Akční plán Pirátů
pro
kybernetickou bezpečnost ČR

Daniel Mazur
daniel.mazur@pirati.cz

květen 2021

1 Autoři, konzultanti a oponenti

konzultující:
Ondřej Profant (https://www.profant.eu/),
Jan Hamal Dvořák (https://wiki.pirati.cz/lide/jan_hamal_dvorak),
Ivor Kollár (https://wiki.pirati.cz/lide/ivor_kollar),
Alexandr Mansurov (https://wiki.pirati.cz/lide/alexandr_mansurov),
Martin Dlouhý ,
Stanislav Zavadil,
Karel Kadlec ,
Roman Šemík (https://romansemik.cz),
Václav Mach (https://www.facebook.com/mach.vaclav)

oponenti:
Adam Řehoř,
Jakub Kočí,
Marek Šebera,
František Navrkal <frantisek.narvrkal@pirati.cz>,
Lukáš Kolářík <lukas.kolarik@pirati.cz>,
Janka Michailidu <janka.michailidu@pirati.cz>,
Bára Soukupová <bara.soukupova@pirati.cz>,
Ondřej Profant <ondrej.profant@pirati.cz>,
Jan Hamal Dvořák <jan.hamal.dvorak@pirati.cz>,
Jan Hora <jan.hora@pirati.cz>,
Ivor Kollár <ivor.kollar@pirati.cz>,
Alexandr Mansurov <alexandr.mansurov@pirati.cz >,
Martin Dlouhý,
Roman Šemík,
Václav Mach,
Michal Ketner <michal.ketner@pirati.cz>,
Daniel Kolář <daniel.kolar@pirati.cz>

Obsah

2 Předmluva

Kybernetická bezpečnost navazuje na obecnou (fyzickou) bezpečnost společnosti. Z pohledu státu se týká především zabezpečení kritických infrastruktur - dodávek pitné vody, elektřiny, paliv,... Vedle zabezpečení životně důležitých aspektů fungování země se potřeba obecné i kybernetické bezpečnosti vztahuje i na komunikaci veřejné správy a občanů, na data a informace.

Z liberálních principů (viz např. David Boaz: Liberalismus v teorii a politice[1]) plyne, že občan při růstu práv[2] a povinností[3] komunikovat s úřady elektronicky má povinnost spolupodílet se na ochraně svých údajů (viz sociální sítě, rozlišování lží/manipulace/demagogie). Zároveň má ale nárok na to, aby úřady všech úrovní chránily jeho údaje[4]. Bezpečnost kyberprostoru (definice tohoto a ostatních pojmů přebírám z nedávné publikace CZ.NIC[5], které jsou tak v souladu s termíny používanými v legislativě) je úkolem pro každého jednotlivce, stát pro ni nicméně musí vytvořit vhodné prostředí - technologicky, legislativně, organizačně. Stát určuje pravidla, jaké údaje o občanech a právnických osobách vyžaduje, zpracovává a uchovává, proto je na úrovni státu nutné činit všechny dostupné kroky k ochraně dat proti únikům a manipulaci.

Akční plán kyberbezpečnosti (APKB) odpovídá na tuto široce definovanou povinnost státu v geopolitické realitě roku 2020 z pozice Pirátů. APKB je jednou ze vzájemně provázaných součástí akčního plánu informačních technologií resp. digitalizace a překrývá se částečně s Akčním plánem podpory open source[6]. APKB se jen okrajově dotýká aktivit Vojenského zpravodajství a informačních služeb v kyberprostoru. Kybernetická bezpečnost je jednou z nejvyšších priorit moderního státu podobně jako již tradičně obrana a bezpečnost občanů a majetku ve fyzickém světě. Proto očekáváme nutnost zodpovědného řešení případných nesouladů mezi APKB a stávajícími strategiemi a akčními plány[7] Vlády minimálně tím způsobem, že bude perspektiva APKB zahrnuta mezi okrajové podmínky pro implementaci uvedených starších strategických dokumentů.

[1] David Boaz: Liberalismus v teorii a politice, Liberální institut, Praha 2002, ISBN 80-86389-23-5

[2] např. Zákon o právu na digitální služby, `https://www.zakonyprolidi.cz/cs/2020-12`

[3] např. Zákon o evidenci tržeb, `https://www.zakonyprolidi.cz/cs/2016-112`

[4] např. Zákon o zpracování osobních údajů, `https://www.zakonyprolidi.cz/cs/2019-110`

[5] Kolouch J., Bašta P. a kol., CyberSecurity, 2019, CZ.NIC, `https://knihy.nic.cz/files/edice/cybersecurity.pdf`

[6] Například důraz na využívání a rozvoj open source technologií má jednak rovinu kyberbezpečnostní (auditovatelnost), jednak hospodářskou (sdílení zdrojů a šetření jimi), politickou (nezávislost) a strategickou (soběstačnost). Viz Koubek L., Profant O. a kol. Akční plán pro boj s vendor lock-inem a rozšíření využití open source ve veřejné správě, 2019, ČPS, `https://www.pirati.cz/assets/pdf/akcni-plan-opensource-v3.pdf`

[7] např. "Akční plán pro rozvoj digitálního trhu", `https://www.vlada.cz/assets/media-centrum/aktualne/ma_KORN9YAKXSHL_REV_2-fin.pdf`

3 Pojmy a zkratky

APKB	Akční plán kybernetické bezpečnosti (tento dokument)
BOZP	bezpečnost a ochrana zdraví při práci
bug bounty	program odměn za vyhledání a nahlášení chyb v software, který vyhlašovatel používá
FOSS,FLOSS	free/libre open source software; svobodný software s otevřeným zdrojovým kódem
HW	hardware
ICT	informační a počítačové technologie
NCKB	Národní centrum kybernetické bezpečnosti
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OHW	otevřený hardware
OSS	open-source software; software s otevřeným zdrojovým kódem
OSVS	otevřený software pro veřejnou správu
ransomware	škodlivý software, který požaduje výkupné za obnovení přístupu k datům, která předtím zašifroval
RSA	Rivest-Shamir-Adleman - druh šifry s veřejným klíčem
SW	software
VZMR	veřejná zakázka malého rozsahu
ZZVZ	Zákon o zadávání veřejných zakázek

4 Motivace: Kyberbezpečnost jako klíčový aspekt ICT ve veřejné správě

4.1 Proč řešíme bezpečnost v kyberprostoru

Data jsou nejcennější komoditou této doby.[8] Rychlost přístupu k datům, jejich zpracování a rozhodování na základě dat je konkurenční výhodou mezi podniky, mezi jednotlivci i celými státy.[9] Rozhodnutí je nutné činit na základě důvěryhodných dat, což znamená nejen nutnost kontroly důvěryhodnosti zdrojů, ale i zabezpečení informace po cestě k nám. Zároveň roste složitost procesů ve společnosti, čemuž se snažíme čelit[10] zapojením počítačů. To vše tlačí dopředu digitalizaci dat a procesů a jejich přesun do kyberprostoru. Kyberprostor nemá geografická omezení fyzického světa, takže je například ztížená identifikace a sekvestrace pachatelů nezákonné činnosti. O to nezbytnější je důraz na pasivní a preventivní opatření. Součástí kyberprostoru jsou systémy, na nichž závisí životy, soukromí a majetek lidí, fungování státu a společnosti jako celku.

4.2 Aktuálnost

Zprávy o narušení kybernetické bezpečnosti (kybernetických útocích, únicích dat, vyřazení infrastruktur z provozu) se v mainstreamových médiích objevují průběžně. Policie ČR trestné činy spáchané v kyberprostoru monitoruje od roku 2011 a uvádí setrvale rostoucí počet incidentů.[11] Opakované úspěšné útoky proti českým nemocnicím se stamiliónovými škodami a dalším významným cílům[12][13][14][15] jasně ukazují důležitost kybernetické bezpečnosti.

4.3 Legislativní kontext

Kyberbezpečnost jako disciplína ochrany dat a komunikačních kanálů využívaných veřejnou správou a při interakci s ní se v české exekutivě objevuje v roce 2011 se schválením Strategie pro oblast kybernetické bezpečnosti ČR na období[16] 2012 – 2015 a souvisejícím akčním plánem. Kyberbezpečnost byla následně zakotvená v české legislativě[17] od roku 2014 (orientační seznam zákonů a vyhlášek souvisejících s informačními technologiemi veřejné správy a tedy s kyberbezpečností je uvedený v samostatné sekci). Prováděcím předpisem je vyhláška o kybernetické bezpečnosti;[18] oba tyto základní předpisy s komentáři jsou součástí zmíněné

[8] Na důležitost dat upozornily celosvětově případy vytěžování dat v politických kampaních, ať už data uživatelů sociálních sítí (Cambridge Analytica a referendum o odchodu Spojeného království z EU, `https://www.theguardian.com/news/series/cambridge-analytica-files`) nebo přímo únik komunikace volebního štábu (prezidentská kampaň v USA, qurlhttps://www.theguardian.com/us-news/2016/nov/06/wikileaks-emails-hillary-clinton-campaign-john-podesta).

[9] Glenn Finch et al., Analytics: The speed advantage, 2014, IBM Executive report, `https://www.ibm.com/downloads/cas/OY83D1A4`

[10] Herbert A. Simon, Designing organizations for an information-rich world, ve sbírce M. Greenberger (Ed.), Computers, communications, and the public interest, 1971, Baltimore, MD: The Johns Hopkins Press.

[11] `https://www.policie.cz/clanek/kyberkriminalita.aspx`

[12] `https://zpravy.aktualne.cz/domaci/kyberutok-zpusobil-brnenske-fakultni-nemocnici-skody-v-desit/r~2608ab6c808411ea9d470cc47ab5f122/`

[13] `https://www.novinky.cz/krimi/clanek/ucet-za-kyberutok-na-nemocnici-v-benesove-je-59-milionu-pachatel-se-nenasel-40333644`

[14] `https://www.novinky.cz/domaci/clanek/nukib-za-kyberutokem-na-ministerstvo-zahranici-je-cizi-stat-40293037`

[15] `https://zpravy.aktualne.cz/domaci/z-pocitacove-site-hradu-unikla-data-do-zahranici/r~8b9a464c5d3011ea8b230cc47ab5f122/`

[16] `https://www.govcert.cz/download/legislativa/container-nodeid-719/20120209strategieprooblastkbnbu.pdf`

[17] Zákon č. 181/2014 Sb. o kybernetické bezpečnosti, `https://www.zakonyprolidi.cz/cs/2014-181`

[18] Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti, `https://www.zakonyprolidi.cz/cs/2018-82`

publikace CyberSecurity.

4.4 Organizace veřejné správy ČR s aktivní rolí v oblasti kyberbezpečnosti

1. Národní úřad pro kybernetickou a informační bezpečnost[19] (NÚKIB) a v jeho rámci
   - Sekce informační bezpečnosti
   - Národní centrum kybernetické bezpečnosti (NCKB)
   - Vládní CERT České republiky (govCERT.cz)
2. Nevládní sdružení CZ.NIC[20]
   - Národní CSIRT České republiky (CSIRT.CZ)

4.5 Ambice a cíle pro veřejnou správu ČR

Obecně se veřejná správa musí zasadit fungování své, svých systémů a systémů (infrastruktur), na nichž závisí fungování společnosti. Takovými infrastrukturami jsou elektrárny a přenosové soustavy, vodárny a čističky vod, rozvody a vysílače telekomunikačních sítí apod až po systémy finančního sektoru.

