automobilového průmyslu rychle směřuje k automatizovanému řízení. Již za pár let by lidé nemuseli ztrácet čas při řízení některých nových vozidel. Mezi hlavní výhody tohoto pokroku patří jak rychlejší reakce počítačů na různé rizikové situace, a tím snížení počtu dopravních nehod, tak i ušetřený čas řidičů. Některá vozidla již mají schopnost automatického parkování nebo poloautomatické jízdy pod dohledem řidiče. Především počítačové zpracování obrazu ještě musí projít značným vylepšením, aby se dala počítačům svěřit plná kontrola nad vozidly. Je to sice náročný, ale řešitelný úkol.

Ani u vozidel s plně automatizovaným řízením nebude možné vyloučit určitou poruchovost. Může dojít k chybě operačního systému, zkratu na některé z desek s tištěnými spoji atd. Největší nebezpečí ale bude od hackerských útoků.

Počítače v autech s automatizovaným řízením budou mít operační systém, který bude ovládat téměř vše. Tyto operační systémy se ve svém počátečním stadiu budou muset častěji aktualizovat, aby dokázaly lépe řešit různé situace na silnicích. Až na některé možné výjimky se plánuje, že aktualizace budou probíhat přes internet.

Každé zařízení připojené k internetu má jedinečné „internetové“ číslo, kterému se říká IP adresa. Je to obdobné jako například u elektronické pošty, kde je možné mít se stejným názvem pouze jediný e-mail. Pokud se hackerům podaří přiřadit tuto adresu ke konkrétnímu vozidlu, které je připojené k internetu, mohou se pokusit proniknout do jeho operačního systému. Když se jim to podaří, mohou získat plnou kontrolu nad celým vozidlem, a to včetně brzd, řazení, zatáčení, … Demonstrativní ukázky převzetí plné kontroly na vozidly jsou odstrašující. Naštěstí se na zmíněných videích [27–29] jednalo pouze o předem domluvené hackerské útoky, které měly jen poukázat na bezpečnostní hrozby. Hackeři ale také mohou zkoumat internetovou síť v určité oblasti a za určitých okolností mohou určit, které IP adresy zřejmě patří k vozidlům pohybujícím se na vymezeném území. Když budou vědět, jak se „nabourat“ do operačního systému některých značek aut, není pro ně potom tak těžké dostat se k řízení třeba i několika tisíc aut současně, a to třeba jen s pomocí jednoho počítače připojeného k internetu. Pokud by všem vozidlům, jejichž řízení by měli pod kontrolou, dali například v určitý okamžik příkaz prudce zatočit a zabrzdit, zatočit a přidat plyn apod., vyvolali by na silnicích doslova masakry. Na dálnicích by díky větší rychlosti vozidel byla situace vážnější. Výsledkem stisknutí „jediného“ tlačítka by během několika sekund mohly být tisíce mrtvých a raněných osob a v některých případech by tyto počty mohly dosahovat mnohem vyšších hodnot. Takový teroristický útok by u lidí vyvolal ohromné obavy a došlo by k dočasnému omezení zásobování, krátkodobému snížení tržeb většiny podnikatelů, zkrátka by hospodářství mohl přivodit ztráty v rozsahu až několika miliard, nebo dokonce desítek miliard korun. Lidské ztráty by samozřejmě byly nedocenitelné. Nejhorší by bylo, že by se takový útok mohl opakovat a je jedno, jestli by za ním stál kupříkladu nějaký osamocený hacker či nějaká zpravodajská služba libovolné země světa.

Auta napojená na internet mohou být ideálním pomocníkem pro vydírání, likvidaci „nepohodlných“ lidí (někteří novináři, politici, …), poškození hospodářství, odstranění vlády, která nechce plnit něčí příkazy, apod. S trochou nadsázky lze říct, že stisknutím tlačítka se dá ochromit celá ekonomika, a to aniž by bylo nutné proniknout do počítačů elektráren, vodáren a jiných klíčových společností.

