Egovernment
elektronizace veřejné správy

ZA ČESKO DIGITÁLNÍ

HOME OFFICE KVALITNĚ A BEZPEČNĚ

KYBEROBRANA A VOJENSKÉ ZPRAVODAJSTVÍ

OPEN DATA VE VEŘEJNÉ SPRÁVĚ

www.egovernment.cz

č. 1/2020

Úvodní slovo

Vážení a milí čtenáři magazínu Egovernment,

prožíváme dnes velice zvláštní a náročnou dobu. Všichni dohromady a každý zvlášť. Způsob života, jak se nám změnil, je pro všechny něčím naprosto novým, často komplikovanějším a rozhodně s určitou mírou nejistoty směrem do budoucna. Jisté máme jen to, že konec pandemie, respektive konec těch opatření, která nás nejvíce omezují, nebude automaticky znamenat návrat k normálnímu, původnímu stavu. Budeme chudší, my osobně i náš stát. Tedy finančně. Zážitky, které nyní sbíráme, naopak řadu z nás obohatí. Například o poznání, že je smysluplnější a přínosnější věnovat se rodině místo vyplňování tabulek v kanceláři. Mnozí z nás bezpochyby v době domácího poustevničení dojdou k poznání, že chtějí dělat něco jiného a jinak. Všichni totiž děláme nyní věci jinak. A spousta z nás zjišťuje, že to jde. Že dělat věci na dálku může být efektivnější, pohodlnější i zajímavější. Elektronicky dnes nakupujeme, studujeme, pracujeme, komunikujeme se svými blízkými, které nemůžeme navštívit osobně a elektronicky si i pomáháme. Ať se jedná o sbírky finanční, nabídky na ušití roušek, venčení, výrobu důležitých pomůcek ... To vše se právě v těchto vypjatých dnech řeší elektronicky, na dálku, rychle a efektivně.

Je to situace velice neblahá, kterou právě prožíváme, ale je to situace, která nám odhaluje možnosti, jaké našim životům elektronizace nabízí. A ukazuje, jak jsme schopni a připraveni těchto možností využít. My osobně i náš stát. A tady nutno podotknout, že my vyhráváme. Ano stát se snaží nabídnout elektronický přístup, kde jen to jde – datovými schránkami, e-mailem, portálovými řešeními. Ale stejně musí před vstupy do svých budov instalovat papírové krabice, kam občané vhazují papírové formuláře a žádosti. Prostě proto, že jen velice malá část populace má své datové schránky, nebo občanský průkaz aktivovaný pro elektronickou komunikaci. V případě DS jsme v loňském roce překročili milion kusů, ale jen 165 000 patřilo fyzickým osobám, a eOP si pro elektronické využití aktivovalo 250 000 osob. Jen ty mohou dnes, naprosto bez problémů komunikovat s veřejnou správou elektronicky pro osobní záležitosti. Pokud by náhodou již dnes platila novela bankovního zákona, která přináší tzv. BankID, mohlo by takových osob být 5 milionů. Pět milionů občanů tohoto státu by mohlo okamžitě využívat podané elektronické ruky státu, protože se jedná o osoby, které naprosto běžně komunikují elektronicky se svojí bankou a to prostřednictvím tzv. elektronického bankovnictví. Těmi samými hesly, která používají pro vstup do své elektronické banky, by mohly přistoupit i ke službám státu. Elektronicky, na dálku a pohodlně.

Elektronicky se v této době aktivujeme. Pro dobrou věc a vzájemnou pomoc. Jsou zde různé platformy a iniciativy, které sdružují výrobce, poskytovatele technologií a hlavně nápady, nebo finanční sbírky zajišťující nákup všeho potřebného od roušek, respirátorů, jídla až po plicní ventilátory. V přímém přenosu můžeme vidět, že soukromý sektor je vždy o krok rychlejší, efektivnější, inovativnější. Je to logické, stát je stát, z principu je „zkostnatělejší“, protože musí dbát na určitá pravidla a to je často kapacitně i časově náročnější. Soukromý sektor je dynamický, inovativní, ale někdy jde o „neřízenou“ střelu. Je ale zřejmé, že spojení obojího, komerčního a státního a jeho vzájemná spolupráce, ovlivňování a kontrola, může být prospěšná pro nás všechny. I o tom v tomto čísle Magazínu Egovernment najdete články.

Moc bych si přál, nám všem bych přál, aby pro nás byla současná situace poučením a po jejím odeznění jsme z těchto zkušeností vytěžili maximum a to nejen v rámci elektronizace.

Přeji Vám vše dobré,
Michal Jirkovský, šéfredaktor

Obsah

V rámci České a Slovenské republiky vydává:
info◆com s.r.o, Na Zatlance 10, 150 00 Praha 5
www.infocom.cz
IČO: 26426331
zapsána u Městského soudu v Praze
pod č. C – 81357
tel.: 241 412 518
e-mail: egovernment@egovernment.cz
http: www.egovernment.cz
twitter: @EgovernmentMag
facebook: @EgovernmentMagazin

Šéfredaktor: Ing. Michal Jirkovský
Korektorka: PhDr. Helena Veverková
Asistentka: Martina Maksymovová

Grafika: PROPAGANDA, Malá Štupartská 7, Praha 1
Tiskárna: A. R. GARAMOND s.r.o., Belnická 758, 252 42 Jesenice
Registrační číslo: MK ČR E 11364
ISSN 1801-9420

Registrace:

Magazín Egovernment je distribuován, na základě registrace, pracovníkům veřejné správy v České republice a na Slovensku **ZDARMA**. Ostatní čtenáři, kteří nejsou pracovníky veřejné správy zaplatí cenu **100 Kč (4 EUR)** bez DPH**/výtisk, tj. 400 Kč (16 EUR)** bez DPH **ročně**.
S registrací získáte, kromě pravidelného zasílání magazínu, i informace o dalších projektech, které realizuje společnost **info◆com** s.r.o.

ZA ČESKO DIGITÁLNÍ

Náš první a zatím, díky okolnostem i zatím poslední letošní seminář jsme pořádali v únoru v Jihlavě na téma ZA ČESKO DIGITÁLNÍ. Seminář svým vystoupením zahájil po odborné stránce vládní zmocněnec pro IT a digitalizaci Vladimír Dzurilla. V souvislosti s tématem semináře se věnoval především strategii Digitální Česko. I když to, podle jeho slov, měla být strategie trvalá, přece jen je jasné, že se budou muset v rámci jednotlivých záměrů učinit určité korekce, což je ovšem vzhledem k dynamičnosti této oblasti pochopitelné. Znovu přiblížil, že strategie pokrývá tři základní oblasti – Česko v digitální Evropě, Informační koncepce ČR a Digitální ekonomika a gramotnost, které následně podrobněji přiblížil.

ČESKO V DIGITÁLNÍ EVROPĚ

Podle slov Vladimíra Dzurilly se jedná o vše, co je zásadní a co se v oblasti elektronizace v rámci Evropy odehrává na poli legislativy. Jde tedy o veškeré vyhlášky a nařízení. Podstatné je, že tento pilíř zastřešuje Úřad vlády, který podle jeho slov dbá na to, aby nejen touto cestou proudily informace a nařízení směrem k nám, ale abychom případně mohli ovlivňovat jejich znění tak, aby výsledná podoba vyhovovala i našim potřebám.

INFORMAČNÍ KONCEPCE

To je nejdůležitější část celé strategie. Zahrnuje pět pilířů, kterými jsou on-line služby, legislativa, celkové prostředí podporující digitální technologie, centrální řízení IT a vzdělávání úředníků.

DIGITÁLNÍ EKONOMIKA A SPOLEČNOST je dokument, který zahrnuje vše, co se v rámci elektronizace odehrává mimo e-government. Zahrnuje tedy například nové technologie (AI), vzdělávání, ale rovněž i Blockchainové realizace. Je to tedy oblast, která je v gesci MPO.

DIGITÁLNÍ ČESKO – JAK JSME NA TOM?

Pro rozvoj digitálního Česka je nyní, podle slov Vladimíra Dzurilly, naprosto zásadní otázka rozhraní a pro něj je podstatná problematika identity. Podařila se úžasná záležitost v podobě schválení příslušené legislativy podporující využití bankovní identity v rámci služeb e-governmentu. To znamená, že bude možné přistoupit k Portálu veřejné správy i všem ostatním portálům (státní i veřejné správy) přes naši identitu, kterou se prokazujeme při vstupu do elektronického bankovnictví. Je to zásadní moment, neboť doposud e-government postrádal dostatečné množství „klientů“, kteří by mohli plně využívat elektronických služeb. V podobě eOP či DS se tak jednalo cca o 5000 osob. Nyní rázem dojde k navýšení tohoto počtu na 5,5 milionu uživatelů. Jedná se tedy o skutečně zásadní krok, který nebyl ještě v řadě zemí realizován. V ČR by se tak mělo stát počátkem roku 2021.Přímou návaznost na BankID má samozřejmě kontaktní místo a jeho další rozvoj, stejně jako připojení přes internet. Je nutné zajistit, aby elektronické služby bylo možné kdykoliv a kdekoliv využít. V tomto směru se jedná i o rozšíření nabídky služeb, která bude prostřednictvím Portálu veřejné správy (PVS) k dispozici. Podle Vladimíra Dzurilly je i podstatné zavést funkcionalitu elektronické platby tak, aby se jednalo skutečně o plnohodnotné elektronické služby. Je například škoda, že se v případě problematického „e-shopu“ dálničních známek od začátku nepočítalo o začlení do PVS. Jedná se totiž přesně o ten typ služby, který by zde měl být k dispozici, stejně jako elektronické faktury a další. Je tedy nutné, aby byl PVS propojen například s Businessinfo

a řadou dalších portálů tak, aby veškeré tyto služby byly dostupné z jednoho bodu.

Zcela zásadní legislativou roku 2019 je tedy bankovní identita, zákon o právu na digitální službu a digitalizace stavebního řízení. V této souvislosti poděkoval především ICT Unii, která je nejen důležitým iniciátorem, ale i partnerem při tvorbě jednotlivých záměrů. V letošním roce by práce na zákonech samozřejmě měly pokračovat, a to především tam, kde je přímá návaznost na zákon o právu na digitální službu. Jedná se celkově o 150 zákonů, kde je přímá souvislost a kde je tedy nutné provést určité úpravy a změny. Kromě těchto přímých návazností bude z hlediska legislativy prioritou digitalizace zdravotnictví.

CENTRÁLNÍ ŘÍZENÍ IT

V této oblasti dochází k rozšíření kompetencí OHA MV ČR a zároveň vzniká v NAKIT kompetenční centrum. To by mělo být k dispozici úřadům a institucím a pomáhat při správném sestavení veřejné zakázky z pohledu IT agendy. Bude tedy nápomocno při orientaci v celém cyklu, který pokrývají nové dokumenty, jakými jsou Informační koncepce, Národní architektonický rámec, Národní architektonický plán tak, aby byly tyto záměry aplikované a hladce přenesené do jednotlivých resortů.

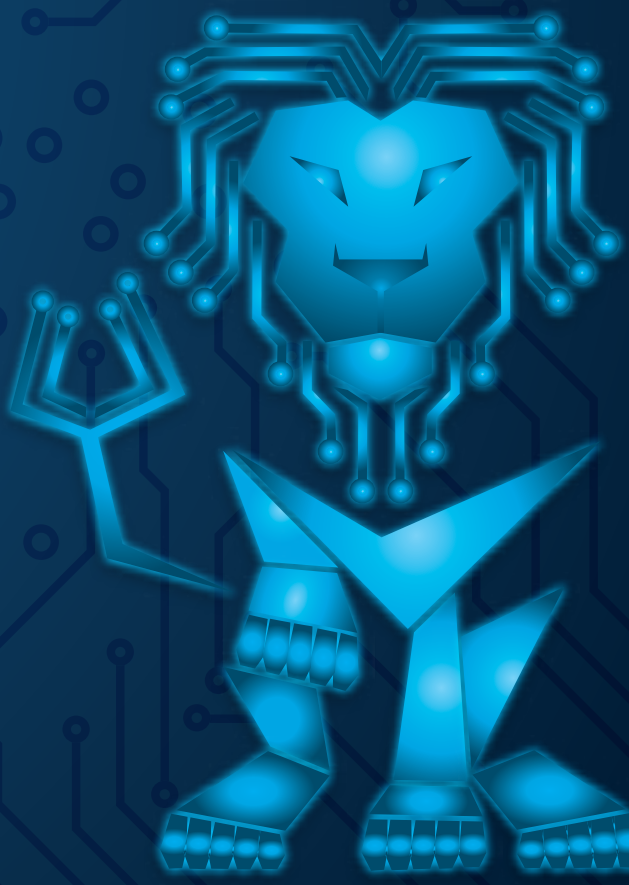
Zajímavou oblastí jsou podle Vladimíra Dzurilly rovněž **DATOVÁ CENTRA**. Zde se dá dle jeho mínění ušetřit značné množství prostředků, a to především konsolidací infrastruktury. O samotném eGovernment Cloudu bude hovořit Miroslav Tůma (str. 10), ale za zdůraznění určitě stojí skutečnost, že cloudová cesta je centralizované řešení, které zvyšuje efektivitu, a to jak v případě infrastruktury, tak výpočetního výkonu.

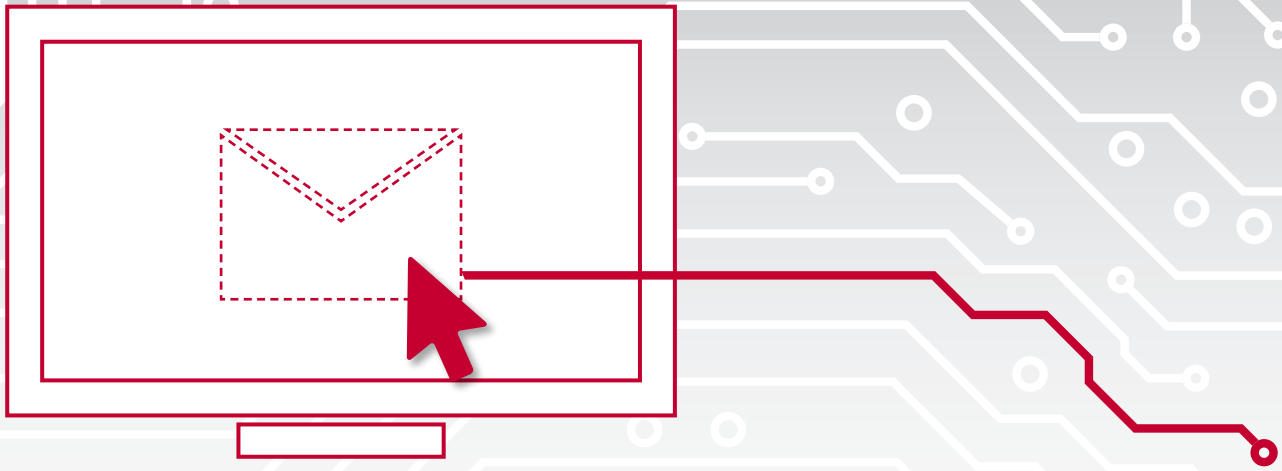
ZMENŠOVÁNÍ ROZSAHU ZAKÁZEK

Určitým způsobem bude nutné změnit rovněž přístup k zadávání zakázek a vnímání jejich rozměru. V minulosti jsme je často brali jako velké celky. Bude nutné se naučit, že není potřeba vždy obměňovat celý systém, že je naopak vhodné umět si jej rozparcelovat na jednotlivé integrační vrstvy, služby, odlehčené portály atp. Je to přístup, který standardně používá komerční sektor a musíme jej naučit i veřejnou správu. Smyslem je, aby zadávání zakázek bylo efektivnější a abychom byli schopni využívat sdílených komponent. I proto v Národním architektonickém plánu vznikl popis sdílených komponent. Konkrétně například v momentě, kdy existuje Národní identita, by se nemělo stát, že s vytvořením nového portálu někde vznikne jiná nová identita. Totéž platí pro platební bránu atp. Směřujeme tedy k daleko většímu využívání sdílených služeb.

ZÁVĚR – VYŠŠÍ EFEKTIVITA

Důležitá změna musí podle Vladimíra Dzurilly nastat i v případě provozních a implementačních procesů tak, aby je veřejná správa realizovala skutečně moderně. Není například nadále přípustné, aby se dva roky nějaký nápad připravoval, následně rok a půl soutěžil a další dva roky realizoval. Znamená to pak, že výsledné dílo je od prvotní myšlenky k dispozici po pěti letech a právě tento cyklus je nutné zrychlit. Měl by tomu napomoci Katalog služeb stejně jako eGovernment Cloud a řada dalších kroků, které směřují k tomu, že bude cyklus pružnější. Je samozřejmě zásadní rozhodnout, jak bude vypadat spolupráce s komerčním sektorem, jak bude propojena samospráva, jaké služby vzniknou a které centrální služby je možné delegovat dál. To jsou, podle Vladimíra Dzurilly, úkoly letošního roku.





KATALOG SLUŽEB A DIGIZÁKON

Ředitel odboru eGovernment MV ČR Roman Vrba navázal svým vystoupením na Vladimíra Dzurillu. Upozornil především, že Katalog služeb je přímým důsledkem zákona o právu na digitální službu, není pouhým triviálním překlopením excelovské tabulky a rozhodně se nejedná o něco zcela nového. Jak zdůraznil, byl takový katalog v podstatě již delší dobu budován, a to pod názvem Úkony na žádost. V současné době jsou, podle jeho slov, práce na katalogu velice intenzivní i proto, že by měl být do poloviny letošního roku kompletně hotový, aby se mohl začít naplňovat obsahově.

Zároveň běží spolupráce s ohlašovateli agend na jejich přípravě, především vysvětlování toho, co přesně je míněno terminologií katalogu, co znamená služba, úkon atd. Jak zaznělo již ve vystoupení Vladimíra Dzurilly, vzniká zároveň kompetenční centrum, které by mělo být natolik zdatné, aby jednotlivým resortům pomáhalo s vyplňováním dat do katalogu. Že to nebude jednoduchá záležitost, dokládá i záměr vybudovat v rámci tohoto centra tým, který se bude věnovat výhradně Katalogu služeb. Ve svém vystoupení se Roman Vrba věnoval podrobněji jednotlivým detailů, které přináší zákon.

Důležitou záležitostí vyplývající ze zákona o právu na digitální služby je **sama povinnost poskytovat digitální služby**, tedy moment, kdy gestor dané agendy by měl poskytovat co nejvíce služeb digitálně a tyto budou evidovány v Katalogu služeb.

Zákonem jsou rovněž definovány formy poskytování digitálních služeb, jedná se o:

Datové schránky – vzhledem k historii datových schránek je touto cestou nabízeno/realizováno cca 65% agend, které tímto naplňují podstatu digitální služby.

Czech POINT je verze, že digitální služba bude k dispozici na kontaktních místech. Tady je nutné zdůraznit, že není možné, aby prostřednictvím těchto asistenčních míst byly realizovány veškeré služby. Bude se jednat spíše o menší procento jednodušších agend. V případě složitějších podání, nebo podání směřujících na banky, operátory atp. nelze předpokládat, že bude k dispozici obsluha natolik fundovaná, aby pomohla s jejich realizací (množství agend a formulářů to vylučuje). To znamená, že prostřednictvím Czech POINTu bude vhodné provádět spíše typově jednodušší úkony – například podání žádosti o vystavení či výměnu příslušného dokladu atp.

e-Mail s kvalifikovaným elektronickým podpisem je rovněž varianta, která funguje již dnes. Problémem je však nízká penetrace kvalifikovaných elektronických podpisů. Zatím není pravděpodobné, že by se tato situace nějak radikálně měnila, a tedy využití této varianty nebude patrně nijak masivní záležitostí.

Portálová řešení – jedná se jak o Portál veřejné správy (PVS), tak ostatní resortní portály, které jsou či budou

specializované na konkrétní podání v rámci jednotlivých resortů. Není to tak, že by existoval jeden portál, který by v sobě obsahoval všechny formuláře a aplikace. PVS je ve své podstatě rozcestník na řadu dalších a tak by to mělo do budoucna i zůstat. Přímo v něm budou umístěny jen ty nejčastěji využívané, případně ty nejjednodušší aplikace. Poslední možnost je **individuální**, kterou si definuje přímo sám gestor.

FORMULÁŘE

Roman Vrba upozornil, že formuláře mají být v digitální podobě už dávno. Například u formulářů v RPP to platí již deset let. Nedá se ovšem říci, že by to někdo v širším měřítku dodržoval. MV ČR nyní, v rámci projektu úplného elektronického podání, hledá řešení. V současné době je již definován standard a MV ČR připravuje jeho představení.

OSVĚDČENÍ DIGITÁLNÍHO ÚKONU

Jedná se o povinnost vydat nějakou formou osvědčení digitálního úkonu, která se týká všech OVM. V současné době je účinnost tohoto požadavku o dva roky odložena, je však nutno se na ni pečlivě připravit.

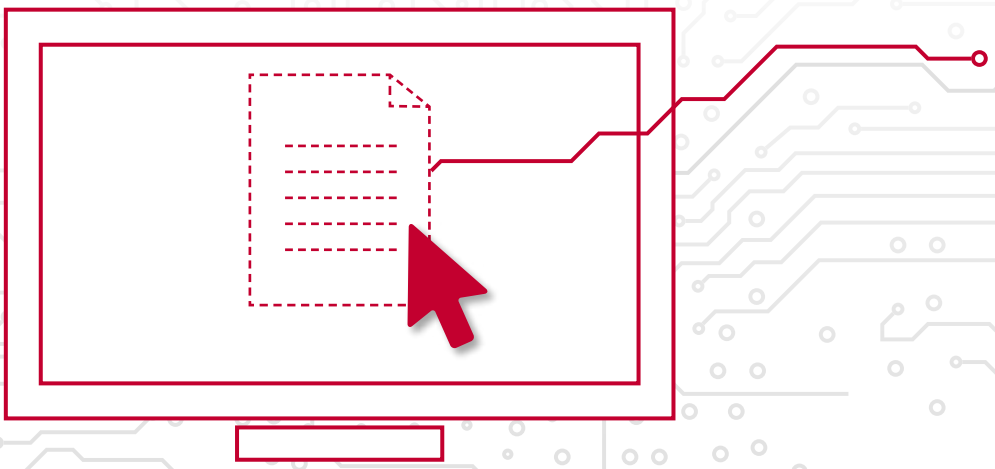
Velkým problémem podle Romana Vrby je i skutečnost, že neexistuje „párování" elektronického podpisu s identitou osoby. I v tomto směru se chystá určité řešení, které by následně umožňovalo díky elektronickému podpisu realizovat daleko větší paletu služeb, neboť bude existovat jistota, že se jím podepsala konkrétní osoba.