Citujme z publikace CyberSecurity, str. 57: ***Domníváme se, že je utopické si myslet, že je možné vytvořit absolutní kybernetickou bezpečnost či absolutně zabezpečený systém, v rámci něhož jsou využívány prvky ICT. ... Jakýkoliv systém je tak bezpečný, jak bezpečný je jeho nejslabší článek (prvek).***

U vědomí toho musí veřejná správa usilovat o maximální přiblížení k ideálu (kyber)bezpečnosti za cenu zdrojů, které na to dle mandátu smí uvolnit. Stav žádoucí k dosažení a udržení odpovídá následujícím tezím:

- Kritická infrastruktura veřejné správy je zabezpečená proti vyřazení z provozu zásahem z kyberprostoru (tj. kyberútokem).
- Informace (data) shromažďované veřejnou správou jsou zabezpečené proti zničení, odcizení, únosu a falzifikaci, a to jak na úložištích tak při přesunech.
- Informační systémy veřejné správy jsou zabezpečené proti vyřazení z provozu.
- Je zajištěna optimální kompetentnost pracovníků v celém rozsahu veřejné správy a kritických infrastruktur.

Poslední cíl je zároveň ambicí i prostředkem k dosažení ostatních uvedených cílů.

4.6 Principy a prvky kybernetické bezpečnosti

O dosažení stavu kybernetické bezpečnosti lze mluvit, když jsou najednou naplněny tři podmínky: ***důvěrnost*** (data jsou přístupná pouze oprávněným entitám), ***celistvost*** (data mohou být měněna pouze k tomu oprávněnými entitami) a ***dostupnost*** (data jsou oprávněným entitám dostupná, kdykoli jsou vyžádaná). Pro tyto tři podmínky se vžil souhrnný pojem ***triáda CIA***[21].

[19] `https://www.nukib.cz/cs/`, vznikl 1. srpna 2017 na základě zákona číslo 205/2017 Sb.

[20] CZ.NIC chrání důvěrnost aktiv proti neautorizovanému vyzrazení. Sdružení implementuje bezpečnostní politiku informací konzistentně, plánovitě a ekonomicky efektivně." `https://www.nic.cz/page/351/`

[21] viz např. `https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-cia-triad/`

Stav kybernetické bezpečnosti lze do určité míry vytvořit optimálním nastavením interakcí mezi třemi prvky: ***lidmi***, ***technologiemi*** a ***procesy***. Tyto prvky rozděluji do více skupin pro snazší práci v rámci tohoto dokumentu.

5 Lidé: Znalostní společnost a rozvoj lidského kapitálu

Důraz na vzdělání všech členů společnosti, ideálně s maximalizací využití potenciálu každého jednotlivce, je klíčovým programovým bodem Pirátů od počátku existence České pirátské strany. Lidský kapitál národa je klíčový v konkurenci ostatních národů. Věřím, že když se jej podaří maximálně zúročit, dokáže ČR jako celek překonat téměř každý hendikep naší země v jiných oblastech – velikost země, stále ještě mládí a nezkušenost naší demokracie, nedostatek strategických surovin a podobně. Lze spekulovat[22], že všechny tyto nevýhody lze vnímat jako stimulující faktory našeho rozvoje a je možné v dlouhodobém horizontu obrátit ve výhodu.

5.1 Pracovníci v ICT veřejné správy

5.1.1 Legislativní rámec zaměstnání ve veřejné správě a dopad na ICT

Zaměstnání ve veřejné správě (ne v obchodních společnostech založených státní správou nebo samosprávou) znamená téměř univerzální podmínky pro zaměstnance bez ohledu na to, jaká je (ne)dostatkovost dané profese v komerční sféře, a tedy jaké jsou podmínky. Pro veřejnou správu je typické:

- **tabulkové platy** a neochota veřejné správy inzerovat pozice s reálným platovým ohodnocením - osobní ohodnocení a odměny jsou typicky zastropované ve vztahu k tabulkovému platu, zájemce o práci se předem nedozví svůj plat – odměňování není srozumitelné ani dostatečně transparentní
- práce monitorovaná **od hodiny** na pracovišti, ne od splněného úkolu
- nadstandardní **dovolená** a některé další benefity (s tímto se soukromá sféra ale již zvládla vyrovnat; i mezi sebou IT firmy v současnosti zaměstnance přetahují benefity, ne výplatou)
- **ochrana pracovníků** na jejich pozicích (jinak též ochrana pracovních míst: obtížné rozvázání pracovního poměru, u státní správy a vedoucích odborů promlouvá i služební zákon)
- velká **byrokratická zátěž**, která (navzdory poučkám o správném řízení) se zapojením ICT nezmenšuje
- **prostředí málo motivující** k dělání práce navíc, k osobnímu rozvoji, k navrhování vlastních "zlepšováků" pro pracoviště či instituci
- větší či menší **prolnutí politiky** do úřadů, a tím i vlivu stranických konexí pracovníků; díky politicky nominovaným správním a dozorčím radám se toto týká i firem zřizovaných samosprávou.

5.1.2 Bariéry budování a udržování expertních týmů ve veřejné správě

Od konce dotcom éry (1995–2001 se rozvíjela bublina v USA, k nám tento boom dorazil rozmělněný v prvním desetiletí 3. tisíciletí) je po pracovnících v ICT značná poptávka napříč společností. To vyhnalo jejich cenu na trhu práce vzhůru a příjmy seniorních odborníků na kybernetickou bezpečnost nyní často přesahují i platy starostů a tajemníků úřadů největších městských částí. Pracovníci ICT jsou tedy ve veřejné správě

[22]Isaac Asimov, *Foundation*, Gnome Press (1951)

placeni méně než by je zaplatil trh a v důsledku toho nemá veřejná správa přístup (statisticky vzato) k těm nejlepším v oboru. Zároveň díky masivnímu outsourcování IT služeb jsou ICT pozice na úřadech téměř 100% degradované na uživatelskou podporu kolegům-úředníkům při problémech - z odborného hlediska - triviálních. To je pro pracovníky na úrovni inženýra ICT silně demotivující a při setrvání ve veřejné správě je nesnadné udržet odbornou kvalitu.

5.1.3 Cesty k získání kvalifikovaných ICT pracovníků

1. **Samosprávy a kraje**:
   - angažování schopných tajemníků úřadů s výbornými obecně manažerskými schopnostmi (měli by odbourat nadbytečnou byrokracii, zavést motivující schémata odměňování na základě splněných úkolů, volnou pracovní dobu, požadavek na in-house údržbu a vývoj maxima z využívaných informačních systémů)
   - sdružování samospráv k využívání identických ICT řešení a tím umožnění (a) sdílení IT odborníků mezi úřady (b) povolování financí pro vývoj vlastních produktů (za předpokladu získání úplných práv k produktu (OSS), a tedy zapojení vlastních ICT pracovníků do vývoje)
   - snižování outsourcingu IT služeb, vzdělávání a zapojování ICT pracovníků v projektech vývoje používaných informačních systémů
2. **Ministerstva, vláda**:
   - tlak na otevřené systémy, aby ICT pracovníci mohli sami pracovat na údržbě a vývoji, (ne triviální uživatelská podpora a hlášení požadavků externím firmám)
   - využívání vlastních ICT týmů k pilotování (a ladění) nových řešení pro úřad nebo jeho agendu
3. **Legislativa**:
   - rozvolnit pravidla pro finanční hodnocení pracovníků veřejné správy ve prospěch „situace na trhu“
   - zákoník práce (pojištění atd.), zákony o krajích, o obcích, o hl. m. Praze, zákon o státní službě a zákon o úřednících územních samosprávných celků: snižovat formální bariéry spolupráci a sdílení zdrojů mezi entitami v samosprávě
   - přijetí zákonů analogických francouzskému „o digitální republice“ a americkému o povinném sdílení zdrojových kódů ve veřejném prostoru

5.2 Ostatní pracovníci veřejné správy

Za naprostou většinu úspěchů kybernetických útoků může lidské selhání[23]. Proto jsou mezi nástroji útoků stále populárnější trojští koně šířící se pomocí e-mailů a komunikačních platforem (messengerů). Z tohoto důvodu jsou ale také právě laičtí uživatelé ICT úřadů kritickou součástí obrany veřejné správy proti těmto

[23] https://blog.getusecure.com/post/the-role-of-human-error-in-successful-cyber-security-breaches, https://cyberprimed.com/ibms-cyber-security-intelligent-index-indicates-that-95-of-all-security-incidents-involve-human-error/

útokům. Úplná zabezpečení koncových stanic a dalších zařízení úřadů proti lidským chybám (tzv. blbuvzdorná řešení) často vedou k praktické nepoužitelnosti zařízení k běžné práci (dlouhé ověřovací procedury, následně nízká produktivita) a tudíž k vědomému obcházení pravidel a doporučení[24].

Aniž bychom měli k dispozici statistiku, lze očekávat, že má většina úřadů má s souladu se zákonem[25] implementované směrnice o vzdělávání zaměstnanců. Vzhledem k důležitosti a dopadu uživatelské kompetentnosti pracovníků je ale zároveň na místě ze všech úrovní podporovat implementace pravidelných školení kybernetické a informační bezpečnosti.

Proto je zcela zásadní udržovat vzdělanost všech zaměstnanců veřejné správy na úrovni přijatelné pro kybernetickou bezpečnost práce. Tento termín volíme záměrně: Tak jako snaha chránit výrobní zdroje vedla k zavedení pravidelných školení bezpečnosti a ochrany zdraví při práci (BOZP) vztahující se i na úřednické profese, stejný krok musí udělat veřejná správa ve věci správného používání ICT z hlediska kybernetické bezpečnosti. Pro účinnou implementaci už existují funkční vzdělávací řešení, které zahrnují webináře i pravidelné rozesílání "trénovacích" phishingových e-mailů všem zaměstnancům.

5.3 Informační a kybernetická gramotnost v populaci

Podle medializovaných průzkumů i odborných publikací (CyberSecurity) jsou informační a kybernetická gramotnost ve společnosti na nedostatečné úrovni. Přitom pokud jde o odborníky – absolventy veřejných vysokých škol v oborech souvisejících s informatikou, kybernetikou a využitím kyberprostoru – nelze říci, že bychom jako země zaostávali. Naopak to, že světové popularity dosáhly antivirové produkty Avast! a AVG, které se nadále udržují na špici, je pozitivním signálem.

Oblast ICT, internet a kybernetické hrozby se velmi rychle vyvíjejí a populace – neodborná veřejnost – logicky zůstává nedostatečně poučená. Oblastí k zaměření veřejné správy jsou proto:

1. poučení o zásadách kybernetické bezpečnosti v každé interakci občana s úřadem (v jednoduchých, přístupných a praktických radách) podobně, jako to dělá většina bank v komunikaci se svými klienty,
2. v rámci regionálního školství působení na osvětu k chování v kyberprostoru, ideálně zahrnující nejen žáky, ale i jejich rodiče,
3. popularizace témat kyberbezpečnosti v hlavních médiích, zejména v televizi.