Není rozumné spoléhat se na to, že výrobci aut dokážou zabezpečit počítače ve svých vozidlech proti hackerům. Výrobci operačních systémů určených pro běžné počítače i servery se snaží ochránit své systémy před útoky hackerů, ale zatím se jim nepodařilo vytvořit takový program, který by před hackery poskytoval 100% ochranu. I kdyby například jedna automobilka nějakým zázrakem dokázala naprogramovat takový operační systém, který by byl plně bezpečný, byl by to jen částečný úspěch, protože auta od ostatních automobilek by stále představovala bezpečnostní hrozbu. Navíc při aktualizacích se občas stává, že se vytvoří nové bezpečnostní „díry“.

Někteří lidé si mohou myslet, že pokud by jezdili zejména ve starších vozidlech, která by neměla řízení ani částečně ovládané počítačem, že by byli v bezpečí. Především u novinářů, kteří odkrývají nejrůznější podvody, trestné činy apod., nebo „nepohodlných“ politiků by stačilo k jejich likvidaci použít například jakékoli protijedoucí vozidlo, které by šlo na dálku ovládat, a bylo by zcela jedno, v jakém vozidle by jeli. Podobný osud by je mohl potkat i za situace, kdyby šli po chodníku či by se pohybovali na jiných místech hlavně poblíž silnice. V těchto případech by nemuselo být možné jednoznačně prokázat, že se jednalo o úmyslný trestný čin.

Návrh řešení k ochraně občanů před automatickým řízením automobilů

Pokrok v oblasti automobilového průmyslu je dobré podporovat, protože počítače dokážou stále přesněji a rychleji vyhodnocovat různé kritické situace a reagovat na ně, ale je nutné zajistit, aby byl v souladu se zájmy lidí. Aby byla výše zmíněná vozidla bezpečná, je zapotřebí zabránit jejich „napadení" prostřednictvím jakékoli bezdrátové sítě, tzn. že musí mít trvale odpojenou řídicí jednotku od všech bezdrátových sítí. Její aktualizace musí být prováděná pouze kabelovým připojením v servisu. Některé automobilky si uvědomují riziko plynoucí z trvalého připojení k internetu, a proto softwarově připojují řídicí jednotku k internetu pouze za účelem aktualizace. Toto řešení také není zcela bezpečné, protože pokud se do řídicí jednotky dostane vhodně naprogramovaný počítačový virus, může zajistit připojení k internetu v libovolnou dobu.

Pro bezpečný provoz těchto vozidel je zapotřebí nahrát potřebné mapy na vnitřní datové úložiště řídicí jednotky, aby nemusela být navigace připojená ani k síti GPS, GLONASS atd. Svoji polohu si vozidlo dokáže snadno zjistit například jen z rychlosti, času a kamerového záznamu. Mapy ve vnitřní paměti řídicí jednotky by se musely opět aktualizovat přes kabelové připojení. V současné době již není problém vložit do paměti jednotky případně podrobnou mapu celé Evropy. Sice by se jednalo o snížení určitého pohodlí uživatelů, protože vozidlo by nemělo přístup k informacím o dopravních zácpách, nehodách a podobně, a tedy by si samo nemohlo nastavit vhodné objízdné trasy, ale z hlediska bezpečnosti by to bylo jediné řešení. Pokud by posádka vozidla chtěla být informovaná o dopravních zácpách atd., a z toho důvodu by chtěla mít možnost ovlivnit trasu, musela by mít externí navigaci připojenou k internetu.

Nechat jezdit nezabezpečená auta po silnicích může být mnohem větší problém, než prodávat zbraně ve volném prodeji osobám starším 18 let, tj. v tomto případě osobám bez zbrojního průkazu. Nezabezpečená vozidla představují odjištěnou zbraň, a mohou být hrozbou i pro svého majitele. Majitelům nezabezpečených vozidel by se určitě nelíbilo, kdyby byli trestně odpovědní za případné ohrožování, zranění či zabití jedné či několika osob svým vozidlem v případě hackerského útoku. Zatímco na střelnou zbraň se musí dělat zkoušky, na tato vozidla se žádná omezení nevztahují (kromě platného řidičského průkazu), i když dokážou udělat mnohem větší problémy, než nějaký osamělý střelec, byť třeba s legálně drženou zbraní.