Jsou zde k dispozici i tzv. **nátlakové možnosti** veřejnosti vůči úřadům, aby skutečně řešily věci elektronicky, to je, aby platilo ono obíhání dat, nikoli občanů. Tedy fakt, že úřady musí využít údajů, které jsou v elektronické podobě v rámci veřejné správy již k dispozici. Jedná se například o souhlas s využíváním údajů, tzn. moment, kdy mohu dát oprávnění přístupu k jiným agendám i někomu dalšímu. Stejně tak zápis do RPP klientem. Jedná se o situaci, kdy je občan držitelem konkrétního oprávnění (rybářský lístek, lovecký lístek, doklad o vzdělání atp.) a nechce jej stále dokola předkládat ve fyzické podobě. Stačí, pokud jej uloží do RPP a nahlásí každému dalšímu úřadu, že se tam musí podívat a sáhnout si pro něj.

Určitou novinkou je **zápis kontaktního údaje**. Již dnes, pokud občan používá datovou schránku, dostává varování či informaci o blížících se termínech konce platnosti jeho průkazů, nebo například OTP vozidla. Nyní, pokud v rámci ROB a ROS vložíme vlastní kontaktní údaje, tj. mobil či e-mail, budeme úřady informováni touto cestou. MV ČR předpokládá širší využívání právě této možnosti, neboť se jedná o zcela praktickou záležitost.

MV ČR buduje **centrální notifikační službu** tak, aby nemusel každý úřad sám budovat svoji vlastní. Totéž se týká i **platební brány**, pro niž nyní MV ČR ve spolupráci s NAKIT připravuje dynamický nákupní systém. Ten by měl být otevřený všem OVM. V současné době je vybráno zhruba 20 OVM, které budou při startu spolupracovat. Krom jiného by mělo být výhodou tohoto postupu definování jednotného designu. Tedy v momentě, kdy bude občan elektronickou cestou cokoliv platit směrem ke státu, měl by jeho přístup vypadat vždy stejně.

Ze zákona o elektronické identifikaci vychází tzv. **úroveň záruky**. Byla zvolena cesta, kdy nebude konkrétní úroveň záruky pro konkrétní úkony stanovena přímo zákonem, ale v Katalogu služeb bude uvedena jak vazba na samotný úkon, tak na úroveň jeho záruky. V případě, že by zde nebyla uvedena, znamená to automaticky úroveň značnou.



Podstatná je podle Romana Vrby i tzv. **technologická neutralita**. Ještě dnes je možné se v rámci veřejné správy setkat se systémy, které uživatele nutí například k použití konkrétního webového prohlížeče, případně k instalaci konkrétní plug-in či dalších nastavení. Stát by ovšem neměl nutit občany něco instalovat, či používat konkrétní produkt. Od 1. 2. 2020 by se to již rozhodně nemělo stát a měl by se dodržovat princip technologické neutrality, tedy možnost přistoupit k dané službě prostřednictvím libovolné technologie. Jediným omezením v tomto směru je cena případné úpravy. Pokud by cena pro zajištění technologické neutrality byla v zásadně až nepatřičně vysoká, pak to není nutné upravovat. Nicméně je to věcí diskuze.

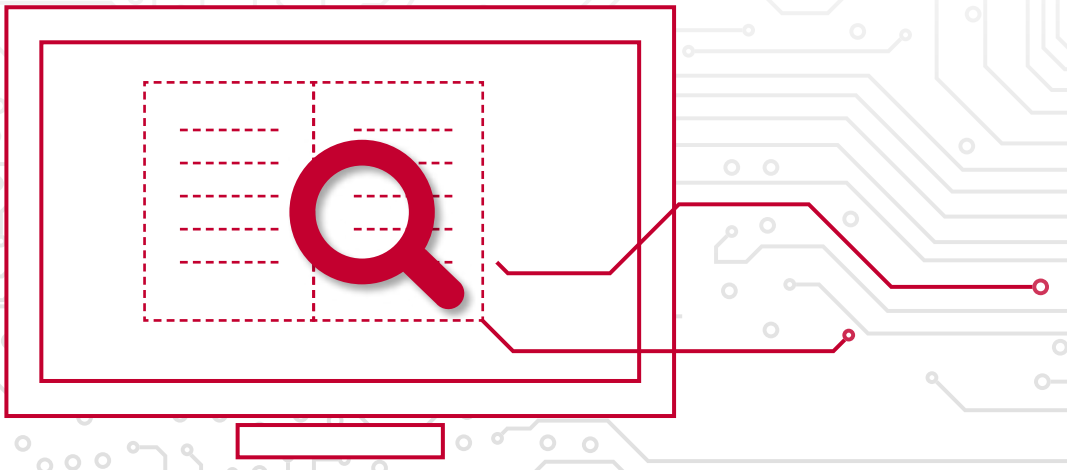
Katalog služeb je rovněž, krom jiného, vhodným **nástrojem pro řízení IT**, respektive jeho rozvoj. V rámci harmonizace digitalizace platí, že daný gestor agendy bude určovat, které agendy budou a v jaké formě a jakém termínu digitalizovány. Pokud tento požadavek schválí vláda, je platný a všichni ostatní jej musí dodržet. Diskutována je rovněž otázka poskytnutí **slevy v případě podání v digitální podobě** (digitálním formulářem). Ta by měla činit 20%, nicméně na výkladu tohoto paragrafu se ještě stále pracuje. Týkat by se však měl skutečně pouze podání v podobě digitálních formulářů.

Jak Roman Vrba uvedl, **Katalog služeb** je skutečně zásadní a výjimečný. Na rozdíl od úkonů na žádost **obsahuje** katalog **skutečně všechny služby**, které stát poskytuje. Tedy jak služby na žádost, tak služby úředně nařízené, a to digitální i nedigitální, tedy i ty, které není možné digitalizovat, a proto nikdy digitální nebudou. Bude to tedy rozsáhlý katalog, který bude dávat přehled o všech službách veřejné správy.

Má však i jiné funkcionality. V samotném popisu jsou provázány příslušné zákony, agendy z nich vyplývající, a to i s odkazem na životní situace. Cílovým záměrem je, aby popisy jednotlivých služeb a úkonů mohly využít i ostatní informační systémy a portály. Tedy například jestliže právě nyní vzniká portál pro jednotnou platební bránu a budou-li popsány jednotlivé služby, které vymezuje toto nařízení, pak by byl nesmysl, aby se tak dělo znovu, když mohou být kdykoliv použity právě tyto popisy.

Samozřejmě v tomto směru hraje velice důležitou roli terminologie, především co je služba a co agenda. Službou v rámci agendy živnostenského podnikání je třeba zřízení ŽL, přerušení, změna..., tedy cokoliv, co je v rámci té agendy činěno, je považováno za službu. Detailnější jsou pak jednotlivé úkony, kdy se může jednat například o samotné podání žádosti, odpověď na tuto žádost atp. Vzhledem k tomu, že jednotlivé úkony mohou být velice detailní, není úplně jednoduché je popsat. I proto vzniká už zmiňovaný tým, který bude pomáhat jednotlivým resortům s naplňováním jejich dat do Katalogu služeb.

Samotný Katalog služeb musí být naplněn do **konce roku 2020**. Zároveň s tvorbou katalogu se pracuje na samotném systému, vyhlášce i metodice. Souběžně probíhá komunikace s ohlašovateli agend. Jakmile bude katalog k dispozici (v polovině roku), mělo by se intenzivně pracovat na jeho naplňování. Bude rovněž propojeno s RPP a ESEL (sbírka eLegislativa). Pracovní termín je do konce roku s malou, měsíční rezervou. Ostrý start musí být 1. 2. 2021.



isss

Doprovodná mezinárodní konference **V4DIS**

TERMÍN POSUNUT NA ČERVEN 2020, SLEDUJTE www.isss.cz

20.–21.4.20 **Hradec**Králové

Kongresové centrum **Aldis**

- **23. ročník** renomované konference – jedné z největších evropských akcí svého druhu
- Mimořádná **příležitost k setkání** se špičkami domácí politické scény, ministry, zástupci státní správy a samospráv z ČR i zahraničí, krajskými či městskými informatiky, vysokými manažery renomovaných firem i nezávislými odborníky
- Přes **200** přednášek a vystoupení během dvoudenního programu, více než **100 prezentujících firem** a institucí
- Rozsáhlá publicita prostřednictvím desítek mediálních partnerů, mezi nimiž nechybí **ČT**, **ČRo** nebo **ČTK**

Konference se bude věnovat zejména těmto tématům

- Jak dál v informatizaci veřejné správy, infrastrukturní projekty, efektivní a centrálně koordinované ICT ve veřejné správě, potřebná legislativa, nové výzvy…
- Další rozvoj efektivní komunikace občanů s veřejnou správou – Portál občana, online služby pro občany a firmy, snižování administrativní zátěže, uživatelsky přívětivé služby…
- Identita v kyberprostoru – NIA, SONIA, identita občana i identita úředníka…
- Rozvoj infrastruktury – podpora regionů a venkova, dotační a nedotační opatření, socioekonomické dopady budování infrastruktury…
- Kybernetická bezpečnost, ochrana osobních údajů…
- Chytrá města, internet věcí, chytré sítě, plné využití potenciálu moderních technologií…
- Cloud, sdílení výpočetního výkonu, sdílené služby, mobilní technologie…
- Transparentnost veřejné správy, otevřená data…
- Digitalizace specifických oblastí veřejné správy – eHealth, digitalizace justice, resortní registry…
- Financování projektů, veřejné zakázky, elektronická tržiště…
- Možnosti implementace zahraničních vzorů a zkušeností…
- Workshopy, panelové diskuse, příklady dobré praxe, populární soutěže…

Další informace týkající se upřesněných okruhů témat a koncepce jednotlivých odborných bloků budou postupně zveřejňovány na

www.isss.cz

eGOVERNMENT CLOUD

Ředitel odboru kybernetické bezpečnosti a koordinace informačních a komunikačních technologií Ing. Miroslav Tůma, Ph.D., navázal na předřečníky především informací o stavu realizace eGovernment Cloudu v ČR. V rámci úvodní rekapitulace hovořil o tom, proč jsme se vlastně začali v ČR bavit o cloudu. Zdůraznil, že všechny důvody stále platí – od správy datových center přes zefektivnění poskytování služeb až po jejich jednotnost, centralizaci, snížení nákladů a vyšší bezpečnost. To vše je stále aktuální a pomoci vyřešit všechny prvky systému může právě cloud. V průběhu doby je evidentní, že se využívání cloudových služeb stále zvyšuje. Ještě před několika lety byl u některých úřadů cítit určitý odpor k přechodu do cloudu. Panovalo často přesvědčení, že mít veškeré služby, data i hardware ve svém držení je lepší, rychlejší a bezpečnější. V současné době se stalo cloudové řešení naprostou součástí práce i života, samozřejmou záležitostí, standardním řešením. Důvody pro jeho používání jsou stejné a neustále se prohlubují. Je tedy vhodné jej v komplexním měřítku začít používat v rámci veřejné správy co nejdříve.

HISTORIE

Vše se odvíjí od roku 2015 a od strategie a akčního plánu kyberbezpečnosti. Prvotním záměrem nebylo ani tak vybudovat Cloud Computing v dnešním měřítku. Šlo spíše o to dát najevo, že chceme-li realizovat Cloud Computing, může být právě eGC tou správnou variantou. Postupně však bylo jasné, že jiná cesta není. Bylo tedy nutné nastavit potřebné mantinely. Právě snaha o jejich nastavení vedla k vytvoření závěrečné analytické zprávy, kterou vláda svým usnesením přijala. Bylo tak stanoveno, jak vlastně bude eGC vypadat, jaké bude mít zakotvení v legislativě a jak budou vypadat jednotlivé postupy, aby byly skutečně realizovatelné.

STRUKTURA

Dnes má eGC jasně definovanou strukturu. Skládá se ze dvou částí – komerční a státní. Komerční část umožňuje standardní chování trhu, tedy soutěž. Ve státní části jsou, či budou systémy řazeny napřímo. Podstatné je, že obě části spolu nijak nekomunikují, nejsou nijak propojeny. Důvodem je skutečnost, že státní část eGC je zaměřena výhradně na systémy, které jsou z pohledu státu nejvýznamnější – tedy systémy zařazení dle bezpečnostní úrovně 4. Metodika klasifikace jednotlivých systémů dle bezpečnostních úrovní vychází do jisté míry ze zákona o kyberbezpečnosti, ale nekopíruje přímo kritické informační systémy. Je poněkud hlubší a zaměřená především na cloudové služby, tzn. systémy, které jsou na základě tohoto vyhodnocení v kategorii 4, musí být zařazeny ve státní části eGC, neboť ta je plně pod kontrolou státu. Naopak systémy, které jsou vyhodnoceny v kategoriích nižších, směřují do komerční části eGC a neměly by se objevit ve státní, mimo jiné z kapacitních důvodů.

Komerční část je nyní víceméně již spuštěna, jsou dokončovány poslední kroky k tomu, aby mohly být realizovány první služby v pilotním režimu.

ZÁKLADNÍ PRAVIDLA

Základními pravidly eGC je:

- rozdělení do dvou částí;
- nulová konkurence těchto částí;
- státní část je plně pod kontrolou státu;
- vstup do cloudu je jednoznačně dobrovolnou záležitostí.

Není žádné nařízení, které by kohokoliv nutilo, že musí jít do cloudu. Bude však nařízení, které říká, že je nutné zvažovat cloudové služby. Tedy je nutné při jakékoliv technologické změně uvažovat na základě metodiky o tom, zda je výhodnější umístit systém do cloudu, či nechat tak, jak běžel doposud. Jedná se o metodiku TCO (určení celkových investičních a provozních nákladů IS za 5 let provozu), která jednoznačně určí, na základě nákladů a tedy porovnání současného provozu s nabídkou komerčních i státních služeb v eGC (dle zařazení), která cesta je výhodnější. V případě, že bude výsledek tohoto porovnání ukazovat na výhodnější model s využitím eGC, vzniká subjektu povinnost využití těchto služeb. (Výjimkou mohou být situace, kdy převedení do cloudu by z nějakého objektivního důvodu bylo velice, až nepatřičně komplikované.) Tento přístup znamená, že k naplňovaní eGC bude docházet postupně, nejčastěji v momentu konkrétních úprav či změn.

Bylo provedeno hodnocení systémů kritické informační infrastruktury a významných informačních systémů státu pro jejich zařazení do konkrétní bezpečnostní úrovně. I když chybí ještě vyhodnotit cca 15 %, už nyní je zřejmé, že systémů s úrovní 4, tedy těch, které budou automaticky zařazeny do státní části eGC, nebude více jak 50. V ostatních úrovních je ve třetí skupině zařazeno cca 80 %, ve druhé 18 % a v první se nenachází žádný systém. Důležité je však, že se zatím byly hodnoceny pouze kritické a významné IS, nikoli všech ISVS. Stanovení počtu bylo však důležité především pro kapacitní a finanční nároky. U komerční části je celý přístup daleko jednodušší, protože je stanoven na základě soutěžení. U státní části je nutné připravit odpovídající legislativu a samotné řešení.

Paralelně s bezpečnostní úrovní se provádělo u jednotlivých systémů hodnocení TCO. Z něho vyplývá cenový rozptyl jejich pořízení od 0 do 0,5 mld. Kč. Byly zároveň posuzovány náklady na jejich pětiletý provoz, které se podle druhu systému pohybují od 330 tisíc do 1,3 mld. Kč. Tím byla určena jakási průměrná hodnota 19 mil. Kč ročního provozu. Je to však pouze určitý prvotní údaj pro vzájemné porovnávání jednotlivých systémů. Rozhodně není možné tvrdit, že automaticky ty systémy, které stojí pod 19 mil., jsou výhodnější a naopak. Jedná se pouze o určité vodítko při výběru systémů i komerčních nabídek.

VARIANTY POSKYTOVÁNÍ

Služby v rámci komerční části budou poskytovány buď tzv. napřímo, nebo prostřednictvím partnera či integrátora. Platí však, že vše musí být nastaveno tak, aby v případě jakýchkoliv potíží bylo kdykoliv možné přejít k jinému poskytovateli cloudových služeb.

Každá služba by měla být zanesena v katalogu služeb. Každý poskytovatel, pokud chce takovou službu poskytovat, ji tedy musí zanést (prezentovat) do katalogu. Služba projde schvalováním a teprve poté je v katalogu uveřejněna. Paralelně jsou v katalogu viditelné nabídky od zadavatelů, kteří si vybírají k následné soutěži ze zařazených služeb. Podstatné je, že katalog by měl být neustále rozvíjen.
Současně s katalogem jsou podstatné rovněž smluvní podmínky, které jsou definovány jak pro komerční, tak státní část a jejich splnění bude vyžadováno jako zachování minimálního bezpečnostního standardu. Samozřejmě, že zadavatel si v rámci výběru může tyto základní podmínky zpřísnit, pokud to uzná za vhodné.

ŘÍDÍCÍ ORGÁN

Výkonem funkce řídícího orgánu je pověřeno MV ČR. Řídící orgán – ŘoeGC – je tak arbitrem, který by měl koordinovat celý eGC, dohlížet a garantovat jednotný informační systém, ale hlavně řešit schvalování a zařazování nabídek v rámci katalogu služeb, případně řešit arbitrážní činnost zařazování systémů do jednotlivých bezpečnostních úrovní.

Jsou jasně definovány činnosti, které v rámci celého životního cyklu cloudu budou tvořeny jednotlivými poskytovateli či konzumenty služeb. Vše by mělo vždy začínat určitým soutěžním rámcem (DNS dynamický nákupní systém), na který pak navazují jednotlivé minitendry, které se do jisté míry mohou překrývat, neboť bude záležet na vzájemné nabídce a poptávce umístění jednotlivých systémů či změn. Konkrétně v tomto okamžiku jsme ve fázi, kdy je připraven první katalog, připraveno vypsání prvního DNS, provedena předběžná konzultace, kterou se celý mechanismus ověřil a potvrdilo se, že v rámci trhu nenarazíme na nějaký problém. Nyní dojde k naplňování katalogu a vypsání DNS, což je otázka měsíce až měsíce a půl. Zhruba v tomto rozmezí by měli být kvalifikováni první dodavatelé a následně budou vypracovány první katalogové listy, vypsány první minitendry a dojde ke spuštění prvních služeb, od cloudových až po konzultační, integrační či migrační. Tím bude nabízena možnost komplexního servisu pro přechod systému do cloudu a garantován celý postup.
V rámci Digitálního Česka jsou k dispozici dostatečné zdroje pro rozvoj, a to jak z pohledu kapacitního, tak finančních prostředků nutných pro budování eGC. Samotný IS nutný pro eGC bude vycházet z dosavadních, již existujících systémů. Je zde řada portálů, které se budou modifikovat, doplní se variantou pro cloud s provazbou na NEN atp. Jde o to postupně synchronizovat vše, co je k dispozici do jednoho funkčního celku.

LETOS

V letošním roce je možné očekávat posílení týmů ŘOeGC pracovníky vyčleněnými výhradně na problematiku eGC. Bude dokončeno hodnocení bezpečnostních úrovní a TCO pro první systémy. Dále dojde k dopracování legislativního ukotvení, alespoň v případě státní části eGC. V tomto směru je nutné vyřešit určitý problém spojený s tím, jak může stát zadat konkrétní systém přímo do státní části cloudu konkrétnímu provozovateli.
Bude tedy sestaven samostatný útvar jako řídící orgán eGC, vytvořen katalog, vypsány pilotní DNS a to vše bude předloženo vládě, která může posvětit následující kroky. Pak bude skutečně možné konstatovat, že začíná provoz a následný rozvoj eGC a budeme moci realizovat vyšší bezpečnost a efektivitu jednotlivých systémů.

OSOBNOST eGOVERNMENTU 2020

GORDIC

NOVÝ TERMÍN
14. 10. 2020

14. 10. 2020, 19:00
Nová budova
Národního muzea
Praha

www.egovernment.cz

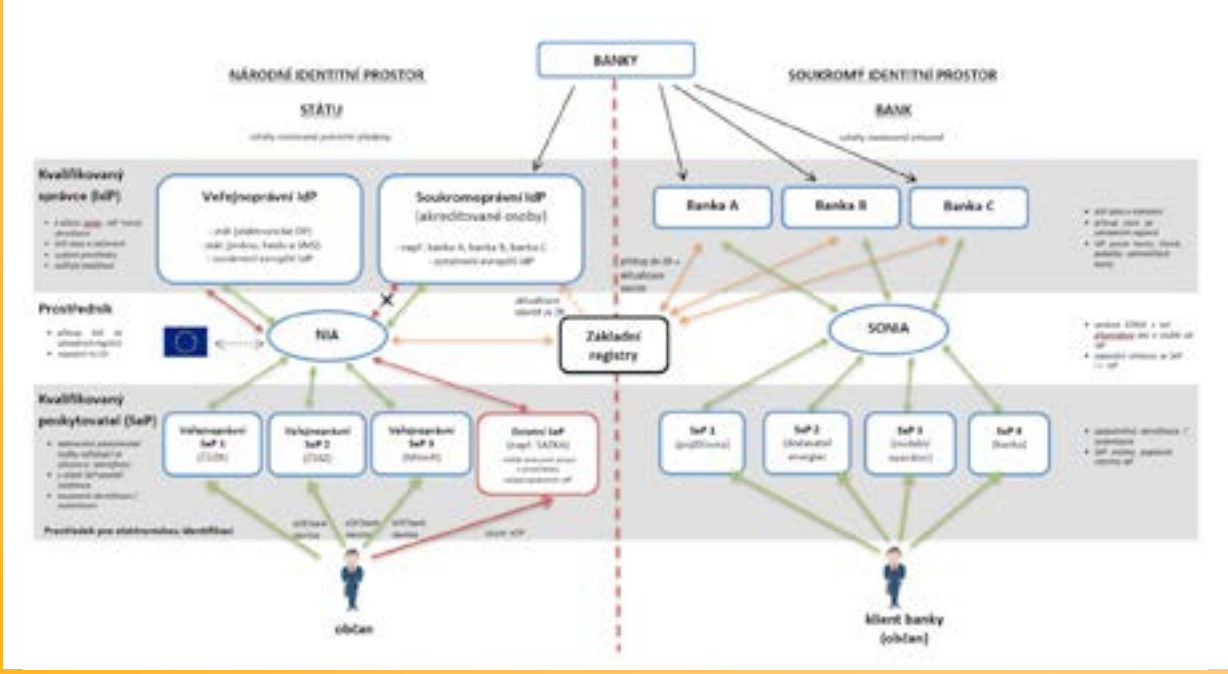
DNA E-GOVERNMENTU?