6 Technologie: K bezpečnosti cestou otevřeného designu

Ze technologie označujeme soubor hardwarových a softwarových řešení zahrnující (1) *implementaci* hardware (sestavy sítí, serverů a koncových stanic) a software (aplikací informačních systémů), (2) použité *algoritmy a formální struktury* pro reprezentaci, uchovávání a přenos dat.

Na úrovni designu hardware či výběru algoritmů pro software je optimalizace vždy možná jen v historickém kontextu, tedy podle toho, jaké architektury a algoritmy jsou k dispozici v daném místě a čase. Například kryptografické algoritmy nyní prakticky neprolomitelné (RSA) se mohou stát bezcennými[26,27], jakmile dojde

[24] analogicky k `https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/10/01/why-the-rule-of-law-suffers-when-we-have-too-many-laws/`, `https://www.cato.org/publications/commentary/law-complicated-why-shouldnt-ignorance-be-excuse`

[25] zákon č. 312/2002 Sb., o úřednících územních samosprávných celků

[26] `https://www.root.cz/clanky/kvantove-pocitace-jako-hrozba-na-kterou-nejsme-pripraveni/`

[27] Podle některých dohadů to už nastalo. Již se ale také vyvíjejí kryptografické algoritmy, které mají kvantovým počítačům odolat. `https://cs.wikipedia.org/wiki/Postkvantová_kryptografie`

k praktickému zapojení kvantových počítačů. Pro praktickou kyberbezpečnost ve veřejné správě je ale základním principem, že veřejná správa používá *důvěryhodná hardwarová a softwarová řešení*. Ideální odpovědí na tento požadavek je zásada používání tzv. otevřených technologií, tedy technologií, které umožňují veřejné správě (1) efektivně ověřit, že HW ani SW neobsahuje bezpečnostní chyby ani záměrná „zadní vrátka" pro ovládnutí systému neautorizovanou stranou, (2) případné bezpečnostní chyby v reálném čase opravit, a to za využití vlastních lidských zdrojů. Tato vlastnost znamená, že jsou taková řešení veskrze *auditovatelná*.

Otevřené technologie dělíme na otevřený hardware[28] (OHW) a software s otevřeným zdrojovým kódem (OSS). OHW je svým způsobem ještě důležitější než OSS, a to kvůli jednosměrné vzájemné závislosti. Zde jsou uvedené úrovně od základní po nejvyšší:

1. **Fyzická vrstva (hardware)** je základní, chyby v ní lze záplatovat skrze firmware, už ne v software běžící na vyšší úrovni – výrobci IC typicky diagramy neposkytují, ale jednou z charakteristik OHW je právě poskytnutí úplné dokumentace výrobcem. Fyzikálními metodami (různé mikroskopie, vysoké náklady, ale díky dostupnosti na veřejných VŠ k dispozici i veřejné správě) je možné diagramy do jisté míry rekonstruovat. Použitím těchto metod je OHW auditovatelný analogicky k OSS.[29]

2. **Firmware**, tedy oživující software integrovaného obvodu. Pokročilé integrované obvody a samozřejmě složená zařízení (např. základní desky PC) mají firmware z továrny a výrobce po různou dobu poskytuje k firmware aktualizace. Mohou ale mít od výrobce HW zabudovaný i další software, o kterém nikdo (mimo výrobce a hackerů) nic neví[30].

3. **Úroveň operačního systému**, ovladačů, komunikačních protokolů vnitřních a vnějších rozhraní.

4. **Úroveň uživatelských aplikací**, tj. serverů, klientů, používání certifikátů a šifrování.

Pouze zcela otevřená řešení mohou být úplně auditovatelná a tím i mít potenciál být zcela důvěryhodná[31]. Je možné je prověřit jak na výskyt chyb, tak na „zadní vrátka" úmyslně umožňující neautorizovaný přístup k datům či úplnému ovládnutí zařízení neautorizovanou osobou. Zcela otevřená zařízení (tzn. zařízení sestavená jako otevřený hardware a s firmware s otevřeným kódem) na trhu v současnosti prakticky neexistují. Řada „zavřených" digitálních součástek (integrovaných obvodů, mikroprocesorů) nemá otevřenou alternativu.[32] Proto je v kontextu OHW třeba zpracovat možnosti podpory jeho vývoje a ve střednědobém horizontu rozšíření jeho využití, včetně komerční sféry.

6.1 Software s otevřeným zdrojovým kódem

V souvislosti se software s otevřeným kódem (OSS) vstupují do hry licenční ujednání[33], tedy práva objednatele na nakládání se SW, zejména na čtení, šíření a vlastní modifikaci zdrojového kódu. Z hlediska

[28] Firmware otevřeného hardware je sám o sobě OSS, aby bylo možné hardware považovat za otevřený.

[29] Optimální k auditu jsou integrované obvody, jejichž tranzistory jsou vyrobené mikronovou technologií, tedy opticky rozlišitelné. Stávající procesory CPU jsou vyrobené 7-nanometrovou technologií, hluboko pod rozlišovací schopností optických mikroskopů. Tyto procesory jsou tím pádem z principu těžko auditovatelné, pokud vůbec; elektronové mikroskopy (SEM) sice mohou mít potřebné laterální rozlišení, ale zobrazují jen povrchovou vrstvu. Integrované obvody CPU jsou vybudované se 3D strukturou a k zobrazení hlubší struktury je tu svrchní vrstvu třeba nejprve odstranit. Všechny metody k odstranění vrstvy v řádu desítek atomárních vrstev způsobují „promíchání" atomů ve směru kolmém na povrch. Není tedy jisté, že po odstranění jedné nebo několika vrstev křemíkové součástky bude pro elektronový mikroskop struktura ještě laterálně čitelná.

[30] viz OS MINIX v procesorech Intel Core, který běží na úrovni -3 a jen výzkum typu reverzního inženýrství objevil jeho existenci

[31] Faktická důvěryhodnost se pak buduje tím, že je systémový audit skutečně provedený a nalezené chyby a "díry" odstraněné.

[32] I poměrně populární produkt CZ.NIC Turris Omnia je otevřený jen částečně, a to díky operačnímu systému OpenWRT.

[33] `https://en.wikipedia.org/wiki/Open-source_software#Comparisons_with_other_software_licensing/development_models`

kyberbezpečnosti je nezbytná alespoň „source-available“ neboli „shared source“ licence, která umožní kompletní audit kódu vzhledem k hrozbám. Požadavky „otevřeného software“ nebo „svobodného software“ pro veřejnou správu, tedy s licencemi přenášejícími dispoziční práva na vlastní modifikaci pro opravy a vývoj, jsou motivované hlavně potřebou bránit vendor lock-in[34]) a tedy snížit náklady veřejné správy. Zabránění vendor lock-in znamená umožnění konkurence mezi dodavateli služeb „údržba“ a „další vývoj“ aplikace. Přesto je zabránění vendor lock-in žádoucí i v souvislosti s kyberbezpečností – možnost vývojářské práce prováděné zaměstnanci veřejné správy pomáhá v budování vlastní expertní báze lidských zdrojů.

Pozn.: ČR je sice členem Open Government Partnership[35], ale v jeho rámci řeší pouze transparentnost a kvalitu práce veřejné správy; o otevřeném OSS v něm není ani slovo.

6.2 Otevřený hardware

Existuje několik iniciativ v akademickém a zejména neziskovém sektoru[36], které otevřený vývoj hardware deklarují jako cíl. Seznam (zdá se, že udržovaný) alespoň částečně otevřených HW produktů včetně Turris od CZ.NIC lze najít na Wikipedii.[37]

Zavřený hardware s otevřeným operačním systémem, např. mobilní telefony Pine64, Purism, Meizu nebo BQ, nebo PiPhone nebo ZeroPhone založené na Raspberry Pi OHW platformě, ovšem z hlediska kyberbezpečnosti považujeme za realizaci postupných cílů na cestě, ne za konečnou metu.

Vývoj hardware v režimu OHW sice může přilákat pozornost velkých firem v případě celních válek mezi mocenskými centry světa, ale obecně je jeho vývoj znevýhodněný tím, že pro masy koncových uživatelů (konzumentů) není kyberbezpečnost jejich zařízení tématem.[38] Je šance, že medializace událostí typu vážných důsledků narušení kyberbezpečnosti (ransomware, který ochromil benešovskou nemocnici a činnost OKD na konci roku 2019) pomůže situaci zlepšit.[39] Zatím je ale povědomí o kyberbezpečnosti v populaci nízké (evropská situace se pravděpodobně moc neliší od výsledků amerického průzkumu[40]). Zároveň platí, že OHW nenabízí úspory v designu a výrobě, proto stabilní producenti uzavřeného hardware zvyklí na patentovou ochranu a patentové soudní války nebudou mít motivaci se do vývoje OHW pustit. Naopak lze očekávat bitvy u soudů a v médiích[41][42] podobné těm mezi velkými IT korporacemi a vývojáři Linuxu.

6.3 Aktivní podpora rozvoje OSS a OHW

Veřejná správa má možnosti podpořit vývoj OSS a OHW, zejména poskytnutím financí pro

- aplikovaný výzkum a vývoj funkčních prototypů,
- projekty proof-of-concept, tedy ověření potenciálu pro komercializaci vynálezů,
- vlastní vývoj OSS pro veřejnou správu,
- programy „bug bounty“ u OSS využívaným veřejnou správou,

[34] https://cs.wikipedia.org/wiki/Proprietární_uzamčení
[35] https://www.opengovpartnership.org/wp-content/uploads/2019/06/Czech-Republic_Action-Plan_2018-2020_CZ.pdf
[36] https://fossforce.com/2019/06/where-open-hardware-is-today/
[37] https://en.wikipedia.org/wiki/List_of_open-source_computing_hardware
[38] https://www.tripwire.com/state-of-security/featured/cybersecurity-is-just-too-much-trouble-for-the-general-public-claims-study/
[39] https://www.welivesecurity.com/2018/10/04/ask-public-cybercrime-cybersecurity/
[40] https://www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/
[41] https://www.linuxexpres.cz/novinky/soud-potvrdil-pokutu-pro-microsoft
[42] https://www.linuxexpres.cz/novinky/oracle-se-nechce-smirit-s-prohrou-ohledne-javy-pravni-bitva

nebo následováním některých dalších (nebo všech) příkladů dobré praxe ze světa (výše).

Podpora OHW se od podpory OSS v něčem bude odlišovat, protože pouze komerční sektor má prostředky pro výrobu v objemech potřebných pro konkurenceschopnost. Zároveň OHW nelze na rozdíl od OSS (viz třeba příklad adopce Nextcloud německou federální vládou) snadno pilotovat v ostrém provozu úřadů – problémy s funkčností software lze snáze ustát než výpadek a ladění hardware.