Protože auta s různým stupněm automatizovaného řízení se již běžně prodávají, je nutné v nejbližších měsících přijmout důrazná opatření. Auta, jejichž řídicí jednotka, případně i navigace napojená na řídicí jednotku, se může připojit k bezdrátové síti, musí být zbavena homologace pro provoz na pozemních komunikacích v České republice. U stávajících vozidel je zapotřebí znemožnit připojení řídicí jednotky k bezdrátovým sítím. To znamená, že toto odpojení nelze řešit softwarově, ale pouze fyzicky.

V rámci ochrany občanů České republiky bude nutné na hranicích zajistit kontroly vozidel, třeba jen ve smontovaných halách, a všem autům, která nebudou mít výše uvedenou úpravu, neumožnit vjezd na území České republiky. Toto opatření by současně řešilo problémy s ukradenými auty, díky kontrole technických průkazů, omezilo by se pašování drog a zbraní, …

Protože o tomto problému se běžně ví již několik let, tak lze předpokládat, že v rámci boje proti terorismu se tímto problémem již dlouhodobě zabývá Bezpečnostní informační služba (bylo by žádoucí BIS poučit, že by u svých kontaktních informací [příloha č. 5] měla uvádět datovou schránku) a zároveň to zajisté tvoří značnou část pracovní náplně nově zřízeného útvaru nazvaného Centrum proti terorismu a hybridním hrozbám. *Dosud jsme nezaznamenali žádné kroky Úřadu vlády České republiky ohledně řešení této hrozby, a proto se na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ptáme na studii (včetně evidenčního čísla v rámci elektronické evidence pošty) o těchto bezpečnostních hrozbách, ve které nepochybně je i časový plán na zabezpečení hranice České republiky a způsoby homologování těchto vozidel. Studii stačí nakopírovat na přiložené DVD. Odpověď prosíme písemně ve 30denní lhůtě od obdržení tohoto dopisu.* V případě neposkytnutí odpovědi na tento dotaz budeme au-

tomaticky předpokládat, že vláda ČSSD a ANO zřejmě hájí zájmy nadnárodních společností na úkor zdraví a životů občanů České republiky, a to navzdory všem ujištěním, které veřejnosti dává. Taková ujištění lze potom považovat za dezinformační kampaň, kterou by mělo prošetřit minimálně Centrum proti terorismu a hybridním hrozbám. Každý si zajisté dokáže udělat sám názor, jestli vláda ČSSD a ANO jedná v souladu se zájmy občanů České republiky.

Přílohy

1. Dopis týkající se EET, který byl odeslán na Ministerstvo financí 14. 12. 2016.
2. Dílčí odpověď Ministerstva financí k dopisu v příloze č. 1.
3. Rozhodnutí Ministerstva financí k dopisu v příloze č. 1.
4. Dopis týkající se návrhu mýta, který byl odeslán na Úřad vlády České republiky 24. 7. 2016.
5. Chybějící název datové schránky u kontaktních informací BIS.
6. Stav projednávání novely zákona č. 289/2005 Sb., o Vojenském zpravodajství.