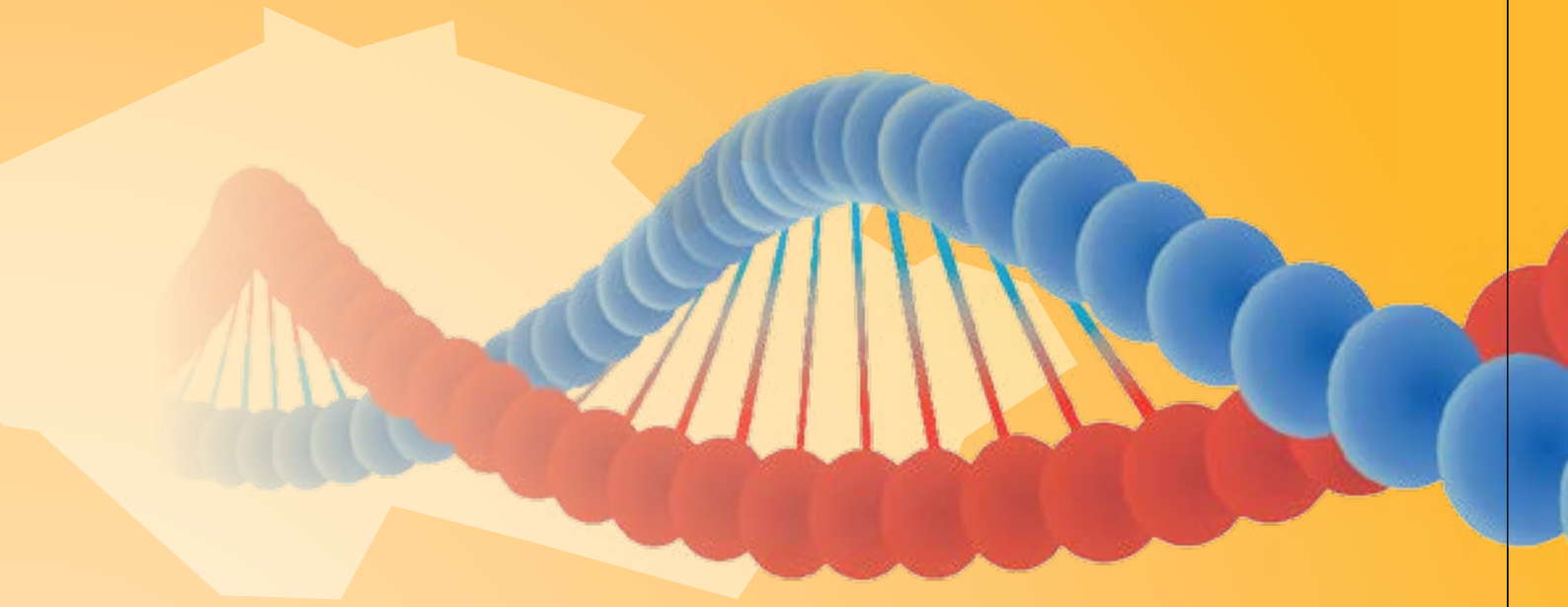
Své vystoupení zaměřil prezident ICT Unie Zdeněk Zajíček na bankovní identitu, ale jak sám upozornil, vzal ji spíše jako určitý předstupeň k něčemu, o čem by chtěl v následujících měsících, možná letech vést skutečně živou diskuzi a co by se mělo by stát žhavým tématem.

BANK ID

Legislativní změna zákona o bankách umožní, aby tyto instituce směly vlastní identitní prostředky (přístupová práva - údaje pro vstup do internetového bankovnictví),nabízet nejen svým klientům a nejen pro přístup ke službám jediné banky. Bude možné, aby s těmito prostředky mohli klienti přistupovat ke službám státu a případně i ke službám jiných komerčních poskytovatelů. Přístupovými údaji k internetovému bankovnictví bude tedy klient moci prokázat svoji identitu například vůči službám pojišťovny, letecké společnosti, autobazaru, realitní kanceláře a řady dalších. Ve všech těchto případech by pro vstup, tedy prokázání identity, mělo stačit zadání bankovní identity. V rámci této komerční linie budou moci banky tuto službu – ověření identity – zpoplatnit. Mezi komerčními subjekty bude prokazování identity a její akceptace postaveno na komerčním vztahu. A banky, protože si budou konkurovat, budou poskytovat svoje identitní prostředky. Návrh vychází ze skutečnosti, že banky mají s udržováním kmene klientů a správou jejich identitních údajů a prostředků určité náklady. Tím, že bude možné je poskytovat jako placenou službu někomu dalšímu, dojde k určitému umořování těchto nákladů. Zároveň, protože poskytování této služby bude nabízet větší počet bank, dojde automaticky ke konkurenci nabídky, a tedy regulaci ceny této služby.

Výsledkem bude situace, kdy budeme mít identitní prostředek, který je možné nazvat „bankovní občankou“. Tou se budeme moci v komerčním světě prokazovat téměř vůči komukoliv. Stejně by to ale mělo platit i ve státním sektoru. I vůči službám státu se, na základě uvedené novely, budeme moci prokazovat svojí bankovní identitou. Na rozdíl od komerční sféry prokazování vůči státu (státním organizacím) a vůči samosprávě, tedy vůči obcím a krajům, bude bezplatné. Určitou výjimkou v tomto směru budou „hybridní“ subjekty (školy, zdravotní pojišťovny, nemocnice, zdravotnická zařízení...), u nichž se bude ještě vyjednávat o určitých komerčních podmínkách, neboť se u nich nedá vždy úplně oddělit, kdy přesně taková instituce





vystupuje jako orgán veřejné moci a ve kterých okamžicích vystupuje v rámci soukromoprávního stavu. Mělo by se však jednat o minimální poplatek.

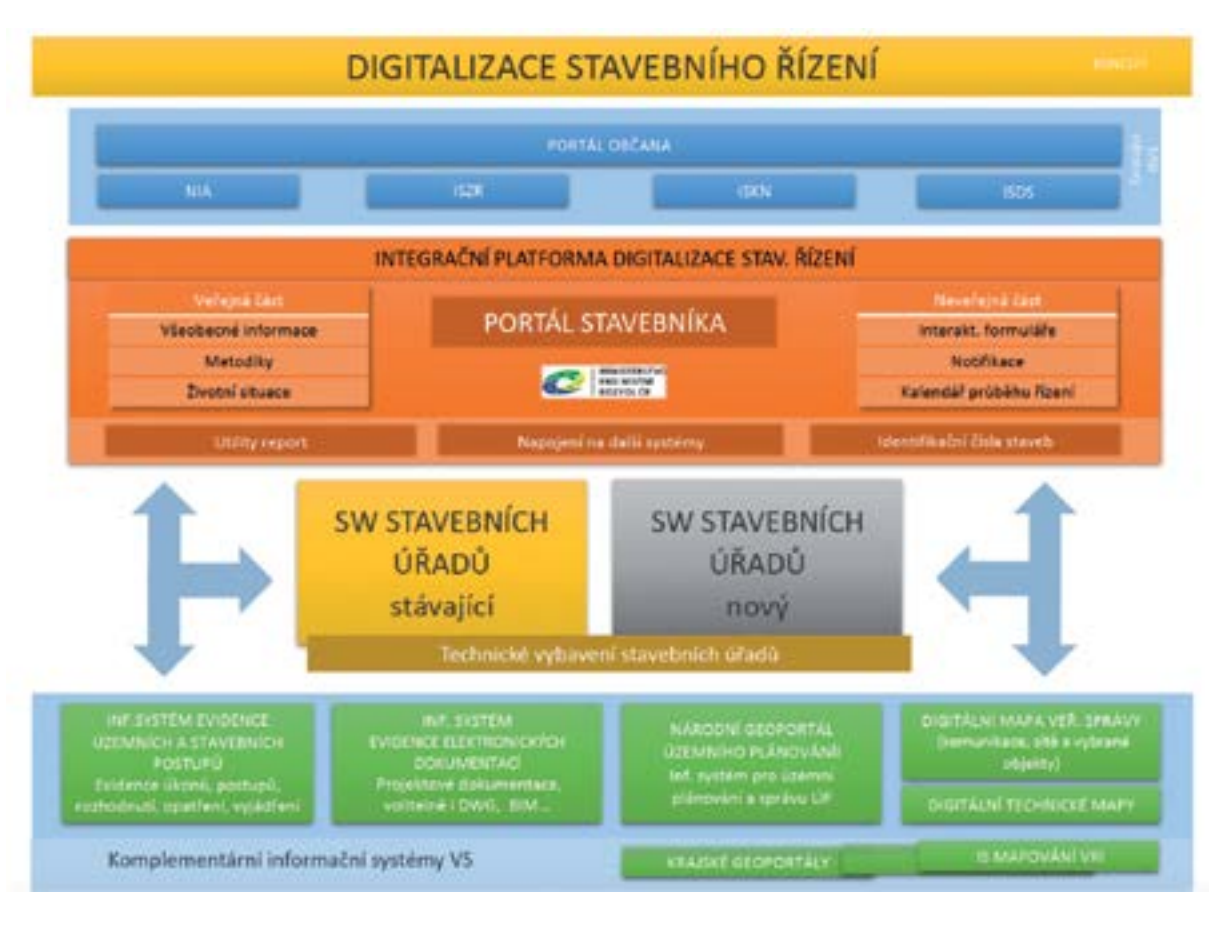
Dojde tedy k situaci, kdy bude identitní svět rozdělen mezi NIA (Národní identitní autorita) a SONIA (SOUkromoprávní NIA) a uprostřed se budou nacházet základní registry. Bankám bude umožněno přistupovat svými informačními systémy k systému základních registrů a touto cestou aktualizovat data o svých klientech směrem do svých vlastních systémů. To je varianta, která bankám uspoří další náklady, ale především uspoří náklady a čas samotným klientům. Ti nebudou nuceni opakovaně předkládat bance, ale i řadě dalších institucí údaje, u kterých to tak nyní musí činit (změna bydliště, změna příjmení, případně další údaje, které si banky budou moci nyní samy ověřit).

SPOLUPRÁCE

Kromě samotného Bank ID jsou tady i další digitální kroky, na kterých spolupracuje ICT Unie spolu s veřejnou i státní správou. Je to samozřejmě zákon o právu na digitální službu, ale také digitalizace stavebního řízení a s ním spojená digitální technická mapa atp. Je zřejmé, že je to do jisté míry klíčový moment, kdy je nutné rozhodnout, jak bude náš stát přistupovat k leckdy velice dynamickým technologickým změnám současnosti. Doposud byl totiž spíše vysoce konzervativní. Základní příčinou toho, proč stát sám o sobě nemůže a není schopen reagovat stejně dynamicky jako komerční sféra, je pravidlo, podle něhož úřad může dělat pouze to, co má zákonem uloženo, a nesmí dělat nic mimo tento rámec. Výsledkem je skutečnost, že úřady jsou spíše opatrnější a méně inovativní, protože inovativnost není obsahem onoho zadání. Snaží se pouze přesně dodržovat to, co je nařízeno. A to je vlastně brzdí. Je to určitá genetická výbava veřejné správy.

DNA

Zdeněk Zajíček při svém vystoupení představil návrh na vytvoření Digitální Národní Aliance – DNA, která by směřovala ke spolupráci státu a komerčního sektoru. Stát, čistě z principu, nemůže vpustit komerční svět do svého rozhodování a řízení, ale je možné, aby hledal styčné body pro spolupráci. Mohla by tedy vzniknout platforma, kde by se dokázal potkávat komerční a veřejný sektor, diskutovaly by o tom, jaké služby by mohly být a v jakých společných projektech by byly poskytovány do veřejné správy zvnějšku. Komerční sektor, který přirozeně sleduje z konkurenčních důvodů inovace a trendy doby, by tedy ovlivňoval státní sektor, přičemž by to nebylo považováno za něco podezřelého. Právě projekt Bank ID jasně ukazuje smysluplnost takového vztahu. Stát totiž, v okamžiku, kdy takto začne s bankami spolupracovat, nemusí budovat složitou strukturu pro vytváření elektronických identitních prostředků. Automaticky využije to, co tady už existuje, tedy to, co banky používají. V tomto případě naopak lze předpokládat, že banky budou určitým garantem kvality a bezpečnosti, neboť i pro ně je důležité, aby data klientů byla ochráněna, a tak lze předpokládat, že v zavádění technologických inovací budou pružnější, než by byl stát sám. Je to situace, ze které mohou profitovat banky, stát i klienti obou dvou.



NEJEN BANK ID

Projektem, který by v tomto směru spolupráce mohl navazovat, je určitě digitálně technická mapa. Byla prosazena ve spolupráci krajů, obcí a soukromého sektoru jako vytváření společného prostoru, ve kterém se budou sbírat nejen data o infrastruktuře v ČR, ale také o objektech a stavbách. Část dat bude pořizovat stát, respektive OVM, územní samospráva. Část dat bude naopak pořízena soukromými vlastníky infrastruktury. A jejich společným zájmem samozřejmě je, aby bylo k dispozici co nejvíce relevantních dat v co nejlepší kvalitě.

Dalším takovým je projekt PES – právní elektronický systém, který zahájila Hospodářská komora. Jedná se o přehled podnikatelských povinností, které vyplývají z legislativy. V tuto chvíli tedy nemá smysl budovat stejný systém třeba na Ministerstvu průmyslu a obchodu, protože jej nedá dohromady, respektive ne tak snadno. Daleko lépe takový přehled sestavuje ten, kdo pracuje pro ty klienty, jichž se týká. Je logické, že úřady pohlížejí na každou problematiku svým úhlem pohledu, nikoli například pohledem podnikatele atp. Bylo by to vhodnější, aby stát využil možností, které mu dává úzký kontakt HK s jejími klienty. Stejně tak by mohly existovat projekty, které by byly realizovány ve spolupráci státu a Agrární komory, Hospodářské komory a státu, bankami a státem, pojišťovnami a státem atp. Stát by tedy vždy měl ke spolupráci přizvat někoho, kdo konkrétní službu poskytuje, kde je možné využít synergii, vzájemně se obohacovat a posouvat dál. Změnit nastavení veřejné správy – změnit její DNA – a svázat komerční a státní svět do úzké spolupráce ku prospěchu obou.

Jedním ze zásadních úskalí rozvoje čehokoliv v rámci veřejné a státní správy jsou soutěže. I malá zakázka trvá měsíce či roky, než se dostaneme k výsledku. Přitom se jedná o službu, kterou může poskytovat banka, jako například Bank ID. Nebude tedy v tomto případě nutné soutěžit systém na identitní prostředky ani v obcích ani v rámci státu. Bude se používat ten, který tady už existuje. Je to pouze o důvěře, nastavení parametrů, samozřejmě i zpracování krizových týmů, pokud by cokoliv nemohlo z nějakých důvodů fungovat. Ale každopádně je to vhodnější přístup, než že by totéž vyvíjel sám pro sebe stát, kraje

a obce. Nebude toho schopen, protože nebude zvládat sledovat trendy a řídit inovace. Vhodně to dokazuje například zvolený princip eGovernment Cloudu (hovořil o něm Miroslav Tůma). Jedná se o přístupy, které mohou realizovat soukromý a státní sektor dohromady ve společném právním rámci, ve společném „nákupním centru". To, že výsledkem je jeden malý, specializovaný obchod a vedle toho velký supermarket, jen odráží momentální potřeby. V synergii je pak možné dohledat úspory na obou stranách při zajištění technologického pokroku.

Je nutné stavět sítě z veřejných prostředků (stát, obce, kraje)? Je to efektivní a správné řešení? Není lepší, aby se ve spolupráci státu a privátního sektoru hledaly modely, jak zefektivnit využívání již existující infrastruktury? Je potřeba stavět efektivně, nemá smysl stavět paralelní sítě státu a soukromého sektoru, je potřeba je sdílet, tedy hledat technické, právní a bezpečnostní řešení, které to umožní.

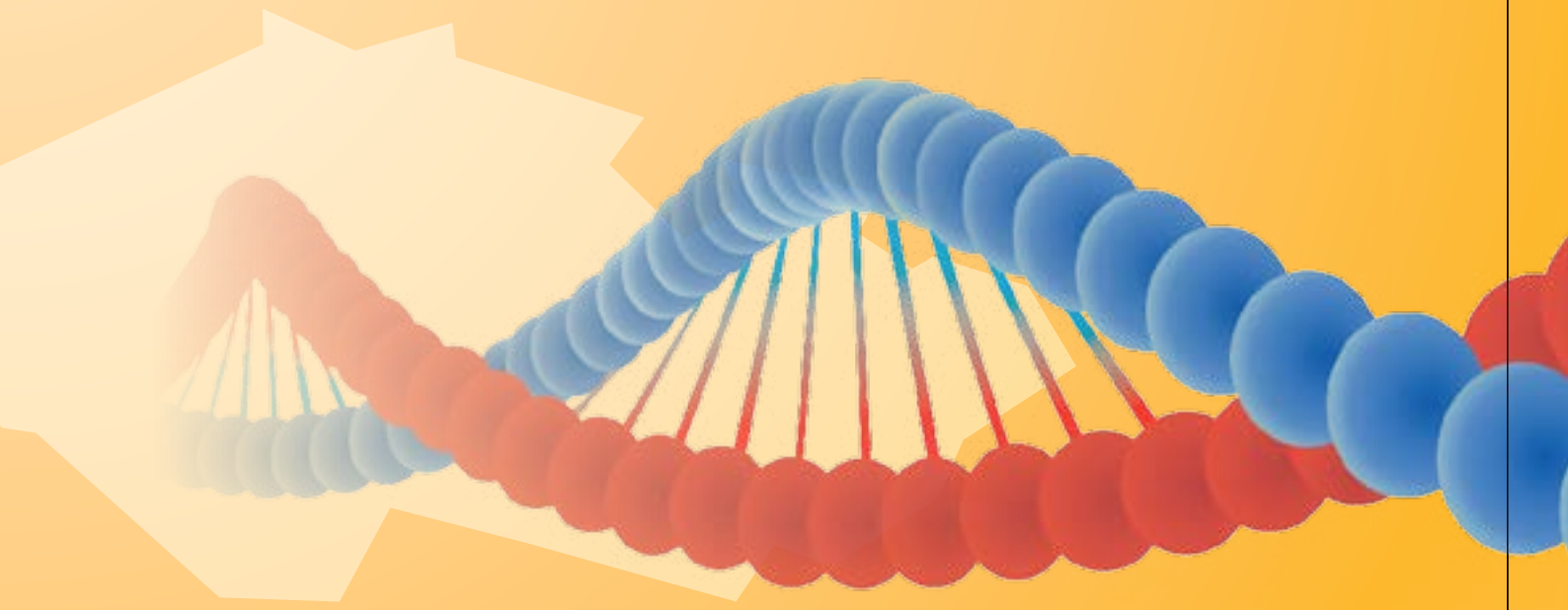
V rámci kybernetické bezpečnosti je možné prohlásit, že soukromý sektor je skutečně nešťastný z toho, že se o tomto tématu nemluví veřejně ve smyslu, jak zabezpečit společný kybernetický prostor. Škody, které v kyberprostoru nějakým útokem vznikají, totiž nevznikají jen státu, ale rovněž soukromému sektoru. Nemožnost spolehnout se na elektronickou poštu v rámci určitého ministerstva je nepříjemné, ale skutečnost, že konkrétní nemocnice nemůže v důsledku kyberútoku operovat, tedy neobsluhuje klienty, je varující. Přitom je lhostejné, zda je státní či soukromá, malá či velká. Totéž platí pro banky, utility, operátory. Mít dobrý zákon o kybernetické bezpečnosti je nutné, ale není tím vše vyřešeno. Je důležité o hrozbách mluvit a vytvořit platformu, aby spolu mohli navzájem komunikovat ti, kteří jsou schopni těmto hrozbám čelit.

ZÁVĚR

Partnerství veřejného a soukromého sektoru je tedy velké téma. Má bez pochyby svá rizika, o kterých je nutné vědět a sledovat je. To ale neznamená, že máme dál budovat sféru státu a veřejného sektoru odděleně. Je potřeba, aby společně oba tyto sektory stát inovovaly. Stát musí být z principu konzervativní, protože tak chrání své nastavení, ale bez invence ze strany soukromého sektoru se nebude rozvíjet.

Proto Zdeněk Zajíček volá po vzniku **DIGITÁLNÍ NÁRODNÍ ALIANCE**, do které by měli být přizváni všichni, kdož jsou schopni se podílet na hledání inovací a dalších směrů přístupu.

Prostor pro setkávání a vzájemnou spolupráci zde je, nyní je třeba najít odvahu s vědomím, že taková spolupráce není příznakem něčeho nekalého, ale je to svazek, z něhož těží stát, firmy i občané.



Služba vytváření kvalifikovaných elektronických podpisů na dálku I.CA RemoteSign

V současné době rostou nároky na zjednodušení a zrychlení procesů založených na smluvních vztazích, ale také na dalších obchodních dokumentech. Řešením je využívání elektronizace agend, a tedy i vytváření elektronických dokumentů, které musí plnohodnotně nahradit dokumenty fyzické, a to včetně podpisů. Jedině kvalifikovaný elektronický podpis je ekvivalentem vlastnoručního podpisu a pro jeho vytváření je nezbytné, aby podepisující osoba měla k dispozici bezpečné zařízení – kvalifikovaný prostředek pro vytváření elektronického podpisu (QESCD) v podobě čipové karty nebo USB tokenu.