V rámci podpory OHW z pozice veřejné správy je proto důležité

- adoptovat komerčně racionalizovanou strategii: od mapování potenciálního odbytiště přes plánování výrobků pro trh za 3 až 10 let po začátku projektu až po snahu o co nejčasnější přenesení ověřených konceptů/prototypů do komerční sféry
- hledat cesty motivace tradičních výrobců uzavřeného hardware k zapojení do financovaných projektů,
- nezdráhat se podpory byť jen částečně otevřených řešení jako postupných cílů,
- skrze nastavení pravidel pro projekty z rozvojových fondů EU využívat již vybudované infrastruktury (výzkumné i podnikatelsky akcelerační) v našich velkých městech nebo v příměstských oblastech (Praha – inkubátor VŠE, Dolní Břežany – ELI-Beamlines, Brno – CEITEC, Ostrava – klastr IT4Innovations,...)
- iniciovat spolupráci na těchto projektech nejen v ČR (byť je to ideální z hlediska jurisdikce a vize „soběstačnosti“), ale i v rámci EU.

6.3.1 Legislativa a procesy

Procesy v orgánech veřejné správy, organizacích přímo řízených vládou a ministerstvy a organizacích zakládaných nebo zřizovaných veřejnou správou musí směřovat k naplňování účelu těchto orgánů a organizací v mezích daných zákony. Za účelem nastolení a udržení stavu kybernetické bezpečnosti je třeba vybrat určitý soubor činností a optimalizovat jejich provádění tak, aby se navzájem doplňovaly.

Je vhodné rozpoznat dva pohledy na procesy:

1. Proces má naplnit nějakou část účelu organizace resp. úkolů veřejné správy, tedy například poskytnout službu občanovi, pořídit či evidovat majetek, generovat zprávu (agregovaná data) pro nadřízený nebo kontrolní orgán, a podobně.
2. Proces má představovat takovou manipulaci s daty, která v každém okamžiku naplňuje triádu podmínek kyberbezpečnosti CIA (viz výše), a tedy ideálně všechny relevantní předpisy.

Optimalizace procesu vůči těmto dvěma pohledům není totéž, často se výsledek jedné a druhé naopak výrazně liší. Typicky pohled č. 1 upřednostňuje proces, který minimalizuje náročnost na zdroje veřejné správy, zejména na čas úředního aparátu. Lapidárně řečeno je pohled č. 1 pohodlnější než pohled č. 2, zahrnuje méně úkonů, méně vygenerovaných dokumentů, menší objem komunikace mezi složkami veřejné správy. Pohled č. 2 znamená postup, který neoptimalizuje na „poměr cena/výkon“ a tato kyberbezpečnostní režie může administrativu snadno zahltit. Proto je žádoucí předpisy na všech úrovních (od zákonů po interní regule jednotlivých složek veřejné správy) vytvářet tak, aby představovaly naplnění pohledu č. 2 takové, které je z pohledu č. 1 („poměru cena/výkon“) co nejméně náročné.[43]

[43] viz opět pojednání Herberta A. Simona, odkaz č. 9 pod čarou, str. 40-41.

6.4 Globální kontext

6.4.1 V kyberprostoru jsme všichni sousedé

V reálném prostoru vzájemná vzdálenost zemí do značné míry určuje souvislost mezi vnitřní politikou a ekonomikou jednotlivých zemí a jejich vzájemným, mezinárodním vztahem. Ekonomiky ČR a sousedních zemí jsou propojené, občané a politici jsou velice citliví na jakékoli politické výkyvy v sousední zemi. Mají potřebu reagovat a reakce se mohou pohybovat od verbálního komentáře přes vnitřní opatření (třeba celní, ostraha hranice,…) až po vojenský konflikt. U zemí geograficky vzdálených klesá důležitost společenských, politických a ekonomických rozdílů mezi národy a země velikosti ČR si může dovolit problematické země „neřešit“. Základní vlastností globálního kyberprostoru (fyzicky neseného internetem) je to, že neexistují implicitní bariéry na geografických hranicích zemí. V kyberprostoru neexistuje rozdíl mezi „sousední“ a „vzdálenou“ zemí: kyberútoky jsou vedené stejně snadno ze zařízení na území ČR jako ze zařízení kdekoli jinde po světě, osoby útočníka a zařízení využitá v útoku se mohou vyskytovat jakkoli rozptýlené po světě.

6.4.2 Role ekonomiky a politiky fyzického světa

Reálný svět promlouvá do hledání optimální kyberneticky bezpečná řešení tím, že je špička vývoje hardwarových komponent i nejrozšířenějšího software soustředěná do několika málo geografických lokalit po světě. Něco podobného platí o datových centrech populárních cloudových služeb (Google) a sociálních sítí (Facebook). V důsledku toho jsou svrchované státy jako ČR závislé na technologických výrobcích jiných zemí: masově vyráběný hardware pochází převážně z Číny, Taiwanu, Jižní Korey a Spojených států.[44] Lze se důvodně obávat, že tato závislost již dnes znamená faktické omezení státní suverenity[45] stejného stupně závažnosti, jako je naše závislost na dovozu ropy a zemního plynu. Suverénní státy se obecně snaží udržovat a rozšiřovat svoji suverenitu. Tato pozice je do nějaké míry vyvažovaná právě benefity v oblasti mezinárodní bezpečnosti. Jakkoli nemá na území ČR sídlo žádný globálně významný výrobce hardware nebo operačních systémů, díky postupné harmonizaci legislativy zemí EU lze přistupovat k výrobkům jiných zemí EU jako k méně rizikovým než jsou ty pocházející z vnějšku. Zároveň na úrovni EU existují finanční nástroje/dotační programy, skrze které lze se mohou výzkumné týmy z ČR zapojit do vývoje hardware a software podle našich kyberbezpečnostních potřeb.

Druhým dopadem fyzického světa je dlouhodobé zakořenění tzv. uzavřených řešení, tedy designů a implementací chráněných právními nástroji ochrany duševního vlastnictví. Taková HW a SW řešení jsou z pohledu uživatele černou skříňkou a jejich zabezpečení stojí na fikci „bezpečnosti utajením“.[46] Naproti tomu otevřené technologie, které jsou zároveň na špici vývoje a mohou tak nabízet „bezpečnost od základu“,[47] mají podstatně kratší historii a podstatně menší okruh firem má obchodní model s otevřenými technologiemi

[44] Dominantním producentem součástek a zařízení kompatibilních s 5G standardy je čínská firma Huawei. Vedle mnoha bezpečnostních chyb je argumentem proti jejich používání veřejnou správou vnitřní i mezinárodní politika samotné Číny. Zároveň dominantní výrobci centrálních a grafických procesorů pro osobní počítače Intel, AMD a nVidia mají sídlo ve Spojených státech. Přinejmenším o procesorech Intel je prokázáno, že kromě neúmyslných bezpečnostních chyb (viz videozáznamy z konferencí Black Hat) obsahuje distribuci operačního systému MINIX (`https://www.zdnet.com/article/minix-intels-hidden-in-chip-operating-system/`). Tento operační systém je v továrním nastavení otevřenými „zadními vrátky“ k ovládnutí počítače. Bezpečnostní výzkumníci (`https://www.zdnet.com/article/researchers-say-intels-management-engine-feature-can-be-switched-off/`) už objevili návěští (implementované zřejmě na žádost americké vlády v rámci tzv. programu High Assurance Platform), kterým lze většinu modulů Minixu vypnout, a tím podstatně omezit nebezpečí využití této záměrné díry.

[45] Eva Kislingerová, Ivan Nový a kol., Chování podniku v globalizujícím se prostředí, 2005, C.H.Beck

[46] obvyklý anglický termín je „security by obscurity“

[47] anglicky „security by design“

kompatibilní. To je asi nejvýznamnější slabina[48] plánu na realizaci kybernetické bezpečnosti skrze otevřené technologie.

Při tom všem ale vlády několika států během poslední dekády rozpoznaly roli otevřených technologií z hledisek bezpečnosti i hospodárnosti. Jejich kroky tak tvoří bázi následováníhodných příkladů pro veřejnou správu od legislativní a vládní úrovně po samosprávy. Následuje několik příkladů.

7 Aktivity veřejných správ ostatních zemí hodné následování

7.1 Spojené státy americké

Od roku 2016 platí v USA ustanovení[49], že každá federální agentura každý rok uvolní zdrojové kódy alespoň 20 % software, který si nechala na zakázku vytvořit. Publikace probíhá v doméně `https://code.gov/` . Od té doby mají agentury za povinnost pořizovaný software zasmluvnit odpovídajícím způsobem, tedy včetně práv na publikaci zdrojového kódu. Tuto myšlenku je možné převzít a implementovat i v ČR a přes rozdílech v právních systémech by mělo být možné převzít i odpovídající ustanovení ve smlouvách s dodavateli software.

7.2 Evropská unie

Po ročním pilotu a vyhodnocení EU-FOSSA projektu[50] rozběhla EU v únoru 2019 program „EU Bug Bounty for FOSS“[51], tedy program odměn za vyhledání a nahlášení chyb v 15 vybraných programů typu FOSS (tj. „free open source software“, tedy „svobodný software s otevřeným zdrojovým kódem“).

Fuguje také Open Source Observatory[52], komunitní projekt na úrovni EU sdružující národní a komunální administrativy, soukromý sektor a občany (OSS nadšence, zástupce akademického sektoru apod.) Projekt provozuje znalostní bázi (Knowledge Centre) a poskytuje ad-hoc právní podporu ve věci licencování otevřených řešení pod European Union Public License (EUPL). Za zmínku stojí například projekt ISA[53] zaměřený na propojování platforem v rámci administrativy i mezi stakeholdery za účelem snížení byrokracie.

7.3 Německo

ITZBund roku 2016 pilotovalo a 2017 spustilo ostrý provoz OSS úložiště Nextcloud (Owncloud) pro cca 300 000 zaměstnanců státní správy. Německá veřejná správa tak šla cestou zřízení „soukromého cloudu pro

[48] Otevřenost technologií je z velké části otázkou licenčního modelu, a těch je zejména v oblasti software hodně. Na jedné straně jsou otevřené licence, které umožňují uzavření a komercializaci odvozených děl (FreeBSD, MIT), na druhé licence vynucující otevřenost i pro odvozený software (GNU GPL). Jelikož pro účely kyberbezpečnosti postačují licence volného nakládání se zdrojovým kódem a software pro modifikaci za účelem oprav i dalšího vývoje, v tomto dokumentu neřeším rozdíly mezi open-source software licencemi ani rozdíly mezi ideou „software s otevřeným zdrojovým kódem“ a filosofií „svobodného software“. Striktně vzato i Shared Source Initiative od fy Microsoft vyhovuje požadavku auditovatelnosti software. V posledních letech se děje stále častěji, že velcí výrobci uzavřeného software jako Microsoft, Oracle, Google apod podporují open-source iniciativy a organizace, někdy zakládají vlastní. Zároveň s tím získávají své zástupce ve vedení těchto organizací (např. The Linux Foundation, `https://www.linuxfoundation.org/about/board-members/`), což vede část komunity ke znepokojení a podezření z toho, že postupně dojde k „nepřátelskému převzetí a privatizaci“.