Použité zdroje

1. Generální finanční ředitelství. *etržby - Férově pro všechny* [video]. 6. 6. 2016 [cit. 15. 2. 2017]. Dostupné z: https://www.youtube.com/watch?v=-LubYoMYhOU. Reklama trvá 30 s.
2. BDO. *Specifika projektu: elektronická evidence tržeb* [online]. Verze 1.22. Únor 2015, revize leden 2016 [cit. 15. 2. 2017]. Dílčí revize MF. Dostupné z: http://www.mfcr.cz/assets/cs/media/Studie_EET-2015_v02.pdf.
3. Ministerstvo financí. *Závěrečná zpráva hodnocení dopadů regulace (RIA): návrh zákona o evidenci tržeb* [online]. 3. 6. 2015 [cit. 15. 2. 2017]. Dostupné z: http://www.psp.cz/sqw/text/orig2.sqw?idd=114749.
4. Ministerstvo financí. *Metodika výpočtu dopadů zavedení elektronické evidence tržeb* [online]. [cit. 15. 2. 2017]. Dostupné z: http://www.mfcr.cz/assets/cs/media/Informace-zadost-106_2016-09-20_Info-106-99-MF-30553-2016-10-1750IK.pdf.
5. *The Biggest Data Breaches in 2016, So Far* [online]. 16. 12. 2016 [cit. 15. 2. 2017]. Dostupné z: https://www.identityforce.com/blog/2016-data-breaches.
6. *List of data breaches* [online]. Poslední úpravy 14. 2. 2017 3.06 [cit. 15. 2. 2017]. Dostupné z: https://en.wikipedia.org/wiki/List_of_data_breaches.
7. *World's Biggest Data Breaches: selected losses greater than 30,000 records* [online]. Poslední úpravy 5. 1. 2017 [cit. 15. 2. 2017]. Dostupné z: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.
8. *These were the biggest hacks, leaks and data breaches of 2016* [online]. 15. 11. 2016 [cit. 15. 2. 2017]. Dostupné z: http://www.zdnet.com/pictures/biggest-hacks-security-data-breaches-2016/.
9. Identity Theft Resource Center. *Data Breaches* [online]. [cit. 15. 2. 2017]. Dostupné z: http://www.idtheftcenter.org/data-breaches.html.
10. KIRK, Jeremy. *Kaspersky: Banks, Governments, Telcos Hit by Fileless Malware: same attack techniques used to command ATMs to dispense cash* [online]. 9. 2. 2017 [cit. 15. 2. 2017]. Dostupné z: http://www.databreachtoday.com/kaspersky-banks-governments-telcos-hit-by-fileless-malware-a-9678.
11. LORD, Nate. *The History of Data Breaches* [online]. Poslední úpravy 27. 1. 2017 [cit. 15. 2. 2017]. Dostupné z: https://digitalguardian.com/blog/history-data-breaches.
12. GREENWALD, Glenn. *Glenn Greenwald: how the NSA tampers with US-made internet routers* [online]. 12. 5. 2014 [cit. 15. 2. 2017]. Dostupné z: https://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden.
13. ZETTER, Kim. *Stealing Data From Computers Using Heat* [online]. 23. 3. 2015 [cit. 15. 2. 2017]. Dostupné z: https://www.wired.com/2015/03/stealing-data-computers-using-heat/.
14. SANGER, David E. − SHANKER, Thom. *N.S.A. Devises Radio Pathway Into Computers* [online]. 14. 1. 2014 [cit. 15. 2. 2017]. Dostupné z: http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html?hp&_r=0.
15. HUSSAIN, Farzan. *8 Technologies That Can Hack Into Your Offline Computer and Phone* [online]. 14. 7. 2015 [cit. 15. 2. 2017]. Dostupné z: https://www.hackread.com/hacking-offline-computer-and-phone/.