Ne vždy je takové řešení pro uživatele vhodné a jednoduše použitelné. První certifikační autorita, a.s. (I.CA), připravila a nabízí nové řešení, tzv. elektronické podepisování na dálku pod obchodním názvem I.CA RemoteSign.

Uživatel této služby nemá vlastní bezpečné zařízení – QESCD, ale využívá vzdáleného přístupu k bezpečnému zařízení, které je spravováno akreditovaným poskytovatelem služeb vytvářejících důvěru, a to plně v souladu s požadavky Nařízení EU 910/2014 – eIDAS (články 51 a 52).

Služba I.CA RemoteSign umožňuje vytváření kvalifikovaného elektronického podpisu na mobilních zařízeních (mobilní telefony a tablety). Uživatel má vždy k dispozici speciální aplikaci, kterou využívá pro přijímání požadavků a vytváření kvalifikovaného elektronického podpisu. V současnosti jsou v rámci služby podporována mobilní zařízení s operačním systémem Android nebo iOS. Dalším krokem je rozšíření pro další typy zařízení (PC/NB) na platformě Windows.

Služba I.CA RemoteSign podporuje vytváření elektronických podpisů ve formátech PAdES-B-B a PAdES-B-T dle EN 319 142-1a CAdES-B-B a CAdES-B-T dle EN 319 122-1.

Aktivace služby, správa identit a prodloužení služby

Aktivace služby probíhá na obchodním místě I.CA. Na obchodním místě je provedeno ověření totožnosti uživatele (žadatele o službu) a jeho registrace. Po provedení registrace uživatel získá podklady pro aktivaci služby, tzv. aktivační obálku, která (jako jediná) obsahuje potřebné „tajemství“ pro zpřístupnění práce s privátním klíčem, k němuž byl vydán příslušný kvalifikovaný certifikát. Poté si uživatel stáhne aplikaci I.CA RemoteSign a pro její aktivaci použije kód z aktivační obálky, kterou získal při registraci. Během procesu aktivace dochází ke generování

Podepisování dokumentů

1. Poskytovatel služeb vytvoří požadavek na podpis dokumentu.
2. Požadavek je vložen do systému I.CA RemoteSign (RSiCon) na straně poskytovatele služeb.
3. Systém I.CA RemoteSign odešle notifikaci o novém požadavku k podpisu příslušnému uživateli.
4. Uživatel v aplikaci I.CA RemoteSign zaslaný požadavek podepíše.
5. Podepsaný požadavek je předán a uložen na do systému I.CA RemoteSign na straně poskytovatele služeb.
6. Poskytovatel služeb si převezme podepsaný požadavek a provede jeho zpracování.

prvního párů klíčů pro danou identitu a vydání prvotního kvalifikovaného certifikátu. Po aktivaci aplikace je služba okamžitě dostupná.

Technické řešení

Poskytovatel služeb vkládá požadavky k podpisu prostřednictvím komponenty RSiCon, která je integrována v jeho interním systému. Na základě jeho požadavku dojde v komponentě RSiCon k realizaci procesů nutných pro realizaci podpisu (výpočet hash, vytvoření náhledu dokumentu atd.).

Na I.CA RemoteSign Server, provozovaný v prostředí I.CA, je následně zaslán požadavek obsahující potřebné informace. I.CA RemoteSign server systému poskytovatele služeb vrací informaci o úspěšném založení požadavku spolu s daty, která je nutné uchovat do okamžiku ukončení podepisovací transakce.

Po založení požadavku k podpisu v systému I.CA RemoteSign I.CA kontaktuje jednotlivá aktivní zařízení daného uživatele formou push notifikace. Po otevření push notifikace dojde k otevření mobilní aplikace I.CA RemoteSign. Po autentizaci uživatele (heslem, případně biometricky) se zobrazí seznam požadavků čekajících k podpisu. Uživatel si může u jednotlivých dokumentů zobrazit detailní informace.

Každý požadavek má definovanou platnost, což je časový údaj definovaný poskytovatelem služeb. Po jeho uplynutí požadavek k podpisu expiruje a uživatel jej nemá dále možnost podepsat.

Pokud se uživatel rozhodne požadavek podepsat, je vyzván k zadání hesla pro podpis na dálku. Je-li heslo správné, vytvoří se kvalifikovaný elektronický podpis hashe podepisovaných dat.

Po vytvoření podpisu dochází k tzv. notifikaci systému poskytovatele služeb, který je touto cestou informován o změně stavu podpisové transakce. Na základě této notifikace systém poskytovatele služeb zavolá prostřednictvím komponenty RSiCon systém I.CA RemoteSign. Dojde ke stažení kryptogramu do systému poskytovatele služeb a následnému sestavení kompletního podepsaného dokumentu. Podepsaný dokument je následně vrácen volajícímu systému poskytovatele služeb a je možné s ním nakládat jako s jakýmkoliv jiným elektronicky podepsaným dokumentem.

Bezpečnost

Kvalifikovaný elektronický podpis je vytvářen na certifikovaném HSM (QESCD) ve správě kvalifikovaného poskytovatele služeb vytvářejících důvěru.

Veškerá komunikace mezi mobilním zařízením uživatele a službou I.CA RemoteSign je šifrována speciálně vytvořeným protokolem.

Data předávaná do systému I.CA RemoteSign nezahrnují obsah podepisovaného dokumentu.

Náhled dokumentu v PDF formátu nebo odkaz na stažení podepisovaných dat jsou předávány v zašifrované podobě. K jejich dešifrování může dojít až na koncovém zařízení podepisujícího uživatele.

V rámci procesu aktivace prvního zařízení uživatele dojde k úpravě zabezpečení přístupu k privátnímu klíči takovým způsobem, že nadále již k přístupu nepostačuje obsah aktivační obálky, ale je nutná kombinace tajemství uloženého v zařízení uživatele (generovaného v rámci aktivace) a hesla pro podpis na dálku, jež si uživatel během aktivace zvolil.

Během procesu podpisu neopouští privátní klíč k certifikátu bezpečné prostředí HSM modulu, pouze dojde v zařízení uživatele k sestavení tzv. SAD (Signature Activation Data), která obsahují autorizaci použití klíče uživatele na konkrétní hash hodnotu. Tato SAD jsou zaslána do HSM modulu, kde dojde k ověření jejich správnosti a po úspěšném ověření je proveden podpis pomocí privátního klíče uživatele nad příslušným hashem. Tato vzniklá hodnota kryptogramu je pak následně použita pro sestavení celé struktury elektronického podpisu dle příslušných norem.

Závěr

Služba I.CA RemoteSign umožní podepisovat dokumenty (uzavírat smlouvy, závazné objednávky nebo jiné dokumenty) uživatelům chytrých telefonů, tabletů i PC/NB. Služba je využitelná různými poskytovateli služeb, jako jsou banky, pojišťovny, dodavatelé energií a řada dalších obchodních subjektů a rovněž orgánů veřejné moci.

Roman Mašata,
vedoucí projektu a key account manažer,
První certifikační autorita, a.s.

MÁM SEN

I Have a Dream (česky Mám sen) je vžité pojmenování pro historický projev Martina Luthera Kinga, Jr., jehož nosnou myšlenkou bylo volání po rovnosti ras a konci diskriminace (zdroj: Wikipedia).

Mám také sen o konci diskriminace, o konci diskriminace elektronického podpisu, elektronické pečeti, časového razítka a všech dalších náležitostí, spojených se slovem – bohužel zatím jen bájným – Paperless. Pokud hovořím o diskriminaci, nemyslím nějaké legislativní překážky, ale překážky v kontextu užití všech elektronických věcí, spojených s autorizací dokumentů, a zahájení budování skutečného Paperless v každé firmě, na každém úřadu. Řekněme si to otevřeně, rovnoprávnost elektronického podpisu s podpisem „modrou" už tady máme drahně let, ale kam jsme to se zaváděním Paperless reálně dotáhli? Dovolím si říct, že moc daleko ne.

Zákony sice máme, ale překážek je pořád dost a ty ceny... Jen si vezměte takový elektronický podpis. Pokud chceme (a já věřím, že chceme) používat kvalifikovaný elektronický podpis, popř. kvalifikovanou elektronickou pečeť jako tu správnou metu pro Paperless autorizaci obsahu, nezbývá nám nic jiného, než si pořídit kvalifikovaný certifikát pro podpis/pečeť na nějakém kvalifikovaném prostředku – token, čipová karta. A ten mít neustále při sobě... Vlastnit zařízení, na kterém token, čipová karta funguje, ideálně se nevzdalovat od počítače, protože na mobil, tablet a jiný než podporovaný systém můžete zapomenout. To má být ten Paperless? To má být ta jednoduchost užití?

Mám sen. Mám sen o používání elektronického podpisu, které nemá limity, které je jednoduché, funguje kdekoli, na čemkoli, z práce, z domova, kdykoli, kdy máte čas, kdykoli to potřebujete. Mám sen, že díky této jednoduchosti už nebude skutečnému Paperless nic bránit. Smlouvy elektronicky, faktury elektronicky, různá potvrzení, žádosti atd., atd. jen elektronicky, veškerá komunikace jen elektronicky a ověřitelně, bez ohledu, na kterém kontinentu, či v které zemi se nacházíte. A co potom archivace? Krásně bez papíru, a to s minimálními nároky na systémy (využití stávajících), čas a peníze.

Asi si nyní říkáte, že toto přece všechno už jde. Ano, ale... Kolik znáte lidí, kteří mají elektronický podpisový certifikát a kteří jej používají, kolik statutárních zástupců podepisuje smlouvy elektronicky, kolik úředníků využívá elektronický podpis? A kolik z nich je schopno takový dokument přijmout a zpracovat? Každý ve firmě či na úřadě, nebo jen vyvolení? Proč ne všichni?

Jednoduše:

- je to drahé;
- je to nepohodlné;
- je to svazující (konkrétní počítač, konkrétní systém...);
- může se to ztratit;
- složité na údržbu.

A myslím, že pár dalších důvodů by se našlo...

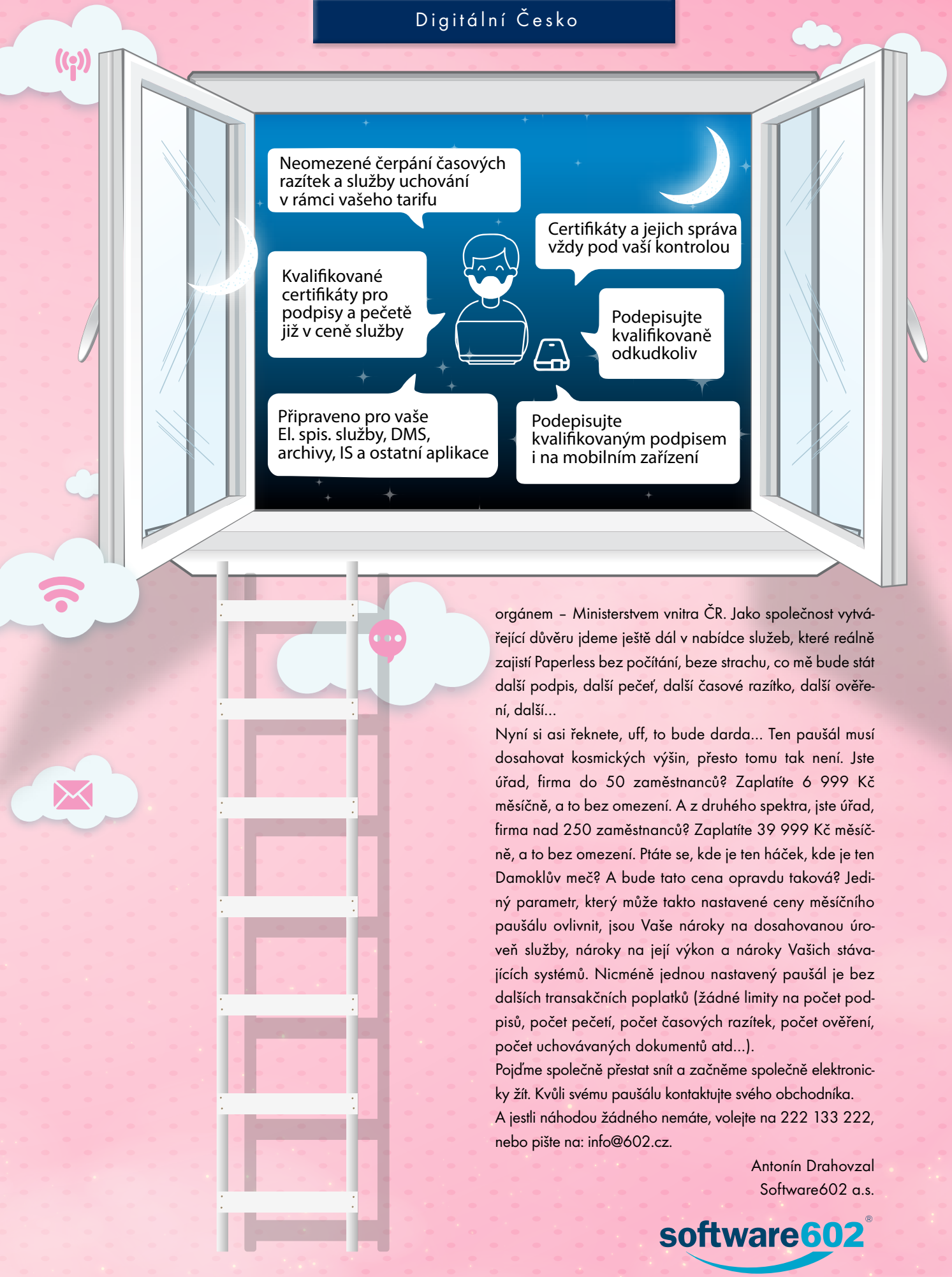
Zkusme na to jít opačně, a to pozitivně:

- legislativně pokryto;
- technicky pokryto;
- archivačně pokryto;
- systémově pokryto.

A teď jen jak to zařídit a nebrat si na to úvěr.

Zkusme ještě maličko snít ... Jeden paušál a v něm máte vše: potřebujete 100 kvalifikovaných podpisů – máte je, potřebujete 10 pečetění – máte je, chcete každý podpis, každou pečeť chránit časovým razítkem – máte je, chcete každý dokument skutečně a nezávisle ověřit bez ohledu na jejich množství – můžete, chcete každý dokument dlouhodobě uchovat, aby byl i za 20 let ověřitelný – máte to. Jeden prsten vládne všem – pardon – jeden paušál vládne všemu.

A nyní je čas přestat snít a vrátit se do reality, protože ta už není jen snem. Software602 doplnila svoji certifikaci na eIDAS služby ověření a uchování elektronických certifikátů o další službu poskytování vzdáleného podepisování a vzdáleného pečetění: služby jsou povoleny dohledovým



orgánem – Ministerstvem vnitra ČR. Jako společnost vytvářející důvěru jdeme ještě dál v nabídce služeb, které reálně zajistí Paperless bez počítání, beze strachu, co mě bude stát další podpis, další pečeť, další časové razítko, další ověření, další...

Nyní si asi řeknete, uff, to bude darda... Ten paušál musí dosahovat kosmických výšin, přesto tomu tak není. Jste úřad, firma do 50 zaměstnanců? Zaplatíte 6 999 Kč měsíčně, a to bez omezení. A z druhého spektra, jste úřad, firma nad 250 zaměstnanců? Zaplatíte 39 999 Kč měsíčně, a to bez omezení. Ptáte se, kde je ten háček, kde je ten Damoklův meč? A bude tato cena opravdu taková? Jediný parametr, který může takto nastavené ceny měsíčního paušálu ovlivnit, jsou Vaše nároky na dosahovanou úroveň služby, nároky na její výkon a nároky Vašich stávajících systémů. Nicméně jednou nastavený paušál je bez dalších transakčních poplatků (žádné limity na počet podpisů, počet pečetí, počet časových razítek, počet ověření, počet uchovávaných dokumentů atd...).

Pojďme společně přestat snít a začněme společně elektronicky žít. Kvůli svému paušálu kontaktujte svého obchodníka.

A jestli náhodou žádného nemáte, volejte na 222 133 222, nebo pište na: info@602.cz.

Antonín Drahovzal
Software602 a.s.

software602®

Co je a co není rozumná elektronizace samosprávy

Slova. Slova. Slova. O tom je nyní elektronizace veřejné správy. Jakoby se doposud tolik věcí dělalo špatně, jakoby se centrální plánování po třiceti letech vrátilo a snažilo se své okolí přesvědčit, že ke každému kroku je třeba plán či strategie, která nemůže být jiná než akční.

Štěstím sektoru samosprávy je, že pozornosti centrálního dohledu i zájmu trochu uniká. Pompa nově připraveného předpisu o právu občana na digitální služby zcela pomíjí obce, města i kraje. Povinnosti plynoucí ze zákona se organizací samosprávy netýkají. Nově připravovaný dohled nad veřejnými zakázkami v oblasti IT je také určen centrálním entitám státní správy. Vodítka a znaky toho, co je vlastně standardem e-governmentu pro obce, města a kraje, chybí.

Katalyzátorem rozvoje byly evropské dotace

Hlavními oblastmi zájmu radnic v oblasti informačních technologií byly v minulých letech portály, bezpečnost přístupů k informačním systémům a agendové informační systémy. Projekty IROP výzev 26, 28 a 10 společně s výzvou MPSV v programu Zaměstnanost pomohly mnohým obcím zásadně zlepšit agendové informační systémy, případě postavit první portálová řešení pro občany. Z dostupných informací vyplývá, že oblast realizace portálů pro občany je na dotace přímo navázána. Jen málo projektů „otevřených úřadů" bylo řešeno čistě z rozpočtu obce.

Podle informací z Ministerstva pro místní rozvoj budou hlavní programy v oblasti informačních technologií mířit na bezpečnost a řešení pro občany. Je tedy zřejmé, že mnohé obce a kraje budou čekat na slibovanou podporu a odsunou investiční projekty na rok 2022, kdy se reálně budou moci podporované projekty realizovat. Přistoupíme-li na to, že evropské dotace jsou jediným hnacím motorem změn v informačních technologiích v obcích a krajích, je nutné zodpovědět otázku, jakým způsobem rozvíjet technologie v dotační proluce mezi rokem 2019 a 2022.

Nová řešení pro rok 2020 – občan a informace a rozhraní

Funkcionalita informačních systémů pro občany se přímo odvíjí od informačních zdrojů (AIS), které má obec k dispozici. Portál občana nebude obsahovat možnost rezervovat si úředníka online, když na straně úřadu není systém, který čas a možnosti úředníka spravuje. Stejně tak není možné občanovi nabídnout elektronickou úhradu poplatku za psa, pokud obec neprovozuje aplikaci správy poplatků. Příprava informací, agendových informačních systémů do rozhraní, přes které si portálová řešení předávají data, je klíčovým (a často opomíjeným) předpokladem úspěšného a rychle zvládnutého projektu. Nepřipravené rozhraní je zcela jasně nejčastějším slabým místem pro implementaci každého úžasného řešení pro občany. Souběžně s rozvahou na připojení agendových informačních systémů je proto třeba připravit komplexní logiku registrace a přihlašování občanů. Z praxe vyplývá, že pokud úřad důkladně nepromyslí, jakým způsobem se občané do portálového řešení budou přihlašovat, jsou tyto úvodní kroky občana do elektronického světa často ty poslední, které občan zkusí.

Přihlašovacích metod je na trhu mnoho a není tak neobvyklé, že se úřad spokojí s jedním způsobem registrace a přihlášení (NIA nebo datové schránky), které celý projekt pošlou do červených čísel, protože o portál klienti ztratí zájem. Je velmi obtížné jednou ztracené klienty dostat k řešení zpět. Příprava pro elektronické služby občanům je tak zvláště důležitá. Na trhu jsou dostupná řešení, která jsou schopna zajistit služby přihlášení i samotného zprostředkování informací z agendových systémů do externích portálů, stejně jako přenos dat z portálu do agendového informačního systému a zpět. Výhodou nasazení takového řešení je možnost následného rychlého napojení portálu a celé řady registračních a přihlašovacích metod, včetně ověřování klienta prostřednictvím základních registrů.

Trend participace a personalizace informací

Trendem posledních let jsou elektronická řešení umožňující participaci občanů na výkonu samosprávy. Webové aplikace na základě participačního mechanismu dovolují

PORTÁLOVÝ BACKOFFICE PROXIO
Inovativní řešení pro portálová řešení obcí

- Všechny současné registrační a autentizační metody
  - Národní identitní autorita
  - Přihlášení prostřednictvím datové schránky
  - MOJEID
  - BANK ID
  - Registrace na přepážkách (včetně ověření občana prostřednictvím ISZR)
- Standardizované rozhraní pro výměnu dat
- Možnost registrace právnických osob
- Všechny agendy jsou provozovány v souladu s požadavky GDPR

občanům navrhovat projekty k realizaci, vybízejí k souná-ležitosti s územím prostřednictvím hlasování o projektech nebo v anketách. Participace, propojení občana s vede-ním obce, nativně patří do portálového řešení, kde má občan svůj účet, jímž s úřadem obce komunikuje. Portálo-vá řešení by proto měla obsahovat vícekanálový přístup k informacím. Ukazuje se, že vyhledávání na stránkách obcí je složité, občan se často neorientuje v zakořeně-ných názvech, které úřad používá (jako jsou názvy odbo-rů či kompetencí). Nejúčinnějším rozcestníkem jsou život-ní situace, které jsou však často zpracovány s právními a velmi složitými texty ze stránek Ministerstva vnitra. Pří-prava rozcestníku, který vede k vyřešení konkrétní životní situace, musí být pečlivá, pro občana/klienta je třeba volit lehce stravitelný jazyk. Na konci každého popisu životní situace musí být řešení: rezervace času úředníka, elektro-nické podání dokumentu nebo přímý odkaz na elektronic-ké zpracování agendy v portálu.

Mnoho měst si v roce 2019 pořídilo portál občana, jehož jedinou funkcionalitou jsou elektronické formuláře. Rozča-rování občanů i správců portálu nad nízkou využitelností takové elektronické služby ukazuje nepromyšlenost i jed-notvárnost přístupů dodavatelů softwarových řešení pro občany. Jako ideální cesta se ukazuje kombinovat úhrado-vé funkcionality (elektronické platby za obecní/městské poplatky) společně s vybudováním vícekanálové a per-sonalizované komunikace občan – úřad. Tento přístup zaručuje využitelnost portálu občana v době udržitelnosti i naplnění indikátorů ze studií proveditelnosti.