[49] `https://www.cio.gov/2016/08/11/peoples-code.html`

[50] `https://joinup.ec.europa.eu/collection/eu-fossa/implementation`

[51] `https://ec.europa.eu/digital-single-market/en/news/eu-bug-bounty-programme-open-source-software-gives-awards-eur-25000`

[52] `https://joinup.ec.europa.eu/collection/open-source-observatory-osor/about`

[53] `https://ec.europa.eu/isa2/home_en`

potřeby federální vlády“[54] [55]

28.10.2019 byl vyhlášený projekt Národní pakt kybernetické bezpečnosti, který má poskytnout rámec pro propojování (networking) subjektů působících v Německu v oblasti kybernetické bezpečnosti[56] [57]. Dle prohlášení z 19.9.2019 zintenzivňuje spolkové ministerstvo vnitra činnosti k posílení digitální suverenity federální státní správy. Znamená to postupné snižování závislosti na jednotlivých poskytovatelích IT (tedy boj proti vendor lock-in) a vyhledávání alternativ pro některá softwarová řešení. Předpokládá se důraz na řešení s otevřeným zdrojovým kódem.[58] [59]

7.4 Francie

Od 7.10.2016 platí Zákon o digitální republice: Státní správa je aktivním zadavatelem, konzumentem i tvůrcem OSS řešení.[60] Příkladem je OSS platforma Ministerstva práce[61] a komunikační platforma RIOT[62] používaná veřejnou správou.

7.5 Velká Británie

Od 2017 funguje jasný příklon k open source[63]. Běží open source blog a v rámci doporučení k volbě technologických řešení uvádí i kyberbezpečnostní hlediska[64] (např. viz dokument Minimum Cyber Security Standard z roku 2018[65] nebo řada dokumentů s doporučeními[66]).

7.6 Španělsko

Od roku 2012 se státní správa přesunula na OSS. [67] [68] [69]

[54] https://www.zdnet.com/article/open-sources-big-german-win-300000-users-shift-to-nextcloud-for-file-sharing/

[55] https://fossbytes.com/german-government-open-source-cloud-nextcloud/

[56] https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2019/10/nat-pakt-cybersicherheit.html

[57] https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/nationaler-pakt-cybersicherheit/nationaler-pakt-cybersicherheit-node.html

[58] https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2019/09/digitale-souveraenitaet-oeff-verwltg.html

[59] https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.pdf?__blob=publicationFile

[60] https://www.numerique.gouv.fr/publications/politique-logiciel-libre/pratique/#contenu

[61] https://code.travail.gouv.fr/

[62] https://element.io, původně https://riot.im/app/#/welcome

[63] https://www.gov.uk/guidance/be-open-and-use-open-source

[64] https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice-related-guidance#security

[65] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/719067/25062018_Minimum_Cyber_Security_Standard_gov.uk__3_.pdf

[66] https://www.gov.uk/guidance/make-things-secure#related-guides

[67] https://securitronlinux.com/bejiitaswrath/spanish-government-moving-to-open-source-software-take-that-microsoft/

[68] https://www.theinquirer.net/inquirer/news/2265108/spains-extremadura-government-switches-40-000-pcs-to-linux-and-open-source-software

[69] http://techpresident.com/news/22258/governments-autonomous-spanish-regions-are-promoting-open-source-software

7.7 Kazuistika – Linux

Dle seznamu vlád, které nasadily operační systém Linux[70] má za sebou adopce nebo vývoj a nasazení vlastních linuxových distribucí řada zemí na různých úrovních veřejného sektoru. Zvlášť stojí za povšimnutí USA, kde se od Obamy (2009+) Linux prosadil i na běžných koncových stanicích (nepočítáme superpočítače, vojenské drony a jiné podobné systémy), a příběhy z Německa[71] a Švýcarska. Opakovaně se objevuje komentář, že je volba open-source vs. closed-source (Linux vs. Microsoft) činěna politicky, ne na základě technologických nebo ekonomických aspektů. Nicméně bez ohledu na rozhodnutí vlád pracují servery počítačových sítí po celém světě na operačních systémech založených na linuxu.

[70] `https://en.wikipedia.org/wiki/List_of_Linux_adopters#Government` (seznam vypadá dlouho neaktualizovaný)
[71] `https://www.linuxjournal.com/content/german-open-source-experiment-things-not-going-plan`

8 Doporučené priority v kybernetické bezpečnosti pro ČR:

8.1 Priority v oblasti software

8.1.1 Migrace ICT veřejné správy k otevřeným bezpečným řešením - software (P1-S)

Opatření:

1. Definice kategorií otevřeného software pro veřejnou správu (OSVS) a prioritizace pro jednotlivé úrovně veřejné správy (O1-S1) V souvislosti se zaváděním zákona o právu na digitální služby.
2. Mapování globálního rozvoje OSVS, bezpečnostní screening existujících řešení (O1-S2)
3. Formalizace standardů kybernetické bezpečnosti - software (O1-S3)
   - Prosazování skutečných elektronických podpisů (zároveň s návrhem jejich přenosu na otevřené platformy), datových schránek atp.
   - Budování systému podpory otevřených technologií (počínaje seznamem licenčních standardů, které budou definovat množinu "otevřených technologií") vyvíjených třetími stranami včetně (a) placení "dobrovolných příspěvků" na svobodný software jinak zdarma, (b) "bug bounty" soutěže pro dlouhodobou udržitelnost.
   - Kybez aspekty OOÚ mohou směřovat k posunu od autonomních PC jako koncových zařízení na úřadech k pouhým terminálům - bez možnosti skutečně lokální kopie dokumentů. Záhodno zpracovat pro a proti těchto řešení v kontextu skutečné úrovně bezpečnosti dat na lokálních discích.
   - Ve spolupráci s NÚKIB definovat standardy bezpečnosti IT dodávek. Lze navázat na činnost amerického National Institute of Standards and Technology (NIST) a spolupráci s ENISA.

   Pozn.: Část agendy NIST zastává v ČR Český metrologický ústav (ČMI), část agendy zejména pro stavebnictví vede Úřad pro technickou normalizaci, metrologii a zkušebnictví (ÚNMZ). Stojí za úvahu legislativně sjednotit starost o normy (včetně těch kyberbezpečnostních) pod jeden úřad.
4. Budování infrastruktury pro přejímání, sdílení, údržbu a vývoj OSVS (O1-S4)
   - Budovat a udržovat vlastní datová centra pro VS („cloud" mimo organizaci je z hlediska bezpečnosti prostě „cizí počítač") s maximálním zapojením otevřených technologií. Formulovat strategii pro vyvážení centralizace a distribuovanosti, tedy vyvážení rizik podlehnutí jednorázovému útoku (zranitelnější je centralizovaný systém) a náročnosti na zdroje (distribuovaný systém je dražší).
   - Toto je přístup aplikovatelný nezávisle na tom, jestli budou technologie otevřené, uzavřené či co; z pohledu VS je komerční cloud prostě "počítač třetí strany" a jelikož firmy mění majitele bez možnosti zásahu státu, nelze nijak zaručit, že se data nedostanou do rukou "drsných hráčů", kteří budou mít zájem držet VS v šachu a získávat nefér výhody.
5. Procesy hodnocení existujících OSVS a jeho adaptace (O1-S5)
6. Finanční podpora využívaného SW zdarma, komunitního testování a odstraňování chyb (O1-S6)
   - na úrovni samosprávy prosadit formou interní směrnice finanční dotace výrobcům používaného FLOSS úměrně (podle možností, ale je třeba domluvit nějaký algoritmus) cenám komerční konkurence na trhu a počtu reálných uživatelů na úřadě; zde je nutné prozkoumat terén a napříč politickým

spektrem prosazovat hledisko, že toto NENÍ platbou za software zdarma, je to podpora prospěšné činnosti analogická dotacím do sportu nebo kultury nebo do veřejného prostoru skrze participační rozpočty

7. Grantová podpora výzkumu algoritmů pro kybernetickou bezpečnost a vývoje bezpečného OSVS na veřejných výzkumných institucích (O1-S7)

   - Podporovat vývojová centra (výzkum a vývoj HW, SW, algoritmů, implementací) při rozpočtových organizacích/univerzitách. - křemíkové součástky (IC) už dávno mají verze "military" kvality[72], není důvod princip neokopírovat pro HW a SW pro kritické infrastruktury - z příkladu produktů Apple/Macintosh ("it just works") je zjevná výhoda společného vývoje HW a SW (od operačního systému přes ovladače po high-end aplikace) - ze zkušenosti studené války je zjevně zásadní, že se technologie vyvinuté pro armádu a kosmický program dostaly do civilního užití a tím se výzkum a vývoj zaplatily; nyní je ale jiná geopolitická situace a masivní kopírování technologií (nejvíce Čína) znamená vysychání peněz "za duševní vlastnictví"; budou nutné doplňkové strategie, jsou-li jaké

8. Vývoj OSVS: Vlastní, zakázkový, grantový (O1-S8) Zavést zákonnou odpovědnost dodavatele ICT za zranitelnosti odhalené v nějaké době od akceptace dodávky bez ohledu na to, jestli na to smluvní ujednání pamatuje nebo ne. Zákon by poskytoval nějakou dobu na přípravu firem (než vstoupí v platnost), ale v důsledku by znamenal, že má zákazník nárok na to, aby se dodavatel vždy po určitou dobu musel starat o odstranění všech objevených zranitelností v dodaném systému.

9. Zavádění bezpečných OSVS (O1-S9) Pro zavádění SW do jednotlivých pracovních stanic (desktopy, ntb úředníků i zastupitelů)

   - upřednostňovat open source software (FLOSS) pod svobodnými licencemi (GNU GPL, MIT,...); seznam alternativ k obvyklému komerčnímu[73]
   - podporovat (příspěvky na kurzovné) vzdělání úředníků i politiků v používání těchto programů Kategorizovat potřeby úřadů, aby bylo možné pokrýt 90% z jejich počtu standardizovanými řešeními.

   To přinese

   (a) úsporu prostředků na vstupu, dostupnost pro malé obce a jejich svazky

   (b) možnost sdílení podpory v ICT údržbě a vývoji a tedy vytvoření dedikovaných týmů centrální podpory

   (c) přímý centrální dohled na kyberbezpečnost a informační bezpečnost

8.2 Priority v oblasti hardware

8.2.1 Aktivace a rozvoj trhu pro otevřený hardware (P1-H)

Opatření:

[72] `https://www.youtube.com/watch?v=55z_0BYb5is`

[73] například dle `https://downloadpedia.org/alternative/`, ale určitě existují lepší zdroje/seznamy na webu; teoreticky můžeme v návaznosti na AP a tuto kuchařku udržovat vlastní

1. Definice kategorií otevřeného hardware (OH) a prioritizace pro veřejnou správu (O1-H1) Pozn: Hardware nemůže být (až na výjimky) specifický pro veřejnou správu, musí být schopen prosazení v různých segmentech B2G trhu v konkurenci uzavřeného hardware.