16. *MIT vytvořil dopravní model z údajů o poloze uživatelů mobilních telefonů* [online]. 5. 9. 2016 [cit. 15. 2. 2017]. Dostupné z: http://www.smartcityvpraxi.cz/moderni_technologie_11.php.
17. ČÍŽEK, Jakub. *Stačí telefonní číslo a hacker vás bude odposlouchávat lépe než NSA* [online]. 7. 6. 2016 [cit. 15. 2. 2017]. Dostupné z: http://www.zive.cz/clanky/staci-telefonni-cislo-a-hacker-vas-bude-odposlouchavat-lepe-nez-nsa/sc-3-a-182655/default.aspx.
18. ŽOFČIN, Maroš. *Odposlech je hračka. O chybě v mobilních sítích se ví roky* [online]. 28. 12. 2016 [cit. 15. 2. 2017]. Dostupné z: http://www.mobilmania.cz/odposlech-je-hracka-o-chybe-v-mobilnich-sitich-se-vi-roky/a-1334338/default.aspx.
19. *Speciál: Elektronická evidence tržeb EET* [online]. 31. 10. 2016 [cit. 15. 2. 2017]. Dostupné z: http://www.businessinfo.cz/cs/clanky/special-elektronicka-evidence-trzeb-eet-71195.html.
20. Poslanecká sněmovna Parlamentu České republiky. *Usnesení výboru pro bezpečnost k vládnímu návrhu zákona č. 289/2005 Sb., o Vojenském zpravodajství* [online]. 14. 2. 2017 [cit. 15. 2. 2017]. Sněmovní tisk 931/4, usnesení výboru pro bezpečnost č. 155. Dostupné z: https://www.psp.cz/sqw/text/orig2.sqw?idd=120909.
21. Privacy International. *What is metadata?* [online]. [cit. 15. 2. 2017]. Dostupné z: https://www.privacyinternational.org/node/53.
22. CRAWFORD, Douglas. *Metadata is Dangerous* [online]. 17. 5. 2016 [cit. 15. 2. 2017]. Dostupné z: https://www.bestvpn.com/metadata-is-dangerous/.
23. Yandex. *Yandex mail* [online]. [cit. 15. 2. 2017]. Poskytovatel bezplatných e-mailových účtů. Dostupný z: https://mail.yandex.com.
24. BRANCH, Philip. *Is it possible to circumvent metadata retention and retain your privacy?* [online]. 30. 3. 2015 [cit. 15. 2. 2015]. Dostupné z: http://theconversation.com/is-it-possible-to-circumvent-metadata-retention-and-retain-your-privacy-39429/.
25. BOGLE, Ariel. *Planning to avoid Australia's data laws? Not all VPNs are created equal* [online]. 13. 10. 2015 [cit. 15. 2. 2017]. Dostupné z: http://mashable.com/2015/10/12/australia-data-retention-vpns/#uTxqDa.Ef8qu.
26. BERKA, Petr. *Dobývání znalostí z databází - mnohostranná interpretace dat* [online]. 4. 10. 2006 [cit. 15. 2. 2017]. Dostupné z: http://sorry.vse.cz/~berka/docs/4iz450/KDDprehled.pdf.
27. DURDEN, Tyler. *Caught On Tape: Hackers Take Control Of A Moving Tesla From Miles Away* [online]. 27. 9. 2016 [cit. 15. 2. 2017]. Dostupné z: http://www.zerohedge.com/news/2016-09-27/caught-tape-hackers-take-control-moving-tesla-model-s-miles-away.
28. SAMSON, Kevin. *Hackers Expose New Method For Disabling Vehicles* [online]. 12. 8. 2015 [15. 2. 2017]. Dostupné z: http://www.activistpost.com/2015/08/hackers-expose-new-method-for-disabling-vehicles.html.
29. DURDEN, Tyler. *470,000 Vehicles At Risk After Hackers "Take Control & Crash" Jeep Cherokee From A Sofa 10 Miles Away* [online]. 21. 7. 2015 [cit. 15. 2. 2017]. Dostupné z: http://www.zerohedge.com/news/2015-07-21/470000-vehicles-risk-after-hackers-take-control-crash-jeep-cherokee-sofa-10-miles-aw.

S pozdravem

(za celý kolektiv)

Jiří Řehoř
Jihovýchodní II 867/4
141 00 Praha 4 – Záběhlice
IČO: 71651632
datová schránka: není
(Podnikatel je zapsán v živnostenském rejstříku vedeném na živnostenském odboru v Praze 4, č. j. ZIV/U33661/2008/MAR.)