Moderní agendové informační systémy

Portálová řešení jsou logickým vyústěním elektroniza-ce samosprávních agend, zpřístupňují občanům slu-žby a data obcí a usnadňují každodenní život lidem, kteří musí komunikovat s úřadem. V souběhu s výstavbou por-tálu občana obce proto musí být elektronizovány agen-dy, které doposud byly v obcích realizovány ručně nebo s podporou kancelářských aplikací. Typickým příkladem může být zvláštní užívání komunikací nebo pozemků obce (zábory) – agenda, ve které se zpracovávají žádos-ti občanů (jako právnických osob) o předzahrádky apod. Moderní agendový systém dovoluje přijmout elektronic-kou žádost, podanou portálem, včetně mapového zákre-su předzahrádky. Obdobných příkladů zjednodušujících občanovi podnikatelský život je celá řada. Informační sys-témy musí být připraveny na to, aby s nimi mohl občan komunikovat. Zrychlí se tak vyřízení žádostí a zpřesní se práce úřadu. Vytipování informačních systémů pro komu-nikaci s portálem a jejich úprava je prvním správným kro-kem pro rozšíření služeb občanům.

Rok 2020 patrně nebude v oblasti informačních technolo-gií v samosprávě přelomovou etapou rozvoje elektronic-kých služeb. Může být však rokem příprav a dobře roz-myšleného rozvoje agendového prostředí. Taková snaha bude v následujícím období zúročena.

Michal Karvánek
Konzultant pro veřejnou správu

MARBES CONSULTING

ZONER Software, a. s.
SVĚŘTE SE DO RUKOU PROFESIONÁLŮ

Společnost ZONER Software, a. s., má více než 25 let zkušeností s vývojem softwaru a poskytováním internetových služeb v oblasti e-commerce. Zoner nabízí celou škálu služeb spojených s provozem a zabezpečením on-line projektů, registrací a správou domén, serverhosting a nejširší nabídku elektronických certifikátů všeho druhu.

Zoner je evropskou společností s hlavním sídlem v Brně a pobočkami na Slovensku, v Maďarsku, Japonsku a USA. Společnost se dělí na čtyři samostatné divize – internetové služby, on-line bezpečnost, fotografický software a vydavatelství.

ZONER PHOTO STUDIO

Program pro zpracování fotografií a fotografické dokumentace **Zoner Photo Studio X** je ústředním produktem divize Software. Využívají ho tisíce firem i veřejných institucí, jejichž uživatelům poskytuje nástroje ke zpracování celého životního cyklu fotografií. Za zajímavých licenčních podmínek nabízí vhodnou alternativu pro širokou skupinu řešení – od bezplatných až po drahé komerční aplikace.

Pro účely zpracování fotodokumentace jsou v programu doplněny **speciální nástroje**, které usnadní uživatelům její rutinní zpracování, ale i nástroje, které jsou specifické pro segment pracovníků ve veřejném sektoru (např. anonymizace obrazu v souvislosti s GDPR, spolupráce programu s katastrálními mapami nebo databází RÚIAN pro poloautomatické popisování fotodokumentace metadaty, nejrůznější grafické anotace apod.). Kromě klasické organizace a ukládání fotografií na lokální disky uživatelů poskytuje Zoner Photo Studio X také týmovou spolupráci prostřednictvím služby **Zoner Photo Cloud**, která je plně integrovaná do prostředí programu. Vedle toho existuje několik zákaznických instalací *on demand* vytvořené speciální fotodatabáze **Zoner Photo Depository**, jakožto součást širšího projektu Zoner DAM. Zoner Photo Cloud nabízí specializované nástroje pro ukládání fotografií a propracovaný systém ukládání fotografií s metadaty.
Kromě zpracování fotografií je v Zoner Photo Studiu X pilotně integrován vícestopý střih videa, což rozšiřuje jeho možnosti právě při zpracování obrazové dokumentace v situacích, kdy série fotografií nahrazuje videozáznam.

ELEKTRONICKÉ CERTIFIKÁTY A SPRÁVA DOMÉN

Bezpečnostní SSL/TLS certifikáty Vás denně chrání před různými kyberhrozbami. Díky nim víte, že je Vaše internetová komunikace chráněna, máte jistotu, kdo Vám píše, kdo vytvořil daný dokument, případně Vás upozorní i na phishing. Nejlepší certifikáty poskytuje jednoznačně **projekt SSLmarket.cz**, který je největším prodejcem těchto certifikátů v Evropě, jak potvrzuje i **ocenění Partner roku 2019** od společnosti DigiCert, největší CA na světě. SSLmarket.cz má v nabídce několik druhů webových certifikátů, tím nejdůvěryhodnějším je EV – rozšířené ověření. V rámci této úrovně je oblíbeným produktem **EV certifikát od GeoTrustu**. Je doporučován pro společnosti a organizace, které kladou požadavky na nejvyšší stupeň důvěryhodnosti a dbají na vysokou úroveň zabezpečení.
SSLmarket.cz se zaměřuje jen na ty nejkvalitnější produkty, proto v jejich nabídce najdete i oblíbené certifikáty Thawte od společnosti DigiCert. Kromě tradičních SSL/TLS certifikátů pro webové servery a služby můžete získat osobní certifikáty pro elektronický podpis (S/MIME), kvalifikované certifikáty splňující požadavky e-IDAS, certifikáty pro podpis dokumentů a certifikáty pro podpis zdrojových kódů aplikací.

Jako pracovníci ve veřejném sektoru jistě oceníte i možnost **zabezpečení domén DNSSECem** (rozšíření systému doménových jmen DNS, které zvyšuje jeho bezpečnost). Registraci a správu zabezpečených domén poskytuje další z projektů ZONER Software, **CZECHIA.COM**. Je prvním registrátorem, který má na svých DNS zabezpečeno 100 % .cz domén technologií DNSSEC.

CZECHIA.COM poskytuje nejširší nabídku doménových jmen k registraci na trhu.

U většiny domén jsou v nabídce i **víceleté registrace**, které jsou výhodnější pro Váš rozpočet. Při registraci domény také automaticky získáváte bonus ve formě HTTPS zabezpečení svého webu s certifikátem Basic DV od DigiCertu, e-mailovou schránku na vlastní doméně zcela zdarma v rámci služby inPage mini a možnost vytvořit si základní webové stránky, fotogalerie nebo e-shop díky službě inPage mini.

SERVERHOSTING A HOSTING

Rychlost načítání webových stránek do značné míry ovlivňuje výkon serveru, na kterém jsou data webu a jeho funkční scripty uloženy a které zabezpečují jeho chod. Existuje několik možností, jak bezproblémový provoz webového projektu zajistit. Od webhostingu, přes pronájem virtuálních serverů až po provoz vlastního zařízení.

Projekt ZonerCloud.cz společnosti ZONER Software, a. s., nabízí nejvýkonnější virtuální servery na trhu zapojené v cloudové infrastruktuře. Jednou z mnoha výhod serverů od ZonerCloud.cz je, že nedochází k žádným latencím a případným výpadkům spojení, protože všechny servery jsou umístěny v ČR. Aby ZONER svým klientům zajistil absolutní komfort a bezchybnost služeb, postavil nové datové centrum v klasifikaci TiER III. Obsahuje ty nejmodernější technologie od nejspolehlivějších dodavatelů na trhu, jako jsou DELL a CISCO. Stavba tohoto moderního datacentra vyšla společnost ZONER Software na desítky milionů Kč. Zoner může svědomitě prohlásit, že je Green providerem, na střeše svého sídla vybudoval vlastní solární elektrárnu o výkonu 60 kWp, která slouží pro napájení datacentra. Veškerou další potřebnou energii dále nakupují od společnosti E.ON jen z obnovitelných zdrojů. Že má ZonerCloud.cz ty nejvýkonnější servery, dokazuje i velké výkonnostní srovnání, ve kterém ZonerCloud.cz porazil přední konkurenty.

ZONER Software, a. s., Vám pomůže i s **hostováním** Vašeho webu. Vybírat můžete z webhostingových variant pro Windows, Linux, WordPress, Drupal, Joomla a další. Výhodou je bezproblémová a intuitivní instalace – stačí jedno kliknutí.

Jejich webhosting běží na nejnovější distribuci Debian ve verzi 10.2 (Buster), webserver je Apache 2.4. Podporujeme http/2 (pro rychlejší načítání šifrovaného obsahu), nejnovější verzi protokolu TLS 1.3 a nejnovější rodinu šifer využívajících eliptické křivky ECDH x25519.

Nedílnou součástí webhostingových profesionálních služeb jsou i e-mailová řešení s trojí ochranou (antispam, antivir, antiphishing), kde např. u nejoblíbenějšího programu Linux Plus máte k dispozici neomezený počet e-mailových schránek a 20 GB prostoru.

Pavlína Malachová
obchodní oddělení internet divize

Zoner Zoner Photo Studio

Automat ePodatelny: pomocník ve světě elektronických podání

Snadná implementace, významná úspora času i práce, automatizace řady rutinních procesů – asi takto může vypadat shrnutí nejvýznamnějších výhod, které s sebou nese komponenta platformy GINIS Elektronická podatelna – Automat (dále jen EPA).

Primárním úkolem podatelny je přijetí došlých dokumentů a jejich přerozdělení k dalšímu zpracování. To vše musí proběhnout bezchybně a pokud možno v co nejkratším čase. V praxi to znamená velké množství rutinně prováděných úkonů při zachování maximální pozornosti. A právě zde nachází EPA své nesporné uplatnění. „Jakmile jsme se dozvěděli o možnosti zavedení prvků automatizovaného zpracování datových zpráv, rozhodli jsme se systém otestovat, vyhodnotit a případně nasadit do ostrého provozu. Prvním krokem bylo vytipování několika druhů podání, která lze automatizovaně vyhodnotit a zpracovat, tedy podání přesně identifikovatelná – např. kombinace odesilatele (ID datové schránky) a opakujícího se textu. Pro tento účel jsme vhodné kandidáty nalezli v podáních došlých od automatu základních registrů, od policie a v dokumentech potřebných pro přepis vozidla (CRW),“ popisuje první kroky nasazení EPA do softwarového prostředí Magistrátu města Pardubic vedoucí oddělení strategie a IT služeb Ing. Jan Czagan.

Nástroj EPA provozuje ČTÚ již od roku 2008 a za tu dobu zpracoval 1 548 658 e-podání.

EPA se na Magistrátu města Pardubic implementovala v září 2019. Do konce roku bylo bezobslužně podáno bezmála 900 dokumentů doručených prostřednictvím ISDS. Kromě významné časové úspory díky automatizaci procesu podání je nesporným kladem i eliminace chybovosti díky strojovému charakteru procesu zpracování i předávání. Čísla jsou to už tak sympatická, ale potenciál EPA sahá mnohem dál. Již teď je jisté, že v Pardubicích nezůstanou u 3 typů podání řešených touto cestou. „Pracovníci podatelny už sami iniciativně vytipovávají druhy elektronických podání vhodné pro EPA. Ve své práci jsou často velmi vytíženi a EPA je reálnou možností, jak jim ulevit,“ doplňuje informaci o aktuálním stavu Jan Czagan.

Obdobné zkušenosti s modulem má Magistrát hlavního města Prahy (MHMP), který jím řeší 4 typy podání. Dvě z nich si metodici spisové služby MHMP po prvotní ukázce zvládli realizovat sami, včetně analýzy a nastavení systému. V současné době chystá MHMP implementovat automatizované zpracování pro další typ e-podání, a to pro e-neschopenky. Nejmasivnější využití nalezneme u Českého telekomunikačního úřad (ČTÚ), konkrétně se jedná o 17 typů elektronických podání. ČTÚ využívá modul EPA i pro přenos podání a dokumentů od mobilních operátorů, právních kanceláří zastupujících podnikatele v elektronických komunikacích a vězeňské služby, se kterými si tímto způsobem standardizoval komunikaci a přenos dokumentů. Nástroj EPA je v ČTÚ v provozu již od roku 2008 a od té doby zpracoval 1 548 658 elektronických podání, v letech s největším vytížením se počet zpracovaných elektronických podání přehoupl i přes dvě stě tisíc za rok.

Lukáš Kos
www.gordic.cz

GORDIC

GORDIC

Digitální služby Portálu občana GINIS

Komunikace s úřadem

Elektronické podání žádostí

Pohodlná platba poplatků

Řešení životních situací

www.digitalnisluzba.cz

NOVELA ZÁKONA O VOJENSKÉM ZPRAVODAJSTVÍ

Původně jsme pod názvem Bezpečná obrana – obranná bezpečnost připravovali seminář, který by se obsáhleji věnoval jak kybernetické bezpečnosti, tak kybernetické obraně (viz odložený seminář). Vzhledem k současným opatřením jsme prozatím jeho konání odsunuli. O náhradním termínu budete včas informováni. Vláda však v těchto dnech nejedná pouze o bodech, které přímo souvisí s koronavirovou pandemií, ale i o řadě dalších důležitých materiálech. Jedním z takových je i Novela zákona o vojenském zpravodajství. Ta byla schválena v pondělí 16. 3. 2020, tedy v den, kdy na programu byl i velice diskutovaný zákon o evidenci skutečných majitelů a den, kdy na tiskovou konferemci po jednání vlády byl vpuštěn pouze omezený počet novinářů. Vzhledem k důležitosti novely a citlivosti některých jejích bodů, jsme se rozhodli shromáždit související názory. Jako první jsme požádali ředitele vojenského zpravodajství Ing. Jana Berouna a poslance PSP ČR, člena podvýboru pro obrannou, kybernetickou a bezpečnostní politiku a strategické koncepce ČR Ondřeje Profanta. Postupně se budeme snažit získávat další, naleznete je na stránkách magazínu Egovernment v sekci KYBEZ.

Komentář k novele zákona o Vojenském zpravodajství

Jan Beroun, ředitel Vojenského zpravodajství

Vláda minulý týden schválila novelu zákona o Vojenském zpravodajství, který má za cíl zohlednit specifika kybernetického prostoru při obraně státu a jeho obyvatel. Jedná se o řešení zadaného úkolu stanoveného vládou vycházející z Národní strategie kybernetické bezpečnosti ČR, které umožní detekovat kybernetické útoky a adekvátně na ně reagovat.

Základem pro zajištění kybernetické bezpečnosti státu je potřeba kybernetickým hrozbám primárně předcházet vzděláváním, prevencí, sdílením znalostí, spoluprací, ale i nastavením jasných pravidel. Naprosto totiž postačí, když před většinou běžných útoků budou systémy dobře zabezpečeny, zálohovány a v podstatě ze strany státních institucí (pokud nebudou přímo ony cílem útoku) nebude třeba žádné větší ingerence. S rostoucí intenzitou možných dopadů či v případě sofistikovaných útoků však role státu musí být významnější, jelikož stát musí garantovat bezpečnost svých občanů v kyberprostoru stejně, jako garantuje jakoukoliv jinou formu bezpečnosti. Stát musí být schopen bránit nejen státní instituce, ale také nemocnice, banky, elektrárny a v důsledku tak i životy a zdraví českých občanů, takže význam tohoto zákona je v této době víc než zřejmý.

Aby vše fungovalo, je potřeba erudovaných lidí s odvahou převzít odpovědnost, ale také jim musí být dány kompetence, důvěra a oprávnění konat. Role Vojenského zpravodajství bude spočívat v reakci na ty úplně nejzávažnější kybernetické hrozby. Cílem návrhu je doplnění daného systému o prvky, které v současné situaci státu chybí, přitom jsou nutné k jeho obraně. To vše v návaznosti na to, aby státní instituce společně se soukromou i akademickou sférou spolupracovaly a snažily se pokrýt celé spektrum možných hrozeb.

Kybernetická obrana na státní úrovni je zcela novým prvkem, i proto tato problematika budí velký zájem. My tento zájem vnímáme jako pozitivní, protože se nám díky němu, myslím, podařilo vytvořit precizované znění návrhu. Z připomínkových míst se nám sešlo na 160 připomínek a ozývali se nám i nestátní aktéři. My jsme společně s ministrem obrany samozřejmě mluvili nejen s připomínkovými místy, ale také s různými organizacemi, spolky i s politickými stranami a jsme připraveni s nimi v diskuzi pokračovat i nadále. Kybernetická obrana České republiky musí být naším společným cílem.

Ve státní sféře byl zákon nejvíce projednáván mimo jiné s Národním úřadem pro kybernetickou a informační bezpečnost, Úřadem pro ochranu osobních údajů či ostatními

zpravodajskými službami. Z politických stran se z logiky věci o novelu zákona ve větší míře zajímá Pirátská strana, i na základě jejich relevantních připomínek a přímých jednáních s jejich zástupci došlo ke zkvalitnění znění zákona. Rozumím obavám ohledně zachování soukromí na internetu, které kolem této novely panují. I proto jsme v této problematice změnili naše obvyklé postupy, a ačkoli jsme zpravodajská služba, snažíme se být co nejvíc otevření a transparentní. Účastníme se diskuzí a akcí v rámci odborné i široké veřejnosti či zveřejňujeme potřebné informace na webových stránkách. Snažíme se toto téma vysvětlovat, jak jen nám to prostředí tajné služby dovolí.

Za účelem odhalení kybernetických útoků bude Vojenské zpravodajství umisťovat do sítí operátorů takzvané nástroje detekce, které budou zachytávat pouze předem definované anomálie, na základě kterých bude možné dále reagovat. Návrh zákona velice jasně vymezuje, k čemu a jakým způsobem je možné tyto nástroje umístit a provozovat. Obsah návrhu zákona je již delší dobu podroben odborné diskuzi a prošel významným vývojem. Návrh byl shledán ústavně konformní a obsahuje dostatek záruk a kontrolních mechanizmů, aby nebylo možné vykročit z mantinelů, které svými ustanoveními nastavil.

Komentář k novele zákona o Vojenském zpravodajství

Ondřej Profant, PSP ČR

V Česku rozlišujeme kybernetickou bezpečnost a kybernetickou obranu. Bezpečnost je „měkká", civilní a zajišťuje ji NÚKIB. Obrannou linii má zajišťovat Vojenské zpravodajství (VZ) spadající pod Ministerstvo obrany. Obranou se rozumí ochrana životů obyvatel, územní celistvosti, principů demokracie a dalších podstatných aspektů našeho života před vnějším napadením. Předpokládá se tedy, že VZ může operovat v zahraničí.

Již v minulém volebním období VZ předložilo návrh, jak svou roli sehrát. Tento návrh byl tvrdě odmítnut. V pozadí probíhající pandemie VZ návrh znovu předložilo a vláda ho schválila 16. 3. 2020. Návrh byl do mezirezortního připomínkového řízení opětovně vložen 12. 2. 2019. Zásadní výhrady vyjádřily Ministerstvo spravedlnosti, Hospodářská komora, ICT Unie, Český telekomunikační úřad nebo Česká advokátní komora. Piráti nabídli svou verzi, kterou zpracovali ve spolupráci s nevládní organizací IuRe.

S VZ jsme o návrhu jednali půl roku. Některé naše připomínky byly zapracovány, ale jiné opět ne. Musíme pochválit definici metadat, která má zajistit sledování pouze provozu, nikoliv obsahu komunikace. Též jsou upřesněny podmínky, za kterých může dojít k omezení lidských práv a svobod tak, aby odpovídaly analogiím.

Největším problémem stále zůstává samotná realizace sběru dat. Návrh hovoří o „nástroji detekce" namísto původně použitého „sonda". Piráti prosazovali, aby už v zákoně bylo jasně stanoveno, že data se sbírají pasivními zařízeními z odbočené sítě (např. pomocí optického splitteru), aby VZ nemohlo pomocí těchto zařízení měnit provoz v síti. To by usnadnilo i fyzickou realizaci daných opatření. Bohužel jsme tu opět svědky principu security through obscurity, kdy naše legislativně-bezpečnostní myšlení výrazně zaostává za technickými poznatky.

Velkou neznámou je také termín „aktivní zásah". Zatímco konvenční armáda nemůže za normálních okolností zasahovat v ulicích, VZ by obdobnou pravomoc dostalo, neboť internet nemá hranice a identifikovat útočníka může být téměř nemožné. Osobně se velmi obávám provokací pod falešnou vlajkou, kdy cizí mocnost vyprovokuje VZ k zásahu a následná eskalace konfliktu se později obrátí proti nám.

Dalším bodem sporu je předpokládaná spolupráce s poskytovateli internetového připojení (operátoři, ale i lokální podnikatelé). Ti by měli mít ze zákona povinnost se zpravodajci spolupracovat a detekční zařízení nechat do „svých kabelů" umístit. Návrh ovšem požaduje mlčenlivost a hrozí také likvidačními pokutami, pokud by soukromý subjekt součinnost odmítl. Složitá je i náhrada případné škody.

Představovali bychom si také mnohem důslednější kontrolu ze strany Poslanecké sněmovny, aby se minimalizovalo riziko zneužití. Zahraniční i naše zkušenosti jasně ukazují, jak moc je to důležité. V konečném důsledku i pro samotnou rozvědku, která tím získává větší důvěryhodnost.

Kybernetickou obranu nesmíme podceňovat. Bylo by naivní se domnívat, že nám nic nehrozí. VZ a další bezpečnostní složky státu samozřejmě musí být k dispozici prostředky a oprávnění k tomu nás dostatečně chránit před stále novými hrozbami. Nesmíme se přitom ale vzdát racionálního přístupu a nástrojů demokratické kontroly.

Sítě SD-WAN jsou v oblibě. Dává smysl na ně přejít? Nepřinese to firmám bezpečnostní riziko?

Softwarově definované sítě WAN (SD-WAN) získávají na oblibě u malých a středních firem i velkých podniků kvůli ekonomickým výhodám a přínosům z hlediska výkonu připojení poboček k centrále a cloudové konektivity. Do technologií SD-WAN investují také poskytovatelé komunikačních služeb jako rozšíření nabídky připojení pro své klienty. Jak firmy, tak poskytovatelé služeb ale musí současně řešit otázky bezpečnosti, které jsou s implementacemi softwarově definovaných WAN spojené. Fortinet Secure SD-WAN přináší úsporu nákladů, zlepšuje běh vzdálených aplikací, zvyšuje bezpečnost a zlepšuje uživatelský komfort.