2. Globální zapojení do platforem rozvoje OH - mezivládní, iniciativy for-profit i non-profit (O1-H2)

3. Formalizace standardů kybernetické bezpečnosti - hardware (O1-H3)

4. Budování BGA (business-government-academia) partnerství pro vývoj OH, standardů pro OH a budování odpovídající infrastruktury (EU, ČR, V4,...) (O1-H4)

    - Směřování k maximální míře soběstačnosti: Závislost na přísunu součástek, zařízení, software apod ze zahraničí se podobá závislosti na ropě a zemním plynu; z podstaty je nežádoucí (spojenci nejsou navěky)
    - není to zdaleka jen Huawei/Čína[74], problém může být i čip x86 od Intel/USA[75]
    - nutno rozhodnout, kterou cestou cíl soběstačnosti sledovat:
        (a) snaha přivést ČR na úroveň Silicon Valley nebo Taiwanu z hlediska špičkového vývoje i špičkové produkce,
        (b) snaha ČR vytvořit jen "potenciální soběstačnost" ve smyslu zdrojů pro zásadní mezinárodní krizi, např. nákupem "starých" technologií (ve smyslu duševního vlastnictví), které v době krize umožní v kombinaci s výrobci na území ČR během několika měsíců rozjet výrobu zařízení na úrovni (například) 2000-2010, které rozhodně "utáhnou" kritické infrastruktury (byť třeba budou znamenat zpomalení úložišť apod., viz například Betrusted[76]
        (c) jiná cesta (nebo na soběstačnost přiznaně rezignovat...)

5. O1-H5: Grantová podpora budování expertních týmů pro vývoj bezpečného OH

6. O1-H6: Udržitelné plány migrace kritických infrastruktur a veřejné správy na OH

7. O1-H7: Grantová podpora vývoje bezpečného OH (ideálně pro partnerství veřejných výzkumných institucí a průmyslového sektoru) Analogicky k postupům výše (dotace jednotlivých radnic a/nebo společné vývojové týmy) prosadit podporu vývoje otevřeného hardware; OHW nebude nikdy specifické pro veřejnou správu, proto dává smysl spíše model společného financování výzvy na takový vývoj, kde by příjemcem dotace byly VŠ, výzkumné ústavy apod včetně jiných příspěvkových organizací nebo jimi stopro ovládaných firem (CZ.NIC, Operátor ICT, ...)

8. O1-H8: Podpora podnikání ve vývoji prioritního OH pro veřejnou správu Motivovat technologické firmy k fyzickému ukotvení v ČR – strategicky důležité, aby přímo podléhaly zákonům ČR. Snažit se na území ČR mít zástupce všech úrovní vývoje a výroby – od integrovaných obvodů (Tesla Rožnov) přes čidla a kamery (Jablotron) po koncová zařízení typu PC (nemáme). Opatření s tímto cílem musejí být obecné povahy: investiční pobídky, propojení s technickými VŠ, průhlednější pravidla pro podnikání obecně (jednodušší daňový systém...)

[74] https://www.cvedetails.com/vulnerability-list/vendor_id-5979/cvssscoremin-9/cvssscoremax-/Huawei.html, https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200108-01-phone-en

[75] https://www.youtube.com/watch?v=_eSAF_qT_FY , https://www.youtube.com/watch?v=lR0nh-TdpVg

[76] https://betrusted.io/

9. O1-H9: Grantová podpora budování a provozu infrastruktury pro přímý bezpečnostní audit OH jednotlivých zařízení

10. O1-H10: Tvorba legislativy pro podporu zavádění bezpečného OH

11. O1-H11: Návrh a pravidelná aktualizace typizovaného OSS+OHW řešení Uvážit založení městských společností za účelem tzv. "vnitřního outsourcingu" vývoje a údržby SW a HW. Tento model může zmírnit některá omezení veřejné správy (platy a model odměňování), ale vyžaduje pečlivé nastavení vlastnických vztahů zakladatele (obec, město, městská část) vůči produktům společnosti). Špatné nastavení vede často k neefektivitě podobné úřadu nebo k tomu, že obec musí výsledky práce firmě vzít natvrdo rozhodnutím valné hromady (kde musí být obec majoritním vlastníkem, aby to vůbec šlo).

8.2.2 P2: Rozvoj bezpečnosti kritických infrastruktur (KI)

Opatření:

1. O2-1: Měření efektivity procesů a zpětné vazby z auditu Zavést povinnost provozovat testovací prostředí a povinné on-site kyberbezpečnostní testy před ostrým nasazením každého HW, SW i aktualizace.

   - NÚKIB vydává návody a doporučení[77] a provádí bezpečnostní kontroly kritických infrastruktur. Zákony a ostatní předpisy ale neřeší vynucování implementace opatření, která kontrolní a auditní zprávy doporučí.
   - Ani ve spotřebitelské sféře není bezpečnost proti selhání ICT normou, ačkoli např. počítač Apple po pádu operačního systému obnoví i rozdělanou práci (cosi jako hibernace).

   Na revizi legislativy se váže i revize rolí jednotlivých složek.
   - např. NÚKIB má mimo jiné roli informační, ale zprávy o ohrožení [78], např. ransomware v benešovské nemocnici) jsou podstatně méně časté než je frekvence incidentů v ČR (natož jinde v Evropě a/nebo ve světě); stojí za implementaci intenzivní informování např. po vzoru pražského krizového řízení (bezpečnostní portál) a předávání zpráv z dalších zdrojů - antivirové firmy, mapy útoků (D)DoS[79], zprávy o kritických updatech operačních systémů (a to nejen Windows, ale i Linux, OpenWRT apod)

2. O2-2: Tvorba legislativy pro vynutitelnost opatření plynoucích z auditů informační a kybernetické bezpečnosti Zavést vynutitelnost opatření doporučených jako výsledek auditu NÚKIB dle §16 Vyhlášky

   Revidovat přiřazení úrovní rizik/důvěrnosti/hrozeb/zranitelnosti jednotlivým typům kritické infrastruktury

   - prioritizovaně energetika (elektřina, paliva), páteřní sítě internetu[80] a telekomunikace, nemocnice, pitná voda, dodávky potravin – s ohledem na strategické zásoby státu.
   - pravděpodobný důvod poněkud nízkých kategorií přiřazených inf. v energetických soustavách, nemocnicích, vodárnách apod souvisí s tím, že vyšší třída by znamenala nároky na investice, a to autoři zákona a vyhlášky nechtěli
   - z kom. sektoru, který má kybez povinnosti, kritika:

[77] https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/
[78] https://www.govcert.cz/cs/informacni-servis/hrozby/
[79] https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=2&time=18266&view=map
[80] https://www.cesnet.cz/sluzby/pripojeni/topologie/

a) původní návrh pravidel (rok 2018) byl napsaný právníky, nějaké porozumění elektrárnám, ale nulové IT;
b) ISP: hlášení "běží/neběží u nás kritické aplikace" může být mylné, protože ISP ví o připojených infrastrukturách jen to, co prozradí zákazník; případně může být pravdivé v okamžiku hlášení, ale vzápětí se bez vědomí IS změnit; z logiky věci snad dává smysl jen hlášení "nevíme o tom, že by u nás kritická aplikace běžela", ale není jasná systemická hodnota takového sdělení
c) kybez možno plnit buďto naplněním bodů Vyhlášky nebo získáním certifikace (ISO 27001, možná i jiná), ale protože tyto požadavky neškálují s velikostí firmy, Vyhláška znevýhodňuje ty nejmenší (garážovky nemají dost lidí na přiřazení rolí dle Vyhlášky ani prostředky k utracení za naplnění certifikace); fungující protipříklad: pravidla ICANN pro ISP-> dokud plní ISP povinnosti/pravidla, má být jedno, jak se mu to daří (kolik má lidí, jaké má interní systémy a procesy); NÚKIB od firem povinnosti (které jsou až na případ těch nejmenších nastavené celkem dobře) zatím nevymáhá, ale až začne, bude to pro část trhu likvidační

Navíc k občasným auditům kritických infrastruktur a informování o zranitelnostech publikovaných ve světě dát NÚKIB pravomoc (s prováděcí vyhláškou) provádět některé typy útoků na „živou" infrastrukturu. - pravděpodobně velmi legislativně náročné definovat "přiměřenou" míru testovacího útoku: takový test má smysl, jen pokud dostane systém do realistické zátěžové situace, pokud při této zátěži systém "padne" a je to zrovna systém typů "zásobení nemocnice elektřinou", mohou být (statisticky vzato BUDOU) následky na zdraví a životech - možná je možné takového testy uzákonit jako možné jen v režimu oznámených "kybez cvičení" podobných společným cvičení složek IZS při simulovaných teroristických útocích, havárie jaderné elektrárny, povodně apod. Tato "kybez cvičení" už probíhají, např pod hlavičkou NATO[81], ale netestují reálně naše infrastruktury a trénují jen zlomek odborných zaměstnanců v kybez VS a kritických infrastruktur - v současnosti dokonce když NÚKIB odhalí zranitelnosti, nemá možnost vynutit jejich nápravu: utajování výsledků testů, peněžité sankce nelze u státních institucí uplatnit (stát pokutuje sám sebe)

3. O2-3: Tvorba legislativy pro zvýšení efektivity testování kybernetické bezpečnosti Tlak na redukci byrokracie Provádět cost-benefit analýzy před zavedením každého vnitřního předpisu

4. O2-4: Tvorba legislativy pro koordinaci kyberbezpečnosti ve veřejné správě Vyřešit dvoukolejnost mezi NÚKIB a Vojenským zpravodajstvím.

8.2.3 P3: Vzdělání a expertní lidské zdroje pro veřejnou správu

Opatření:

1. O3-1: Vzdělání pracovníků veřejné správy v kybernetické bezpečnosti práce

   - podporovat (příspěvky na kurzovné) vzdělání úředníků i politiků v používání OSS programů Podporovat/vynucovat další vzdělání pracovníků v oblasti kyberbezpečnosti. školení od interních pracovníků i kompetentních externích vzdělávacích firem
   - zavést pravidelná školení v kyberbezpečnosti v analogii s BOZP, ale častěji, webináře s počítačovými testy, průběžné testování reakcí na phishing apod. Aplikovat, průběžně kontrolovat a vynucovat chování podle seznamů elementárních bezpečnostních návyků a praxe, např.:

[81] https://www.govcert.cz/cs/informacni-servis/akce-udalosti/2720-cesti-experti-jiz-podevate-resili-kyberneticke-utoky-v-ramci-fiktivni-civilni-a-vojenske-mise/

- hesla: uživatelé mají silná hesla, která si pamatují, nepíší na dotčená zařízení;, informační systémy/databáze identit nemají uložená hesla, ale hash-hodnoty "nasolených" hesel
- zálohování: uživatelé ať co nejvíce využívají sdílená úložiště, úřad tato úložiště zálohuje dle nejlepší praxe (vícestupňově podle "stáří" agendy)

2. O3-2: Podpora tvorby týmů ICT podpory sdílených samosprávami využívajícími stejného OSVS Budování vlastních expertních vývojových týmů (HW i SW) pro veřejnou správu, obranu země a jejích infrastruktur. Zařízení připojená k internetu jsou typicky zranitelná[82] díky defaultním nastavením, které buďto výrobce nezáplatuje nebo které nemění admini (nemám data, zda a jak je v české VS rozšířené "neměnění defaultních admin hesel" v routerech nebo zařízeních IoT.