PROČ PŘEJÍT NA SD-WAN

Vhodně zvolené softwarové řešení SD-WAN představuje inteligentní, bezpečnou a ekonomicky výhodnější náhradu za dřívější způsoby propojení poboček a centrály finančně a provozně náročnou hvězdicovou topologií. I když ceny tradičního připojení pomocí pronajatých okruhů mají podle statistik ČTÚ* sestupnou tendenci, nemohou konkurovat nákladům na prosté připojení k internetu.

SD-WAN dokáže automaticky zvolit optimální kombinaci pevných a mobilních způsobů připojení (4G/5G) s ohledem na stanovené priority aplikací a uživatelů, denní dobu, sazby za připojení a další faktory. Eliminuje navíc vedení internetového a cloudového provozu z poboček přes centrální servery. Umožňuje tedy efektivnější a ekonomičtější provoz síťových aplikací, včetně mul-

** Český telekomunikační úřad, Zpráva o vývoji trhu elektronických komunikací 2012-2017*

timédií a aplikací citlivých na zpoždění, typicky hlasového a videokonferenčního provozu.

Zavádění i průběžnou údržbu u technologií SD-WAN usnadňuje centralizovaná správa a možnost zprovoznění bez fyzické přítomnosti technika. Pomocí SD-WAN je možné bez složitého nastavování propojit nové pobočky či detašovaná pracoviště s ústřední podnikovou sítí metodou „plug-and-play".

Výkon a nenáročná správa je také důvodem, proč v SD-WAN spatřují velký potenciál i poskytovatelé komunikačních služeb. Pro ně představuje jednu z možností poskytování síťové konektivity širokému spektru klientů, kteří očekávají výkon WAN odpovídající garantovaným parametrům svých aplikací, včetně cloudových, usilují o snížení nákladů na připojení a požadují vysokou míru bezpečnosti.

PŘÍMÁ KONEKTIVITA VYŽADUJE NOVÝ PŘÍSTUP K ZABEZPEČENÍ

Vedle řady nesporných výhod s sebou využití SD-WAN nese i jistá bezpečnostní rizika. SD-WAN může obcházet podnikové datové centrum či centrální síťovou infrastrukturu a poskytovat přímé připojení k internetu. To znamená, že příchozí a odchozí komunikace poboček ztrácí výhody podnikových firewallů, jednotného řízení a univerzálně platných bezpečnostních pravidel. Typické architektury SD-WAN rovněž rozšiřují prostor pro kybernetické útoky, protože zvyšují počet síťových zařízení, která si útočníci mohou zvolit za cíl, a navíc postrádají pokročilé bezpečnostní funkce.

JAK VYBRAT BEZPEČNÉ SD-WAN ŘEŠENÍ

Se stoupajícím zájmem o SD-WAN a rozšiřující se nabídkou si poskytovatelé a podniky začínají rychle uvědomovat, že ne všechna řešení SD-WAN nabízejí srovnatelné možnosti. Má-li být řešení flexibilní, snadno přizpůsobitelné a především bezpečné, aby dokázalo efektivně podporovat a chránit datový provoz cloudových aplikací, internetu věcí, hlasové a video komunikace apod., vyžaduje úzkou integraci funkcionalit WAN a LAN, podporu vysokokapacitního připojení VPN a integrované zabezpečení, které lze propojit s lokálními i centrálními bezpečnostními řešeními.

V obou dosavadních ročnících nezávislých srovnávacích testů SD-WAN zaměřených na snadnost správy, náklady, výkon a bezpečnost, které pravidelně provádějí světově uznávané zkušební laboratoře NSS Labs, získalo řešení Secure SD-WAN společnosti Fortinet jako jedno z mála nejvyšší hodnocení „doporučené". Firewall nové generace FortiGate, který je nedílnou součástí řešení Fortinet Secure SD-WAN, byl nedávno analytickou společností Gartner jmenován lídrem magického kvadrantu pro síťové firewally pro rok 2019. Kvality řešení od Fortinet potvrzuje i obdržení nejvyššího ohodnocení v kategorii „WAN citlivé na zabezpečení" a umístění v nejlepší třetině všech zbývajících WAN Edge parametrů ve výzkumné zprávě „Kritické možnosti WAN Edge infrastruktury". Tu publikoval Gartner v listopadu 2019 a doporučuje v ní, aby uživatelé považovali soubor kritických schopností za jedny z nejdůležitějších kritérií pro rozhodnutí o pořízení WAN Edge řešení.

Více informací naleznete na www.fortinet.com.

FORTINET

Konsolidujte, automatizujte, jděte do cloudu!

Dlouhý time-to-market pro nové aplikace. Složitá infrastruktura. Vysoké provozní náklady. Chybějící prvky zajišťující aplikační bezpečnost a ochranu proti DDoS útokům. Nízká nebo žádná úroveň automatizace. Jsou Vám tato témata blízká? Pojďte se podívat na to, jak se na tyto oblasti dívá F5 a jak Vám může pomoci na cestě k digitalizaci.

3 VÝZVY PRO MODERNÍ ORGANIZACI

Uživatelská zkušenost a bezpečnost.

Základním předpokladem je vytvořit uživatelsky přívětivou aplikaci a zároveň musí škálovat podle potřeby. Každá moderní služba musí být dostupná na webu a jako mobilní aplikace. Musí být také bezpečná, aby nedošlo k úniku citlivých dat, což je kritické v oblasti portálů státní správy.

Rychlost, agilita.

Celý svět IT směřuje k digitalizaci. Neustále vznikají potřeby vyvinout nové aplikace, díky nimž bude organizace úspěšnější. V soukromé sféře se to jeví jako samozřejmost, ale ve státním aparátu jde o občany a politické body. Většina organizací dnes využívá monolitický typ aplikací založený na aplikačním vývoji typu „waterfall" trvajícím až 1 rok. Nové služby je ale potřeba spustit do několika týdnů. Moderní aplikace jsou postaveny na mikroslužbách. Pro jejich provozování musí ale organizace přijmout kulturu Dev-Ops, ve které jsou vývojové, bezpečnostní a infrastrukturněprovozní týmy úzce propojené. To umožňuje mnohem rychlejší vývoj a spuštění nového kódu.

Vysoké náklady.

Organizace implementující Dev-Ops optimalizují také náklady, protože vývoj trvá kratší dobu a příprava aplikačních služeb je jednodušší. Každá aplikace, aby korektně fungovala, potřebuje aplikační služby. Dnes je běžné, že části aplikačních služeb jsou zajišťovány různými dodavateli, což zvyšuje investiční i provozní náklady a limituje možnosti automatizace. Navíc potřebujete mít specialisty na každou z těchto technologií.

3 VÝZVY = 3 CHYBY

Zmíněné výzvy poukazují na 3 klíčové chyby, které organizace dnes dělají.

Vendor lock-in.

Jedna z těchto chyb se vrací do časů mainframů a týká se infrastrukturního „lock-inu" nebo-li zamknutí se na konkrétní cloudovou infrastrukturu. To ale omezuje přenositelnost aplikací mezi cloudy. Každá aplikace vyžaduje zmíněné aplikační služby, bez ohledu na to, kde je umístěná. Poskytovatelé cloudové infrastruktury nabízejí aplikační služby, ale s omezenou a proprietární funkcionalitou. Pokud se zákazník rozhodne přejít např. z AWS do jiného cloudu později nebo rozšířit stávající privátní VMware prostředí o Azure, infrastrukturní „odemknutí" je velkou výzvou a portabilita služeb významně omezená.

Bezpečnost aplikací až na posledním místě.

Druhá překážka souvisí se zabezpečením aplikací a s konfigurací sítí. Pokud se v organizaci vyvíjí nová aplikace, vývojáři většinou na její zabezpečení nemyslí, jelikož prioritou je dodat funkcionalitu. Na druhou stranu týmům IT bezpečnosti nejde o rychlost, ale o zabezpečení a spolehlivost sítě. Je tedy potřeba integrovat vývojové, bezpečnostní a síťové týmy a zapojit bezpečnost do procesu už od počáteční fáze definování požadavků.

Příliš mnoho management „toolů".

Třetí chyba se týká množství nástrojů pro správu a monitoring používaných v organizaci. Různé týmy používají různé nástroje k plnění svých funkcí a povinností, navíc každý dodavatel má svoje API pro integraci, což vede ke složitosti a vyšším nákladům. A je to nepřítel obchodní flexibility.

MONOLITICKÁ ARCHITEKTURA VS. MIKROSLUŽBY

Pojďme se podívat na možnosti architektury systémů aplikací. V tradiční monolitické architektuře potřebujeme webový server, aplikační server a reverzní proxy. Mikroslužby/kontejnery jsou postavené na Ingress Controlleru, reverzní proxy a Service Mesh (nástroj pro vzájemnou komunikaci mezi mikroslužbami).

Jednou z věcí, které mají ale všechny aplikace společné, jsou **aplikační služby v datové cestě od uživatele k aplikaci**, služby, jejichž cílem je poskytovat uživatelům skvělou uživatelskou zkušenost a aplikacím potřebnou ochranu. Tento řetězec služeb zahrnuje L4 a L7 loadbalancing, aplikační bezpečnost, API gateway, ochranu proti DDoS útokům, DNS, případně Content Delivery Network (CDN) pro rychlejší doručování webového obsahu uživateli.

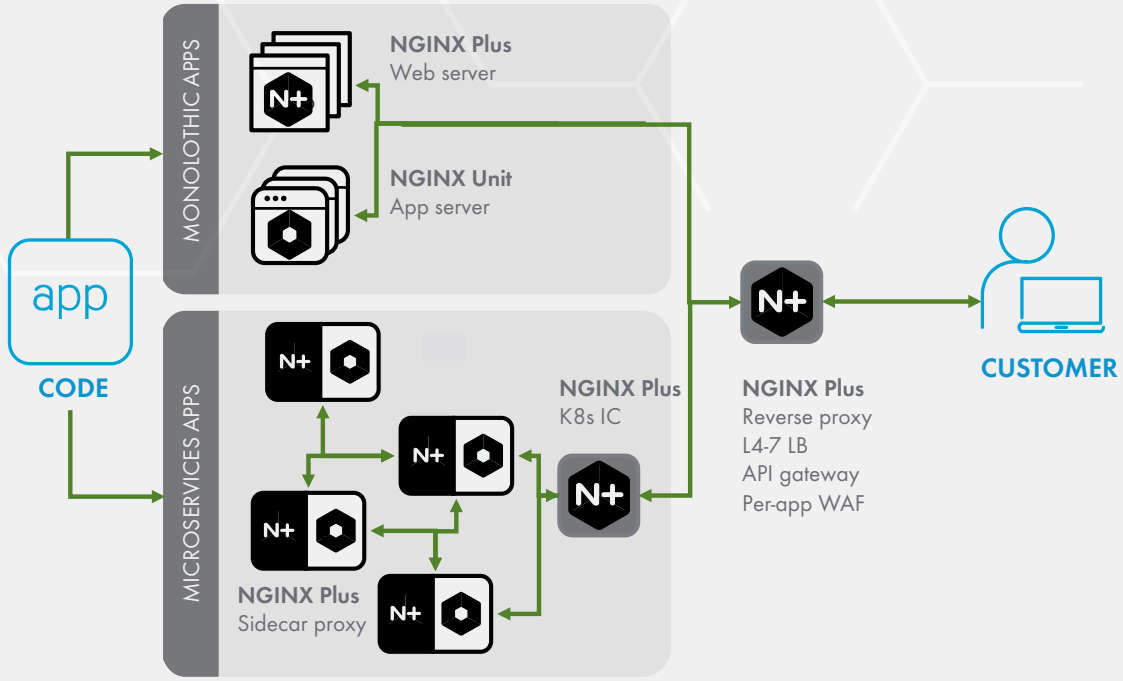
Dnes tato řešení pocházejí od různých dodavatelů a jsou pořizována a provozována různými týmy v organizaci – týmem síťového provozu, vývojáři, architekty, Dev-Ops nebo jsou poskytována jako služba 3. strany (např. DDoS). Každé z těch „silo" řešení také přidává latenci, která se pohybuje v řádu až stovek milisekund a navíc znamená potenciální „point-of-failure".

JAK V TOM VŠEM MŮŽE POMOCI F5 A NGINX?

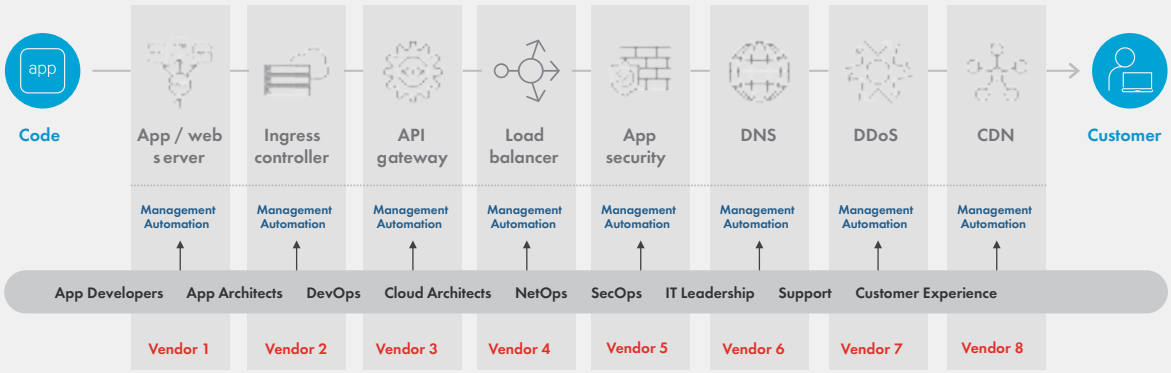
Tento přístup s sebou nese spoustu komplexity. Vize, kterou mají F5 a NGINX dohromady, je konsolidace aplikačních služeb s cílem snížit složitost a náklady, zkrátit čas uvedení nových služeb na trh a ve finále zjednodušit organizacím život.

F5 Networks s produktecm BIG-IP je známý jako lídr v oblasti:

- **Loadbalancingu, včetně terminace TLS/SSL** (Application Deliver Controller – ADC);
- **bezpečnosti webových aplikací** (Web Aplikační Firewall – WAF).



Monolitická vs. architektura mikroslužeb na příkladu řešení NGINX Plus a Kubernetes Ingress Controlleru (K8s IC) a Service Mesh (Sidecar proxy)



„Silo" aplikační služby na cestě od aplikačního kódu k zákazníkovi

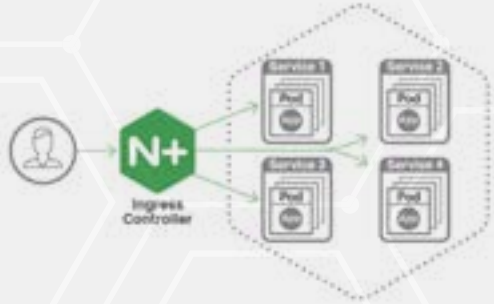
Kromě toho na jednom fyzickém nebo virtuálním zařízení BIG-IP jsou dostupné tyto aplikační služby:

- **DNS** nebo **Global Service Loadbalancing** (loadbalancing mezi geo lokacemi);
- **data-centrový firewall**;
- **L3/L4 DDoS** ochrana proti volumetrickým útokům;
- **L7 DDoS** proti aplikačním DoS útokům, včetně mitigace zlých BOTů.

Služby DNS a anti-DDoS lze také konzumovat z cloudu, který umožňuje lépe se vypořádat s provozními špičkami nebo velkými volumetrickými útoky zahlcujícími uplink.

NGINX technologie vždy byla první volbou pro vývojáře. V Dev-Ops komunitě patřil NGINX k hlavním F5 konkurentům jako jednoduchý softwarový loadbalancer. Dnes je součástí rodiny F5 a s produktem **NGINX Plus** skvěle doplňuje:

- **NGINX Ingress Controller pro Kubernetes**, což je nejrozšířenější orchestrační nástroj pro kontejnery v architektuře mikroslužeb. NGINX Ingress Controller řeší loadbalancing, terminaci TLS/SSL, session persistenci apod. u aplikací nasazených v kontejnerech; Ingress Controller balancující provoz na vstupu do kontejnerového prostředí



Ingress Controller balancující provoz na vstupu do kontejnerového prostředí

- **řešení API Management a API Gateway**, kdy moderní aplikace postavené na kontejnerech generují velké množství API volání. Tuto komunikaci je potřeba řídit, zabezpečit a monitorovat. Řešení na bázi NGINX Open Source je dnes nejrozšířenější API Gateway na světě, využívají ho globálně miliony webových stránek. Na základě toho vznikl enterprise-grade produkt pro zákazníky provozující kritické služby;
- **web server** pro distribuci statického obsahu. Využívá o 90% méně paměti než jiné webové servery a jeho komunitní Open Source verze je celosvětově nejpoužívanější web server (400 milionů webových stránek!);
- **Content Cache pro CDN** pro dynamický i statický obsah. NGINX cache používají největší globální CDN.

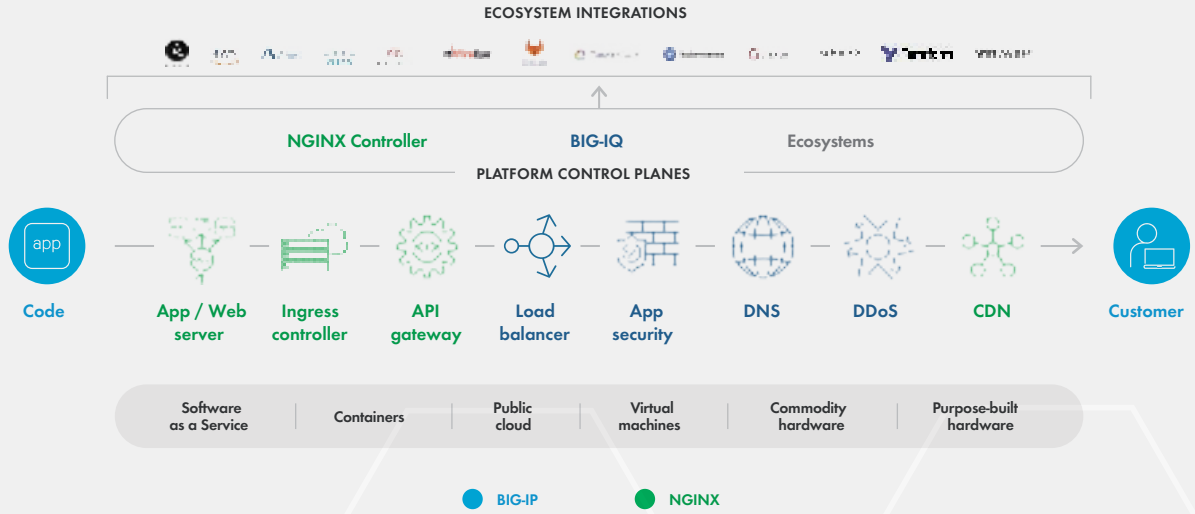
Vítězné skóre 8:2? Konsolidované řešení F5 a NGINX Vám tak umožní 8 různých technologií aplikačních služeb snížit na pouhé 2, což znamená mnohem jednodušší způsob správy ekosystému aplikací, nižší náklady a větší agilitu. Naše finální vize je snížit počet platforem na cestě od aplikačního kódu k zákazníkovi, které lze integrovat s různými nástroji orchestrace, „enterprise-grade" nebo Open Source, počínaje Cisco ACI, Ansible, Openshift apod.

MULTI-CLOUD A VÝZVY

87% firem již má „multi-cloud" architekturu, tj. on-prem prostředí zákazníci kombinují s nasazením aplikací ve veřejném cloudu – většinou Azure nebo AWS, nebo SaaS.

V cloudu pozor na data a nedělejte z pohledu bezpečnosti kompromisy! Poskytovatel cloudu poskytuje dostupnost a bezpečnost cloudové infrastruktury. Zákazník si ručí za bezpečnost aplikací a jejích citlivých dat, za ochranu proti DoS/DDoS útokům, zabezpečení API atd.

Konzistence znamená portabilitu. V cloudu je aplikace potřeba je mít zabezpečené ideálně stejnými technologie-



Konsolidace aplikačních služeb a nástrojů pomocí F5 a NGINX

mi jako v on-premu. Stejný rozsah funkcí aplikačních služeb „doma" i v cloudu umožní také zajistit flexibilní portabilitu aplikací mezi cloudy a eliminaci vendor lock-inu, protože ve všech prostředích stavíte aplikace identicky.

AUTOMATIZACE

Multi-Cloud je jeden z nástrojů digitální transformace. Být efektivní ve správě multi-cloud architektury vyžaduje nasazení automatizace. Pokud nasazuji, konfiguruji a spravuji aplikační služby pomocí API volání a cloudových templatů, mohu tak činit identickým způsobem ve všech prostředích. To mě činí nezávislým a efektivním.

F5 dává zákazníkům k **dispozici „F5 Automation Toolchain",** což je sada automatizačních nástrojů, které umožňují rychlejší a snadnější nasazení a konfiguraci aplikačních služeb F5 pomocí jednoduchých deklarativních rozhraní. Výhodou deklarativního přístupu je, že nepotřebujete být expert na F5, stačí si najít vhodný template na clouddocs.f5.com nebo githubu a v syntaxi jen změnit parametry ve volání. Toolchain navíc umožňuje vývojářům integrovat aplikační služby od F5 do svých CI/CD pipeline (metodika kontinuálního vývoje). A od teď už vývojáři budou na bezpečnost aplikací myslet od počátku bez dopadu na harmonogram spuštění nové služby!
S F5 a NGINX Plus snížíte počet použitých nástrojů a náklady na provozování webových serverů, loadbalancerů, ingress controllerů, API GW, WAF. Zamezíte také vendor-lockinu v multi-cloud prostředí a podstatně zlepšíte spolupráci ve své organizaci.

KDO JE F5

F5 je lídr v oblasti aplikačních služeb. Řešení F5 pro svoje kritické aplikace využívá 25 000 organizací po celém světě. V ČR se na F5 spoléhají státní instituce a polostátní firmy provozující KII státu, kraje, 8 z 9 největších bank, velké komerční firmy, největší čeští operátoři atd.

CO JE NGINX

NGNIX je jedním z dosud největších a nejúspěšnějších SW projektů. Má velkou Open Source komunitu a za poslední desetiletí se stal velmi úspěšným. Tak úspěšný, že na NGINX softwaru dnes běží 400M webových serverů a jako základní kámen ho využívají největší světové CDN.

NEBOJTE SE ZMĚNY

Z diskusí se zákazníky víme, že někteří již začali cestu k digitalizaci, softwaru, Dev-Ops a automatizovanému způsobu práce. Doporučujeme zákazníkům nasazovat řešení F5 a NGINX, které jim může s takovou transformací pomoci. Umožní to zlepšit aktuální výkon aplikací a povýšit aplikace na vyšší úroveň.

Filip Kolář, F5 Networks ČR, f.kolar@f5.com

Obsáhlejší verzi článku naleznete na https://www.egovernment.cz/inpage/f5-b nebo prostřednictvím odkazu na QR codu.

BEZPEČNÁ PRÁCE MIMO KANCELÁŘ NEJEN VE VEŘEJNÉ SPRÁVĚ

Společnost ICZ jako dlouholetý dodavatel síťových, komunikačních a bezpečnostních technologií zajišťuje kompletní životní cyklus řešení od návrhu, přes implementaci a konfiguraci, až po následnou správu. Velký důraz klademe na architekturu vytvářenou na míru potřebám zákazníka. Naše řešení využívá řada významných podniků a institucí v celé České republice. Pracovníci ICZ mají nejvyšší stupně certifikací a společnost ICZ jako celek dosahuje nejvyšších úrovní partnerství s výrobci. Kombinace těchto skutečností prokazuje vysokou odbornost, díky které máme za sebou celou řadu úspěšně realizovaných projektů a spokojených zákazníků.

PRACUJTE BEZPEČNĚ A ODKUDKOLI

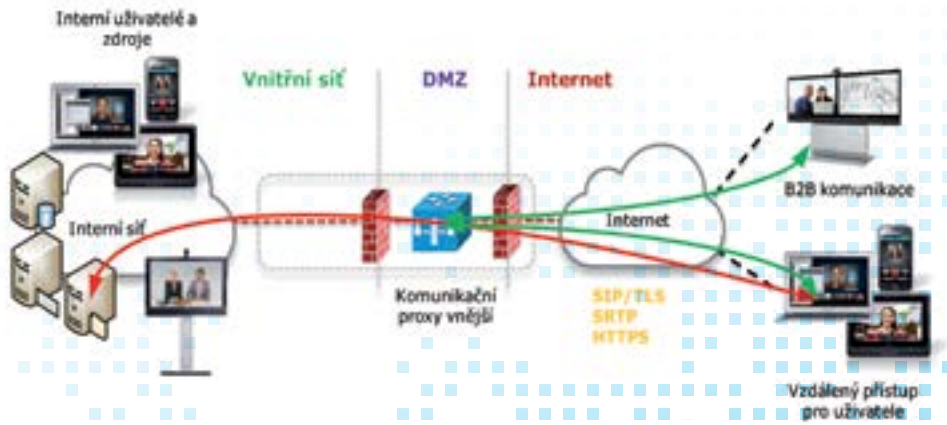
Již delší dobu se ve firemním prostředí skloňují pojmy bezpečnost, kooperace, BYOD (Bring your own device). V posledních týdnech se do popředí dostal pojem home office, který se z vyhledávaného benefitu stal nutnou formou práce. Práce mimo kancelář má však velké nároky na technologie a firemní infrastrukturu. Velkou roli nyní hrají nástroje pro spolupráci na dálku. Komplexnost těchto nástrojů umožňuje vybrat správný způsob komunikace pro konkrétní situaci. Výsledkem je nejen efektivní sdílení informací a značná úspora času, ale v současné době také možnost udržet společnosti a úřady v chodu. Specifikem těchto nástrojů je jejich dostupnost kdykoliv a kdekoliv na všech běžně dostupných pevných i mobilních platformách.

Hlavní funkce:

- sdílení obsahu (dokumentů, prezentací, pracovního prostředí);
- nástroje pro vzájemnou spolupráci nad sdíleným obsahem;
- podpora komunikace všemi dostupnými kanály;
- vlastní podniková řešení i spolupráce v cloudu.

Je důležité si uvědomit, co vzdálený přístup přináší z pohledu bezpečnosti a nároků na infrastrukturu. Zabezpečeným přístupem k firemním zdrojům tento proces teprve začíná. Je vhodné přistoupit k řešení na základě bezpečnostního modelu „nulové důvěry" (Zero Trust). Tedy takový přístup, kdy se na vše v síti pohlíží jako na potenciální riziko. Což neznamená, že se nikdo nedostane k informacím, ale naopak je nutné vědět, kdo, kdy a jak se v síti pohyboval a ke kterým zdrojům přistoupil. Síť, informační systémy a aplikace by měly být chráněny na více úrovních a uživatel by ke své identifikaci měl využít více faktorů.

Využitím tohoto modelu roste bezpečnost v síti a také možnosti využití různých zařízení, které nemá interní IT oddělení pod plnou kontrolou. Ať už jde o zařízení ve vlastnictví uživatelů – mobilní telefony, notebooky nebo domácí počítače, nebo o firemní zařízení, která nelze před zneužitím fyzicky ochránit. Výsledkem je bezpečnější síť a uživatelé, kteří se mohou bez problematických omezení dostat k datům, která potřebují pro svou práci.
Neměli bychom ale rezignovat na bezpečný přístup do firemní sítě z internetu, VPN, neboť šifrovaná spojení obecně jsou nutností. Je důležité si uvědomit, jak bude samotná komunikace probíhat. V případě, že je uživatel připo-



jen šifrovaným spojením a dle doporučení, veškerý jeho provoz směřujeme do sítě společnosti. Jsme schopni jeho komunikaci chránit a monitorovat. V případě komunikace uživatele mimo naši síť ale bude naše konektivita zatížena dvojnásobně. Tento stav většinou nepůsobí problémy v běžném provozu, ale při přesunu významného množství uživatelů mimo počítačové sítě společnosti může nevhodné nastavení bezpečnostních politik způsobit zahlcení linek, tudíž omezenou dostupnost nebo úplnou nedostupnost firemních zdrojů.

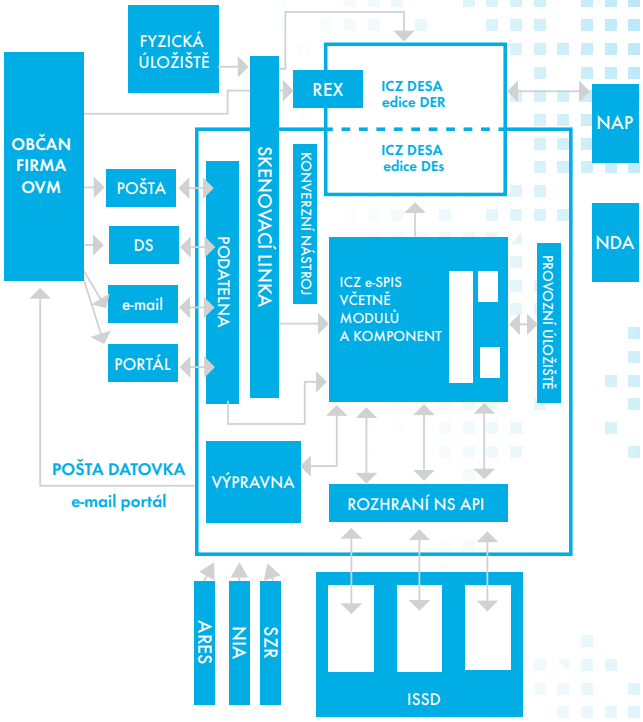
Možnosti vzdálené komunikace a kooperace nám dávají obrovské výhody a při splnění nutných předpokladů v oblasti technologické připravenosti sítě z pohledu výkonu, bezpečnosti a architektury jsou schopny šetřit čas zaměstnanců. Nasazení těchto technologií je však nutné řešit architektonicky správně.

ELEKTRONIZACE VEŘEJNÉ SPRÁVY JE NYNÍ POTŘEBA VÍC NEŽ KDY DŘÍV

V současné době se také ukazuje, že potřeba výraznější digitalizace a elektronizace veřejné správy není jen otázkou zrychlení a modernizace komunikace mezi orgány veřejné moci a subjekty v podobě fyzických a právnických osob, ale také pro umožnění „bezkontaktní" formy komunikace, která může v krizových situacích pomoci k zajištění plynulého chodu veřejné správy. Zavedení elektronizace i do oblasti spisových služeb se tak ukazuje jako správný směr, díky kterému je možné ve velkém rozsahu komunikovat vzdáleně. Dalším vhodným krokem je provozování informačních systémů spisových služeb a úložišť digitálních dokumentů ve formě webových aplikací. Ty totiž umožňují snadný přístup odkudkoli, například i při práci v režimu home office, nebo s ohledem na aktuální stav také z domácí karantény.

Komplexní řešení skupiny ICZ, a.s., v oblasti správy dokumentů přináší velké množství benefitů, a to jak z pohledu samotných funkčních přínosů, tak i z pohledu ochranných prvků pro potenciální uživatele.

Systémy elektronické spisové služby spolu se systémem datových schránek a e-mailovými službami poskytují možnost elektronického zpracování velkého množství agend. Úložiště elektronických dokumentů pak umožňují nejen jejich dlouhodobé ukládání, ale také digitalizaci analogových dokumentů pro účely jejich zapůjčení bez nutnosti osobní přítomnosti žadatele a snížení ekonomické zátěže vytváření a odesílání listinných kopií.



V oblasti funkčních přínosů řešení ICZ můžeme zmínit moderní a designovaný vzhled aplikačních komponent, dále pak intuitivní uživatelské prostředí. Celý koncept aplikačního řešení je navíc postaven v souladu s dlouhodobými zkušenostmi našeho realizačního a vývojového týmu. I při využití širokého spektra nadstavbových modulů, komponent a funkcionalit tvořených na míru pro konkrétní specifické potřeby podniku lze systém vystavět tak, aby byla uživatelům umožněna co nejvyšší míra elektronizace a nezávislosti na hardwarové struktuře společnosti. Celá koncepce je postavena na principech otevřenosti a adaptovatelnosti vůči okolním nebo navazujícím ISSD (Informační systém spravující dokumenty). Pro využití vybraných funkcí tedy není třeba nahrazovat okolní systémy nebo jeho části, ale dle plného souladu s NSESSS (Národní standard pro elektronické systémy spisové služby) lze předmětné řešení lehce adaptovat a využívat.

Kolektiv autorů ICZ

Cisco nabízí pomoc v době šíření koronaviru

Obtížné období, které s sebou přináší šíření onemocnění COVID-19, nám ukazuje, že v první linii nestojí jen zdravotníci, policisté a další nepostradatelné profese, ale také představitelé veřejné správy. Odpovědní činitelé proto musí právě nyní reagovat rychle a přijímat efektivní opatření, která pomohou ochránit občany i ekonomiku.

Aby toho mohli dosáhnout, musí zajistit zachování plné provozuschopnosti svých úřadů, zvlášť když je nyní logická snaha o minimalizaci osobního kontaktu. To ale není snadný úkol ve chvíli, kdy je potřeba realizovat okamžité schůzky a přijímat na jejich základě rozhodnutí. K tomuto účelu se jako ideální jeví využití technologií pro vzdálenou komunikaci a spolupráci. Ty umožní okamžité uspořádání schůzky se všemi výhodami osobního setkání, ale bez rizika šíření onemocnění. Důležité složky řízení tak neriskují, že budou vyřazeny z provozu.

Videokonference zajišťují lepší koordinaci veřejné správy

Aktuálně roste poptávka po těchto řešeních napříč průmyslovými sektory a ani ten veřejný není výjimkou. Před nynější krizí již některé úřady tyto technologie využívaly, ale většina s nimi ještě zkušenost nemá. Proto pro ně nyní může být náročnější rychle vybrat správné řešení a zapojit ho do běžného fungování úřadu – tedy osvojit si ovládání technologie i principy vzdálené komunikace. Společnost Cisco proto přišla s nabídkou poskytnout zdarma své řešení pro vzdálenou komunikaci a spolupráci Webex.

Jako jedna z prvních využila tuto nabídku vláda ČR a vybraná ministerstva. Ve svém příspěvku na sociální síti o tom informoval zmocněnec vlády pro oblast IT a digitalizaci Vladimír Dzurilla: *„Pár hodin po tom, co nám Cisco nabídlo videokonference zdarma, jsme zavezli veškeré vybavení na jednotlivá ministerstva a záhy vše připravili k tomu, aby bylo možné první online zasedání vlády. Doladili jsme i tiskové konference, kde se novináři připojují a online pokládají dotazy. Dnes, po 4 dnech od nasazení, to vypadá jako rutina."*

Řešení Cisco Webex usnadní práci nejen zástupcům města, kraje a státu nebo zřizovaných organizací, případně krizového štábu. Využít ho mohou i složky IZS, školy nebo zdravotnická zařízení. Kromě organizování virtuálních schůzek lze Cisco Webex využít i k operativní komunikaci, jednání zastupitelstev, propojení pacientů s jejich blízkými či lékaři nebo ke vzdálené výuce ve virtuálních třídách. Vše bez potřeby cestování, osobního setkávání a z toho pramenícího zvýšeného zdravotního

Vláda České republiky využívá řešení Cisco pro zasedání, komunikaci a koordinaci aktivit (foto: LinkedIn V. Dzurilly).

Aplikace Webex Meetings má přehledné rozhraní, takže účast na videokonferenci nevyžaduje zdlouhavé proškolení účastníků (foto: Cisco)

rizika. Nezáleží na tom, kde se účastníci schůzky nacházejí, pro její realizaci stačí jakékoliv zařízení připojené k internetu (notebook, mobil, tablet). To je přesně to, co v těchto podmínkách veřejní činitelé potřebují.

Podle nabídky zveřejněné společností Cisco mohou Webex zdarma využít i jednotlivci. Stačí se registrovat na https://cart.webex.com/sign-up. K získání licence pro celý samosprávní orgán – kraj, město a podobně – je ideální kontaktovat společnost Cisco na e-mailu webex.verejnasprava@cisco.com. Odborníci společnosti pomohou s generováním licence a poskytnou potřebnou podporu při instalaci a další rady.

Cisco Webex umožňuje:

- organizovat videohovory až s 200 účastníky;
- mít neomezený počet virtuálních setkání;
- ukládat dokumenty v cloudu;
- nahrávat videohovory;
- video s vysokým rozlišením (HD);
- sdílet obrazovky či integrovat kalendář;
- sdílet soubory a spolupracovat na nich v reálném čase;
- využívat časově neomezené videohovory.

Bezpečnostní řešení ochrání data úřadů i občanů

Dalším očekávaným důsledkem současné situace je nárůst kybernetických hrozeb. Oslabené prostředí je totiž ideální příležitostí pro útočníky. Aby fungování veřejné správy nenarušily útoky na IT infrastrukturu, je potřeba věnovat se také jejímu zabezpečení. Zvláště když mnoho lidí nepracuje z kanceláří, kde by byli připojeni do zabezpečené sítě. Cisco proto v rámci pomoci poskytuje také bezplatné licence u produktů pro zajištění kybernetické bezpečnosti. Její nabídka obsahuje:

- **Cisco Umbrella** je cloudová bezpečnostní platforma, která poskytuje první linii obrany proti hrozbám na internetu, ať už jsou uživatelé kdekoli;
- **Duo Security** umožňuje organizacím ověřovat totožnost uživatelů před samotným přístupem k aplikacím;
- **Cisco AnyConnect Secure Mobility Client** umožňuje lidem pracovat odkudkoli na jakýchkoliv zařízeních a mít přitom bezpečný přístup k datům.

-red–

Více informací o těchto bezpečnostních řešeních a možnosti jejich pořízení zdarma najdete na www.cs.co/61831QBOD.

OCHRANA PROTI KYBERÚTOKŮM: KLÍČOVÝ JE NOVÝ POHLED NA ZABEZPEČENÍ

Rostoucí trendy v mobilitě a cloudu učinily z koncových zařízení nová místa kybernetických útoků. Ty obchází tradiční ochranu a bezpečnostní týmy často nedokáží dostatečně rychle reagovat. Provozy informačních systémů řady institucí tak byly i v České republice v posledních letech a měsících ochromeny počítačovým kryptovirem. Přitom existují sofistikovaná řešení, která dokáží podobným útokům předcházet.

Tým globální technologické společnosti VMware má bohaté zkušenosti při pomoci svým klientům s obnovou po útoku a ochranou proti kybernákazám. VMware nabízí pro ochranu sítě dvě základní techniky. První je antivir nové generace VMware Carbon Black s účinnosti 99,78 %. Druhým klíčovým nástrojem je segmentace a virtualizace síťové infrastruktury pro karanténu nakažených systémů a možnost obnovy produkčních systémů.

Útoky v dnešní době většinou vedou přes uživatelskou stanici do vnitřní sítě a VMware Carbon Black právě na toto myslí. Pomáhá zákazníkům s komplexním zabezpečením koncových bodů a pracovních zátěží a pokročilou bezpečnostní analýzou na ochranu proti sofistikovaným kybernetickým útokům a ke zkrácení reakční doby. Služba VMware Carbon Black aplikuje analýzu big data ve všech koncových bodech, aby předpovídala a tím poskytovala ochranu před současnými, budoucími i neznámými útoky.

Nejviditelnějším příkladem jsou nemocnice

Zdravotnické organizace jsou stále více cílem kybernetických útoků, zejména kvůli množství osobních údajů, které vlastní. Zpravidla jsou i tím typem zařízení, kde jsou kybernetické útoky nejvíce vidět a mohou mít i největší dopad. Příkladem jsou nejen útoky s celosvětovým dopadem, jako WannaCry a NotPetya ransomware útoky z roku 2017, ale i ty lokální z nedávné doby. Před pár měsíci byl v České republice velmi sledovaný kybernetický útok zaměřený na nemocnici v Benešově, velmi čerstvým případem je pak incident z doby vypuknutí koronavirové epidemie, kdy hackeři zaútočili na počítačovou síť brněnské fakultní nemocnice v Bohunicích.

Kybernetičtí útočníci mohou získat přístup, ukrást a prodat informace o pacientovi na „dark webech". Kromě toho umí vypnout či omezit přístup nemocnic ke klíčovým systémům a k záznamům o pacientech, což prakticky znemožní efektivní péči o pacienty. Se zvýšeným používáním lékařských zařízení v rámci internetu věcí jsou možnosti napadení celých systémů stále větší. Problému nepomáhá ani nedostatek IT pracovníků zodpovědných za kyberbezpečnost, natož stagnující rozpočet na zabezpečení v tomto odvětví.

Zajímavé údaje o tomto segmentu přináší loňská zpráva o stavu kybernetické bezpečnosti ve zdravotnictví, která vznikla pod hlavičkou VMware Carbon Black a spolupracovali na ní přední odborníci na bezpečnostní technologie. 83 % dotázaných zdravotnických organizací uvedlo, že za poslední rok zaznamenaly nárůst kybernetických útoků. Dvě třetiny (66 %) dotázaných zdravotnických organizací uvedly, že se kybernetické útoky staly za poslední rok složitějšími.

Možná ještě hrozivější je zjištění, že téměř polovina (45 %) dotázaných zdravotnických organizací uvedla, že se setkaly s útoky, jejichž hlavním cílem bylo právě zničení dat, což by bylo obrovským problémem nejen ve zdravotnictví. A protože plné dvě třetiny (66%) dotázaných zdravotnických organizací uvedly, že jejich organizace byla cílem kybernetického útoku během uplynulého roku, je třeba, aby se všechny instituce a zařízení – nejen ty zdravotnické – na podobné útoky co nejlépe připravily. Tým expertů VMware pro tyto případy uvádí několik kroků.

První kroky pro potlačení kybernákazy pomocí VMware Carbon Black a VMware NSX

Karanténa – všechny systémy infikované kryptovirem se musí obnovit ze zálohy, nebo instalovat z iniciálních zdrojů. Neexistuje cesta, jak infikované stanice očistit. Jakákoliv data bez zálohy jsou těžce obnovitelná. Proces obnovy začíná vybudováním izolované virtuální sítě, do které se obnovují systémy ze záloh. Po úspěšné obnově se do systémů přidává anitivir nové generace VMware Carbon Black a provedou se dále popsaná nastavení.

Výměna aktuálního antiviru za antivir nové generace – tradiční antivirové programy poskytují opožděnou reakci, která je založená na statických signaturách a heuristické analýze. Antivir nové generace VMware Carbon Black je opravdová ochrana od bodu „nula". Technologie kombinuje statickou a dynamickou analýzu kódu pro detekci procesů vyvolaných kryptovirem. Přístup je nezávislý na souborech v každém systému a využívá kontinuální analýzu rizik a profilování na legitimní nástroje využité v provozu. Ochrání tak aplikace proti celému spektru moderních kryptoútoků. Antivir nové generace využívá fundamentálně odlišné techniky pro detekci a blokování zvolené aktivity. Detekuje škodlivý kód a anomálie na koncových stanicích a zasílá je do centra umělé inteligence. Tento antivir nové generace disponuje systémovým přehledem, prozkoumává každý běžící proces na koncových stanicích pro algoritmickou detekci a blokaci nástrojů, technik a procedur hackerů, pomocí kterých jsou vedeny vektory útoků.

Přidání EDR – průměrný čas pro potlačení bezpečnostní události je 66 dní. Systém EDR (Endpoint Detection and Response) oznámí podezřelé činnosti a zašle upozornění. Jeho nasazení zkracuje čas pro potlačení bezpečnostní události o 75 %, navíc dle posledních reportů se zkrátil čas potlačení z 8 hodin na pouhých 15 minut.

Kontrola a náprava v reálném čase – pracovní čas IT profesionálů, kteří odpovídají za velké množství oddělených systémů, je drahý. Pomocí nástrojů Carbon Black se otevírá cesta juniorním pozicím v IT oddělení pro úplný přehled koncových bodů a prostředků pro rutinní úkoly v bezpečnosti (bezpečnostním záplatování, monitoring, izolace). Profesionálové se tak mohou soustředit na šetření a hledání hrozeb.