   Při zavádění nového (rozsáhlého) SW nebo HW

   - postupovat v co nejširším souladu s jinými obcemi, aby řešení a) konvergovala, b) byla s co nejmenším úsilím přenositelná dalším úřadům, c) vedla k možnosti SDÍLENÉ ADMINISTRACE, tedy aby úřady měly podobná nebo stejná řešení a mohli je všechny administrovat stejní pracovníci
   - bez ohledu na cenovou hladinu (i VZMR, tedy mimo režim ZZVZ) usilovat o co nejotevřenější průběh výběrek s co nejvíce účastníky: uveřejnění na profilu zadavatele, aktivní oslovení potenciálních dodavatelů včetně těch, se kterými úřad ještě nikdy smlouvu neměl
   - vždy jmenovat pracovníky, kteří budou mít systém na starosti, aktualizovat jejich popisy práce; toto dejte do Pracovního řádu úřadu nebo jiného závazného interního dokumentu včetně přecházení tého zodpovědnosti na dalšího, když pracovník odejde
   - v návaznosti na školení o systému od dodavatele nechat některé z proškolených pracovníků, aby se sami stali kvalifikovanými školiteli; toto by mělo být součástí strategie vzdělávání zaměstnanců úřadu a je zodpovědností tajemníka/personálního oddělení

3. O3-3: Budování expertních týmů pro audit, návrh a vývoj bezpečného OSVS V rámci velkých měst (např.: nad 100 000 obyvatel) domluvit spoluzaložení a/nebo kofinancování vývojářského týmu, který bude vyvíjet SW pro samosprávy přímo pod samosprávou; nutno vymyslet optimální model, který dá zúčastněným samosprávám maximální "práva na výstupy" a zároveň umožní týmu, aby pro jednotlivé SW projekty mohl čerpat dotace MV, MMR apod.

4. O3-4: Metodické vedení samospráv pro migraci na OSVS NÚKIB, už se děje doporučení, jaké open technologie používat (z hlediska financí, ale aspoň něco)

5. O3-5: Vybudování e-learningu o kyberbezpečnosti pro veřejnost v Portálu občana ve spolupráci s místními školami (regionálními i vysokými) kurzy otevřené i veřejnosti zdůraznění "bezpečnosti chování na sítích" v rámci školních vzdělávacích programů, ideálně podporovat školy v zapojení nejen učitelů a žáků, ale i jejich rodinných příslušníků

8.2.4 P4: Veřejné zakázky na ICT

Opatření:

1. O4-1: Náležitosti smluv u veřejných zakázek - práva a povinnosti ze smlouvy U zakázek na dodávky informačních systémů a ICT infrastruktury dávat do podmínek ZADÁVACÍ DOKUMENTACE a

[82] https://www.youtube.com/watch?v=B8DjTcANBx0

PRAVIDEL SOUTĚŽE (v souladu s Akčním plánem podpory otevřeného software a boje proti vendor lock-in):

- jelikož HW se nevyrábí na míru, pouze sestavuje na míru, explicitně (bodově) zvýhodnit HW řešení s otevřenými komponentami (OHW, resp. splňujícími co nejvíce charakteristik "open hardware")
- dodavatel dodá veškerý zdrojový kód celého hotového systému a sestavovací informace (SW) a systémové diagramy zapojení
- zdrojový kód a diagramy zapojení HW s stanou majetkem objednatele (obce) pro jakékoli použití, tedy NEJEN pro vlastní údržbu a rozvoj, ale i pro další šíření, úpravy a hospodářskou činnost (tedy podobně licenci typu MIT, resp. FreeBSD), aby mohla obec SW nebo i HW neomezeně sdílet (ať už přímo nebo skrze sdružení jako Otevřená města, z.s.)
- data uložená v systému (databáze, fyzické disky,...) jsou permanentně majetkem úřadu
- dodavatel dodá kromě ostrého řešení i "pískoviště" za účelem vzdělávání vlastních i cizích pracovníků, ke kterému bude také poskytovat podporu, ale ke kterému bude mít plná práva (administrátorská i licenčně-dispoziční) radnice
- dodavatel, který má poskytnout i služby "údržba a rozvoj", dodá s každou změnou systému zdrojové kódy aktualizací a aktualizované diagramy zapojení
- i v případě, že údržbu a rozvoj dělá dodavatel za úplatu, ať dostane alespoň jeden pracovník určený radnicí plná práva pro administraci ostrého systému a může je využít
- součástí dodávky má být i školení a příručka pro uživatele a školení a podklady pro administrátory
- dodavatel (smluvní protistrana obce) nesmí využívat než jednu další úroveň subdodavatelů; subdodavatelé mají tendenci se řetězit, každý odebírá s prostředků svoji marži (finanční neefektivita) a často mají po dvojicích mezi sebou uzavřené NDA smlouvy, takže konečný vývojář/výrobce řešení nemůže se zákazníkem (obcí) komunikovat napřímo, nemůže ani po dodání systému "vyřadit" prostředníka (procesní i finanční neefektivita)
- dodavatel se musí po určitou dobu (např. 2 roky) starat o odstranění zranitelností a uposlechnout případných pokynů NÚKIB v rámci ceny dodávky (tj. provádět "záruční opravy").
- zákazník (obec) zadrží vyplacení části ceny zakázky až po uplynutí "záruční doby" a pouze pokud dodavatel splnil své záruční povinnosti.

2. O4-2: Náležitosti zadávací dokumentace u veřejných zakázek
3. O4-3: Tvorba legislativy o povinném sdílení kódu (následování příkladu USA)
4. O4-4: Tvorba legislativy pro zodpovědnost za kyberbezpečnost Zavést v §7 Vyhlášky pro projekty vývoje nového SW (jak v rámci veřejných zakázek, tak při vlastním vývoji) roli „statika kybernetické bezpečnosti" jakožto určitý ekvivalent role "stavebního dozoru" neboli "technického dozoru investora" na stavbách. Roli je nutné v předpisech definovat jako takovou, že pracovník nebo kontrahovaný expert bude mít hmotnou a trestněprávní odpovědnost za bezpečnostní kvalitu díla. Procesy pak je nutné nastavit tak, aby minimalizovaly motivaci k podřadnému výkonu či korupci.

9 Relevantní zákony, vyhlášky a nařízení vlády

Číslo předpisu	Název předpisu	Účinnost od
12/2020 Sb.	Zákon o právu na digitální služby	01.02.2020
110/2019 Sb.	Zákon o zpracování osobních údajů	24.04.2019
99/2019 Sb.	Zákon o přístupnosti internetových stránek a mobilních aplikací a o změně zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů	09.04.2019
250/2017 Sb.	Zákon o elektronické identifikaci	01.07.2018
194/2017 Sb.	Zákon o opatřeních ke snížení nákladů na zavádění vysokorychlostních sítí elektronických komunikací a o změně některých souvisejících zákonů	25.07.2017
297/2016 Sb.	Zákon o službách vytvářejících důvěru pro elektronické transakce	19.09.2016
234/2014 Sb.	Zákon o státní službě	01.01.2015
181/2014 Sb.	Zákon o kybernetické bezpečnosti	01.01.2015
300/2008 Sb.	Zákon o elektronických úkonech a autorizované konverzi dokumentů	01.07.2009
261/2007 Sb.	Zákon o stabilizaci veřejných rozpočtů	01.01.2008
110/2007 Sb.	Zákon o některých opatřeních v soustavě ústředních orgánů státní správy, souvisejících se zrušením Ministerstva informatiky	01.06.2007
310/2006 Sb.	Zákon o nakládání s bezpečnostním materiálem	01.07.2006
262/2006 Sb.	Zákoník práce	01.01.2007
412/2005 Sb.	Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti	01.01.2006
289/2005 Sb.	Zákon o Vojenském zpravodajství	01.08.2005
127/2005 Sb.	Zákon o elektronických komunikacích	01.05.2005
480/2004 Sb.	Zákon o některých službách informační společnosti	07.09.2004
312/2002 Sb.	Zákon o úřednících uzemních samosprávných celků	01.01.2003
240/2000 Sb.	Zákon o krizovém řízení	01.01.2001
131/2000 Sb.	Zákon o hlavním městě Praze	12.11.2000
129/2000 Sb.	Zákon o krajích	12.11.2000
128/2000 Sb.	Zákon o obcích	12.11.2000
148/1998 Sb.	Zákon o ochraně utajovaných skutečností	01.11.1998
216/1995 Sb.	Zákon o Vojenském obranném zpravodajství (úplné znění, jak vyplývá z pozdějších změn a doplnění)	05.10.1995
153/1994 Sb.	Zákon o zpravodajských službách České republiky	30.07.1994
154/1994 Sb.	Zákon o bezpečnostní informační službě	30.07.1994

Číslo předpisu	Název předpisu	Účinnost od
226/2019 Sb.	Vyhláška o zdravotní způsobilosti ke službě v bezpečnostních sborech	01.10.2019
10/2019 Sb.	Vyhláška o způsobu oznamování a zasílání informací a přenosu dat provozovatelem hazardních her, rozsahu přenášených dat a jiných technických parametrech přenosu dat	01.06.2019
82/2018 Sb.	Vyhláška o kybernetické bezpečnosti	28.05.2018
437/2017 Sb.	Vyhláška o kritériích pro určení provozovatele základní služby	01.02.2018
386/2015 Sb.	Vyhláška o náležitostech kryptografických klíčů a autentizačního certifikátu	01.01.2016
316/2014 Sb.	Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)	01.01.2015
317/2014 Sb.	Vyhláška o významných informačních systémech a jejich určujících kritériích	01.01.2015
357/2012 Sb.	Vyhláška o uchovávání, předávání a likvidaci provozních a lokalizačních údajů	01.11.2012
241/2012 Sb.	Vyhláška o stanovení náležitostí technicko-organizačních pravidel k zabezpečení bezpečnosti a integrity veřejné komunikační sítě a interoperability veřejně dostupných služeb elektronických komunikací za krizových stavů	01.08.2012
242/2012 Sb.	Vyhláška o stanovení rozsahu a formy předávané informace o narušení bezpečnosti a ztrátě integrity sítě	01.08.2012
212/2012 Sb.	Vyhláška o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu, a postupech pro ověřování platnosti zaručeného elektronického podpisu, elektronické značky, kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a kvalifikovaného časového razítka (vyhláška o ověřování platnosti zaručeného elektronického podpisu)	01.07.2012
228/2012 Sb.	Vyhláška o stanovení kritérií pro posuzování, zda má více subjektů společnou významnou tržní sílu na relevantním trhu elektronických komunikací	01.07.2012
363/2011 Sb.	Vyhláška o personální bezpečnosti a o bezpečnostní způsobilosti	01.01.2012
405/2011 Sb.	Vyhláška o průmyslové bezpečnosti	01.01.2012
432/2011 Sb.	Vyhláška o zajištění kryptografické ochrany utajovaných informací	01.01.2012
88/2011 Sb.	Vyhláška o technických podmínkách a postupu při pořizování biometrických údajů a podpisu cizince pro účely vydání průkazu o povolení k pobytu	01.05.2011
356/2009 Sb.	Vyhláška o informacích zaznamenávaných v Říčních informačních službách	16.10.2009
193/2009 Sb.	Vyhláška o stanovení podrobností provádění autorizované konverze dokumentů	01.07.2009
194/2009 Sb.	Vyhláška o stanovení podrobností užívání a provozování informačního systému datových schránek	01.07.2009

Číslo předpisu	Název předpisu	Účinnost od
238/2007 Sb.	Vyhláška o předávání údajů pro účely tísňových volání	01.10.2007
117/2007 Sb.	Vyhláška o číslovacích plánech sítí a služeb elektronických komunikací	01.07.2007
52/2007 Sb.	Vyhláška o postupech atestačních středisek při posuzování způsobilosti k realizaci vazeb informačních systémů veřejné správy prostřednictvím referenčního rozhraní	22.03.2007
53/2007 Sb.	Vyhláška o referenčním rozhraní	22.03.2007
3/2007 Sb.	Vyhláška o celostátním dopravním informačním systému	01.03.2007
378/2006 Sb.	Vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb	17.08.2006
327/2006 Sb.	Vyhláška, kterou se stanoví charakteristiky přiměřených požadavků na připojení v pevném místě k veřejné telefonní síti a na přístup v pevném místě k veřejně dostupné telefonní službě a podmínky přístupu k internetu v rámci univerzální služby	01.07.2006
523/2005 Sb.	Vyhláška o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor	01.01.2006
525/2005 Sb.	Vyhláška o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací	01.01.2006
527/2005 Sb.	Vyhláška o personální bezpečnosti	01.01.2006
528/2005 Sb.	Vyhláška o fyzické bezpečnosti a certifikaci technických prostředků	01.01.2006
529/2005 Sb.	Vyhláška o administrativní bezpečnosti a o registrech utajovaných informací	01.01.2006
430/2005 Sb.	Vyhláška, kterou se stanoví kritéria pro posuzování, zda má více subjektů společnou významnou tržní sílu na relevantním trhu elektronických komunikací	26.10.2005
496/2004 Sb.	Vyhláška o elektronických podatelnách	01.01.2005
552/2004 Sb.	Vyhláška o předávání osobních a dalších údajů do Národního zdravotnického informačního systému pro potřeby vedení národních zdravotních registrů	05.11.2004
470/2003 Sb.	Vyhláška, kterou se stanoví rozsah a způsob poskytování informací zdravotnickými zařízeními do Národního zdravotnického informačního systému	31.12.2003
329/2003 Sb.	Vyhláška o informačním systému Státní veterinární správy	30.09.2003
137/2003 Sb.	Vyhláška o podrobnostech stanovení a označení stupně utajení a o zajištění administrativní bezpečnosti	16.05.2003
362/2002 Sb.	Vyhláška Ministerstva vnitra o postupech při provádění spisové rozluky v souvislosti s ukončením činnosti okresních úřadů a o náležitostech spisové evidence při provádění spisové rozluky	15.08.2002
88/2002 Sb.	Vyhláška k provedení knihovního zákona	13.03.2002
366/2001 Sb.	Vyhláška Úřadu pro ochranu osobních údajů o upřesnění podmínek stanovených v §6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu	10.10.2001
483/2000 Sb.	Vyhláška Ministerstva spravedlnosti, kterou se stanoví případy, v nichž nelze povolit nahlédnutí do spisu, neboť jeho obsah musí zůstat utajen	01.01.2001

Číslo předpisu	Název předpisu	Účinnost od
57/2015 Sb.	Nařízení vlády o stanovení rozsahu údajů zapisovaných do informačního systému o služebním platu a způsobu jejich zapisování	01.07.2015
304/2014 Sb.	Nařízení vlády o platových poměrech státních zaměstnanců	01.01.2015
432/2010 Sb.	Nařízení vlády o kritériích pro určení prvku kritické infrastruktury	01.01.2011
295/2010 Sb.	Nařízení vlády o stanovení požadavků a postupů pro zajištění propojitelnosti elektronických systémů plateb a odbavení cestujících	01.11.2010
397/2009 Sb.	Nařízení vlády o informačním systému výzkumu, experimentálního vývoje a inovací	01.01.2010
522/2005 Sb.	Nařízení vlády, kterým se stanoví seznam utajovaných informací	01.01.2006

10 Kuchařky

10.1 Obce, svazky obcí

10.1.1 SWOT shrnutí

- **Strengths**
  - zakázky na HW, SW a související služby jsou relativně malého objemu > prakticky lze zkoušet různá řešení (každé s rozumnou šancí na funkčnost); má-li toto být vytěžované (testbed), je nutná komunikační platforma napříč radnicemi, resp. jejich IT odbory/radními, a samozřejmě zástupci Pirátů v nich
- **Weaknesses**
  - většina obcí má rozpočty malé, IT je popelkou mezi gescemi (oblastmi pro investice a rozvoj HR) v porovnání s výdaji na "viditelné" gesce výstavby a opravy komunikací, údržby veřejného prostoru, hromadnou dopravou... a z jiných důvodů i v porovnání se školstvím a sociálními službami
  - obce nemají vliv na legislativu, musí fungovat a realizovat změny v existujícím zákonném a exekutivním rámci - tedy na prvním místě je soulad se zákony a vyhláškami, na druhém je splnění účelu, pak teprve optimalizace plnění účelu nápravou procesů, zadávacích dokumentací...
- **Opportunities**
  - na poli IT je na úrovni obcí málo lobbistického zájmu přímo mezi politiky
  - málo ideových rozporů mezi politiky, většině stran je IT jedno > lze spojit síly k prosazování
- **Threats**
  - jako na všech úrovních a skoro ve všem je ÚŘAD automaticky v opozici vůči změnám, jeho spolupráce odvisí od osoby TAJEMNÍKA
  - funkční IT není samo o sobě vidět, vidět je (ne)funkčnost úřadu - když úředníci na IT se svádí případná nefunkčnost úřadu, ač jde o neschopnost (nízkou vzdělanost a ochotu k dovzdělání) zaměstnanců úřadu, je velmi obtížné obhajovat i správné kroky; je tedy těžké se změnou systémů a postupů prosadit i dlouhodobou změnu přístupu (úředníků a budoucích koalic)

10.1.2 Co konkrétního se snažit udělat

1. U zakázek na dodávky informačních systémů a ICT infrastruktury dávat do podmínek ZADÁVACÍ DOKUMENTACE a PRAVIDEL SOUTĚŽE (v souladu s Akčním plánem podpory otevřeného software a boje proti vendor lock-in):
   - jelikož HW se nevyrábí na míru, pouze sestavuje na míru, explicitně (bodově) zvýhodnit HW řešení s otevřenými komponentami (OHW, splňujícími co nejvíce charakteristik "open hardware")
   - dodavatel dodá veškerý zdrojový kód celého hotového systému a sestavovací informace (SW) a systémové diagramy zapojení
   - zdrojový kód a diagramy zapojení HW s stanou majetkem objednatele (obce) pro jakékoli použití, tedy NEJEN pro vlastní údržbu a rozvoj, ale i pro další šíření, úpravy a hospodářskou činnost (tedy podobně licenci typu MIT, resp. FreeBSD)
   - data uložená v systému (databáze, fyzické disky,...) jsou permanentně majetkem úřadu
   - dodavatel dodá kromě ostrého řešení i "pískoviště" za účelem vzdělávání vlastních i cizích pracovníků, ke kterému bude také poskytovat podporu, ale ke kterému bude mít plná práva (administrátorská i licenčně-dispoziční) radnice
   - dodavatel, který má poskytnout i služby "údržba a rozvoj", dodá s každou změnou systému zdrojové kódy aktualizací a aktualizované diagramy zapojení
   - i v případě, že údržbu a rozvoj dělá dodavatel za úplatu, ať dostane alespoň jeden pracovník určený radnicí plná práva pro administraci ostrého systému a může je využít
   - součástí dodávky má být i školení a příručka pro uživatele a školení a podklady pro administrátory
2. Při zavádění nového (rozsáhlého) SW nebo HW
   - postupovat v co nejširším souladu s jinými obcemi, aby řešení a) konvergovala, b) byla s co nejmenším úsilím přenositelná dalším úřadům, c) vedla k možnosti SDÍLENÉ ADMINISTRACE, tedy aby úřady měly podobná nebo stejná řešení a mohli je všechny administrovat stejní pracovníci
   - bez ohledu na cenovou hladinu (i VZMR, tedy mimo režim ZZVZ) usilovat o co nejotevřenější průběh výběrek s co nejvíce účastníky: uveřejnění na profilu zadavatele, aktivní oslovení potenciálních dodavatelů včetně těch, se kterými úřad ještě nikdy smlouvu neměl
   - vždy jmenovat pracovníky, kteří budou mít systém na starosti, aktualizovat jejich popisy práce; toto dejte do Pracovního řádu úřadu nebo jiného závazného interního dokumentu včetně přecházení tého zodpovědnosti na dalšího, když pracovník odejde
   - v návaznosti na školení o systému od dodavatele nechat některé z proškolených pracovníků, aby se sami stali kvalifikovanými školiteli; toto by mělo být součástí strategie vzdělávání zaměstnanců úřadu a je zodpovědností tajemníka/personálního oddělení
3. Pro zavádění SW do jednotlivých pracovních stanic (desktopy, ntb úředníků i zastupitelů)
   - upřednostňovat open source software (FLOSS) pod svobodnými licencemi (GNU GPL, MIT,...); seznam alternativ k obvyklému komerčnímu (například dle https://downloadpedia.org/alternative/, ale určitě existují lepší zdroje/seznamy na webu; teoreticky můžeme v návaznosti na AP a tuto kuchařku udržovat vlastní)
   - podporovat (příspěvky na kurzovné) vzdělání úředníků i politiků v používání těchto programů

4. Finanční podpora FLOSS a OHW

   - na úrovni samosprávy prosadit formou interní směrnice finanční dotace výrobcům používaného FLOSS úměrně (podle možností, ale je třeba domluvit nějaký algoritmus) cenám komerční konkurence na trhu a počtu reálných uživatelů na úřadě; zde je nutné prozkoumat terén a napříč politickým spektrem prosazovat hledisko, že toto NENÍ platbou za software zdarma, je to PODPORA prospěšné činnosti analogická dotacím do sportu nebo kultury nebo do veřejného prostoru skrze participační rozpočty
   - v rámci velkých měst (nad 100 000 obyvatel?) domluvit spoluzaložení a/nebo kofinancování vývojářského týmu, který bude vyvíjet SW pro samosprávy přímo pod samosprávou; nutno vymyslet optimální model, který dá zúčastněným samosprávám maximální "práva na výstupy" a zároveň umožní týmu, aby pro jednotlivé SW projekty mohl čerpat dotace MV, MMR apod.
   - analogicky k postupům výše (dotace jednotlivých radnic a/nebo společné vývojové týmy) prosadit podporu vývoje otevřeného hardware; OHW nebude nikdy specifické pro veřejnou správu, proto dává smysl spíše model společného financování výzvy na takový vývoj, kde by příjemcem dotace byly VŠ, výzkumné ústavy apod včetně jiných příspěvkových organizací nebo jimi stopro ovládaných firem (CZ.NIC, OICT, ...)

Figure 1: The Universe

11 Závěr

"I always thought something was fundamentally wrong with the universe" [83]

[83] D. Adams. *The Hitchhiker's Guide to the Galaxy.* San Val, 1995.