Následující kroky s VMware Carbon Black a VMware NSX

Výše popsanými kroky ale plnohodnotná ochrana nekončí. K těm dalším důležitým bodům správného zabezpečení patří zavedení mikro-segmentace. Ta představuje izolaci služeb a aplikací pomocí nástroje VMware NSX. Pro stanovení přesné podoby segmentačních politik lze využít nástroje umělé inteligence nebo strojového učení. Posledním z nezbytných kroků je pak zavedení služby distribuovaného firewallu a IDS/IPS dostupné na všech hypervizorech.

Problémům je třeba předcházet

Všechny instituce spravují velké množství citlivých dat a kritických systémů. I proto by měly využívat možnosti moderních technologií a předcházet bezpečnostním problémům. A transformace kybernetické bezpečnosti pomocí řešení společnosti VMware je navržena tak, aby před těmi nejpokročilejšími hrozbami ochránila.

Eliška Jirovská, VMware Country Manager
for Czech Republic and Slovakia

Ondřej Číž, VMware Lead Solution Engineer

Tomáš Michaeli, VMware Lead Solution Architect

vmware®

ÚVOD DO OTEVŘENÝCH DAT

Významnou roli v konceptu e-governmentu a otevřeného vládnutí sehrávají otevřená data, jejichž principy a technické standardy výrazně usnadňují přístup k veřejně přístupným informacím, podporují jejich strojové zpracování a zejména jejich opakované používání a zhodnocování. Nejedná se o pouhé využití nových technologických možností, ale především o komplexnější přístup k informacím veřejné správy vyplývající z celosvětového fenoménu „otevřenost". Výchozí koncept a také první principy otevřených dat byly formulovány již v prosinci 2007 v kalifornském Sebastopolu zastánci otevřeného vládnutí a v roce 2015 byly upřesněny a zkoncentrovány do zásad v „Mezinárodní chartě otevřených dat", včetně shrnující definice pojmu „otevřená data".

OTEVŘENÁ DATA

„Otevřená data jsou digitální data, která jsou k dispozici s technickými a právními charakteristikami nezbytnými k tomu, aby byla volně používána, opětovně používána a distribuována kýmkoli, kdykoli a kdekoli."

Definice ve spojení se zásadami je dostatečně vysvětlující, přesto si ale některé oblasti problematiky otevřených dat zaslouží pár upřesňujících informací, aby nedocházelo k nevhodným výkladům, nesprávným implementacím a znehodnocení jejich potenciálu.

OTEVŘENOST – „KAŽDÝ MÁ PRÁVO PODÍLET SE NA SPRÁVĚ VĚCÍ VEŘEJNÝCH"

Otevřenost je zastřešujícím konceptem nebo filozofií, která se vyznačuje důrazem na transparentnost a spolupráci a je základem dnešního pojetí světa.
Otevřená data vycházejí z konceptu „otevřenosti" a v podmínkách veřejné správy se tato otevřenost vyskytuje ve dvou podobách. Jedná se o otevřenost právní a otevřenost technickou.

Právní otevřenost je zaměřena na legalizaci získávání dat, ustavení možností jejich sdílení, šíření a možností jejich následného zužitkování. Jedná se o odstranění legislativních bariér zpřístupnění informací spravovaných veřejnou správou a současně o ošetření těch informací, které souvisejí s ochranou osobních údajů, obchodního tajemství, bezpečnosti státu a ochranou autorských práv.
V ČR byla otevřená data legalizována a zavedena do legislativy novelou zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Zákon v §3 zavádí do legislativního prostředí klíčové pojmy v oblasti otevřených dat – strojově čitelný formát, otevřený formát, otevřenou formální normu, metadata a také definuje otevřená data v kontextu veřejné správy ČR:
„Otevřenými daty se pro účely tohoto zákona rozumí informace zveřejňované způsobem umožňujícím dálkový přístup v otevřeném a strojově čitelném formátu, jejichž způsob ani účel následného využití není omezen a které jsou evidovány v Národním katalogu otevřených dat."

ZÁSADY MEZINÁRODNÍ CHARTY OTEVŘENÝCH DAT:

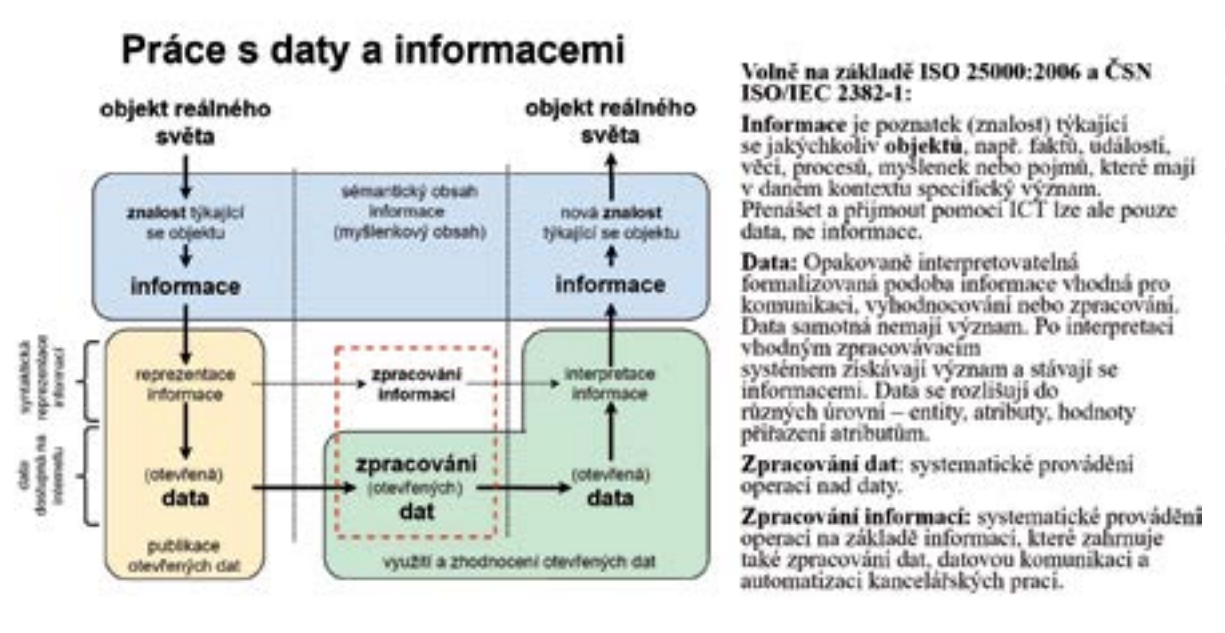
1. Otevřenost jako standard – automatické zveřejňování všech dat až na určité výjimky, například z důvodu bezpečnosti, ochrany osobních údajů, ochrany autorských práv, ...
2. Včasnost a ucelenost dat – důraz na relevantnost dat, tj. měla by být poskytnuta včasně, ucelená, přesná, vysoké kvality, původní a nemodifikovaná.
3. Přístupnost a použitelnost – strojová čitelnost dat, jejich snadná dostupnost, poskytovaní zdarma na základě otevřených licencí.
4. Srovnatelnost a interoperabilita – zajištění snadného vzájemného srovnání a interoperability dat, nutnost dodržování odsouhlasených datových standardů.
5. Zaměření na zlepšení vládnutí a zapojení občanů – zvyšování transparentnosti veřejné správy a zapojení se občanů do správy věcí veřejných.
6. Zaměření na inkluzivní rozvoj a inovace – přinášet výhody a přínosy všem uživatelům, veřejnému sektoru, privátnímu sektoru a celé společnosti.

Technická otevřenost je zaměřena na odstranění technických překážek spojených s publikací a používáním otevřených dat, což vyžaduje standardizaci především již samotné publikace dat, standardizaci používaných otevřených formátů, doprovodné dokumentace, zajištění kvality, dostupnosti a způsobu dohledání publikovaných dat. Zákon č. 106/1999 Sb. ve smyslu § 3 odst. 9 řešení této oblasti usnadňuje definicí pojmu „Otevřená formální norma", což je legislativní nástroj pro stanovení technických doporučení (standardů) s cílem zajištění, že stejná data publikovaná různými poskytovateli budou technicky otevřená a interoperabilní a pro poskytovatele otevřených dat jsou dle § 4b odst. 1 závazná.

PRÁCE S DATY A INFORMACEMI – ZÁKLAD KVALITY DAT

Data a informace jsou často vzájemně zaměňována a považována za synonyma. Základní rozdíl mezi daty a informacemi spočívá v tom, že informace mají konkrétní specifický význam (daný okolním kontextem), data samotná jsou bez významu a slouží k formalizaci informací do podoby vhodné ke strojovému zpracování.

Problém objasňuje následující obrázek, který je vytvořen na základě podkladu publikovaném v normě ISO/IEC 2382-1.



Z uvedeného obrázku je zřejmé, že informace jsou poznatky o konkrétním objektu vymezené specifickým kontextem (zachycené souvislosti na jiné objekty v rámci řešené domény). Význam kontextu lze jednoduše demonstrovat na příkladu pojmu škola. Ta se může vyskytovat v různých kontextech: škola jako nemovitost, škola jako vzdělávací instituce, škola jako zaměstnavatel atd. Je zcela zřejmé, že každému specifickému kontextu budou odpovídat jiná související data a vazby na jiné informace.

Pro strojové zpracování informací je nutná jejich vhodná reprezentace v rámci které jsou převedeny na data a následně je možné i jejich technologické zaznamenání, vhodné pro další zpracování a využívání. Navazujícím zpracováním dat dojde k vytvoření nových dat, jejich interpretaci (přiřazení významu) a vytvoření nové informace (nový poznatek). Tento způsob práce s informacemi je typický pro klasické informační systémy, které mají tu výhodu, že jejich celkový kontext je daný datovým modelem, který je neměnný a trvale známý všem částem i uživatelům informačního systému. Z tohoto důvodu jsou reprezentace informací, stejně jako interpretace dat snadné, neboť celkový kontext informací je uzamčený v uceleném informačním systému.

V případě otevřených dat je způsob práce s informacemi téměř stejný, pouze s tím rozdílem, že ke zpracování otevřených dat dochází obvykle mimo původní informační systémy, ze kterých byla data publikována (v obrázku odlišeno barevně: žlutá oblast – publikace dat z různých IS, zelená oblast – zpracování a interpretace dat v jiných systémech a aplikacích). Aby bylo vůbec možné

s publikovanými otevřenými daty pracovat, je nutné k publikovaným datům přidat informace o jejich významu a v jakém kontextu jsou používána. Prakticky to znamená publikovat s daty také jejich kontext (datové schéma, správně navržený a zdokumentovaný konceptuální model) a související metadata.

PRÁCE S KONTEXTY – POUŽÍVÁNÍ A ZHODNOCOVÁNÍ OTEVŘENÝCH DAT

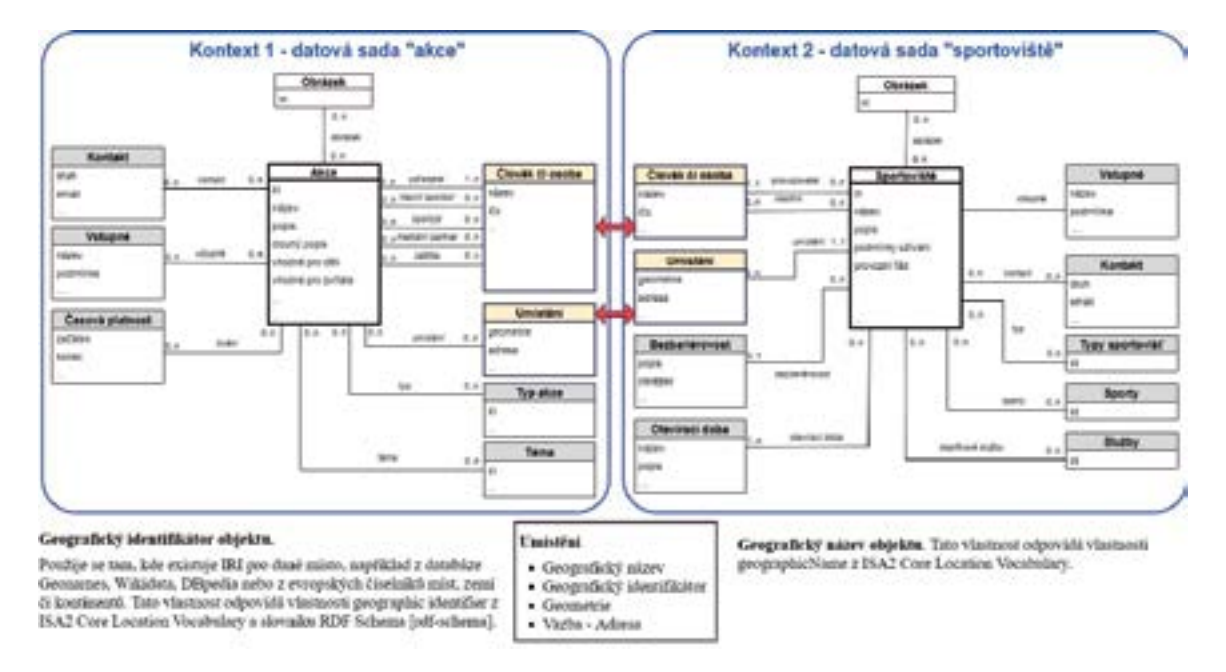
Používání a zhodnocování dat je základním cílem a smyslem otevřených dat. Možnosti jejich využití jsou rozmanité. V nejjednodušším případě se může jednat o pouhou prezentaci dat za účelem jejich zpřístupnění, zobrazení a podpory transparentnosti široké veřejnosti. Při náročnějších využitích půjde o spojování datových sad, hledání nových souvislostí (kontextů) a vytěžování nových poznatků, nebo v případě mobilních aplikací vytváření komplexnějších informací podporujících komfort jejich uživatelů – veřejnosti.

V případě interního využití veřejnou správou mohou otevřená data vyplnit stávající mezery ve sdílení dat jednotlivými organizacemi VS v těch případech, které agendové systémy neřeší, nebo jejichž vzájemná komunikace není součástí sběrnice eGon Service Bus. Příkladem takových mezer jsou například číselníky.

Obrázky níže uvádějí příklad zhodnocení dat pomocí propojení dvou datových sad.

Význam informací v datové sadě „sportoviště" je vyjádřen jejím konceptuálním modelem „Kontext 2". Model zachycuje základní objekt (entitu) „sportoviště" s jejími základními vlastnostmi (atributy) – iri, název, popis, podmínky užívání, provozní řád. Zbývající důležité informace jsou vyjádřeny vazbami na jiné entity, které jsou jejich zdrojem, jako např. provozovatel, vlastník, umístění apod. Model vymezuje specifický kontext informací o sportovišti a tím určuje i význam a smysl jednotlivých informací.

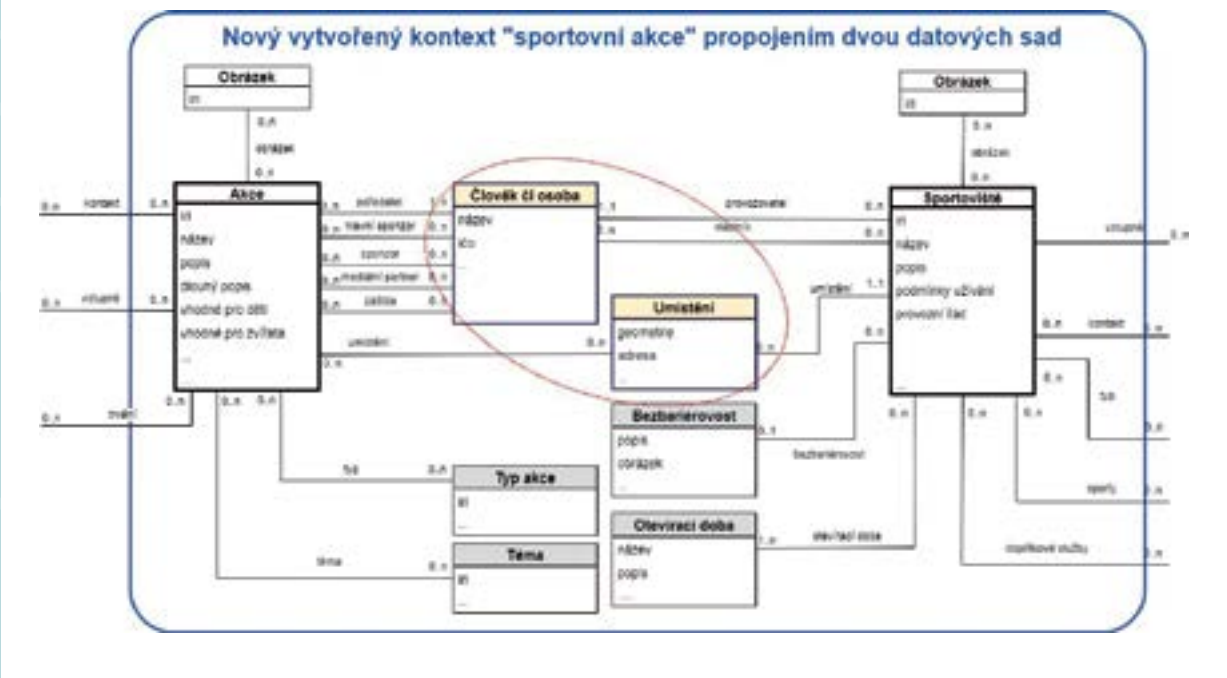
Obdobným způsobem je vyjádřena i druhá datová sada „akce" pomocí „Kontextu 1".



Při prohlídce obou kontextů je poměrně snadné zjistit, že obě datové sady jsou vzájemně propojeny entitami „umístění" a „člověk či osoba" a že se tedy nabízí datové sady propojit a vytvořit tak zcela nový kontext „sportovní akce" – následující obrázek.

Propojeným datovým sadám bude odpovídat nový datový model a interpretace dat i jejich vytěžování získá nový rozměr. Sdělované informace mohou být mnohem obsáhlejší a kladené otázky mohou být složitější a komplexnější – například: *„Jak souvisí poskytování sponzorství (nebo mediální partnerství) u jednotlivých typů akcí s místem konání (hraje roli vazba na vlastníky a provozovatele?)"*.

Názorná ukázka uvádí, že transparentnost není jenom o otevřenosti dat, ale také o možnostech dalšího (strojového) zpracování a jejich kvality.



Způsoby vytváření nových kontextů jsou omezeny pouze kvalitou publikovaných dat a kvalitou jejich popisu. Z použitých kontextů také vyplývá, že některé navázané entity jsou typu číselníků a v takových případech není vhodné vytvářet nové vlastní číselníky ani je nahrazovat konkrétními údaji, ale vždy odkazovat na číselníky již publikované jako samostatné datové sady – viz ukázka níže (další rozšíření výsledného kontextu informací).

OTEVŘENÁ DATA A EU

Pro úplnost popisu konceptu otevřených dat je nutné ještě zmínit pojem „interoperabilita" v rámci EU. Z pohledu otevřených dat se jedná o důležitý aspekt, neboť mezi cíle EU patří vytvoření jednotného digitálního trhu pro podporu a rozvoj hospodářského prostředí, zajištění interoperability evropských veřejných služeb usnadňující komunikaci občanů EU s veřejnou správou a vybudování sdíleného datového prostoru pro podporu inovací, vývoje a výzkumu.

Požadavky na zajištění interoperability v rámci EU jsou definovány pomocí European Interoperability Framework (EIF) na několika úrovních, přičemž otevřených dat se týká zejména právní, sémantická, syntaktická a technická interoperabilita.

Právní interoperabilita – je zaměřena na překonání rozdílností mezi právními předpisy v jednotlivých členských státech, zajištění, aby při výměně informací přes hranice byla zachována právní platnost těchto informací a aby byly dodrženy právní předpisy o ochraně údajů v poskytující i přijímající zemi.

Sémantická interoperabilita – umožňuje organizacím zpracovávat smysluplným způsobem informace z vnějších zdrojů. Zajišťuje, že při výměně informací mezi stranami bude správně chápán a zachován smysl vyměňovaných informací, datových prvků a vztahů mezi nimi. Zahrnuje vytvoření slovníku pojmů pro popis vyměňovaných údajů.

Syntaktická interoperabilita – týká se popisu přesného formátu vyměňovaných informací (dat), pokud jde o gramatiku, formát a schémata.

Technická interoperabilita – souvisí s technickými stránkami zajištění propojení informačních systémů a sdílených informací. Zahrnuje specifikace rozhraní, spojové služby, služby integrace dat, prezentace a výměny údajů.

ZÁVĚREM CITÁT ALBERTA EINSTEINA:

Albert Einstein kdysi prohlásil, že ***„všechno by mělo být tak jednoduché, jak to může být, ale ne jednodušší“***. A to se týká i otevřených dat. Zdánlivá snadnost jejich publikace a k tomu zjednodušené pojetí pojmu „otevřenost“, způsobily, že otevřená data se publikují, avšak různými způsoby a bez zaměření na jejich další použitelnost a zhodnocování. Z těchto důvodů je dále uvedená stručná rekapitulace problematiky otevřených dat a na ně kladených požadavků zcela na místě.

Drahomír Chocholatý

Tento článek vznikl v rámci projektu „Rozvoj datových politik v oblasti zlepšování kvality a interoperability dat veřejné správy “OPZ č. CZ.03.4.74/0.0/0.0/15_025 /001398, který zastřešuje odbor Hlavního architekta Egovernmentu, Ministerstvo vnitra ČR.

STRUČNÁ REKAPITULACE PROBLEMATIKY OTEVŘENÝCH DAT

1. Otevřená data jsou definována:

- Mezinárodní chartou otevřených dat;
- zákonem č.106/1999 Sb., o svobodném přístupu k informacím;
- směrnicí Evropského parlamentu a rady 2019/1024/EU ze dne 20. června 2019 o otevřených datech a opakovaném použití informací veřejného sektoru.

2. Definice ale nestačí, otevřená data především musí:

- respektovat zásady Mezinárodní charty otevřených dat;
- naplňovat definici v zákoně č. 106/1999 Sb. a být registrována v Národním katalogu otevřených dat;
- být publikována takovým způsobem, aby bylo možné jejich další využití a zhodnocování (publikace kontextu a metadat, uznávání standardů, dodržování otevřených formálních norem);
- dodržovat požadavky na kvalitu dat;
- mít ošetřeny podmínky užití;
- naplňovat požadavky kladené na jejich interoperabilitu nejen v rámci ČR, ale i v rámci EU,

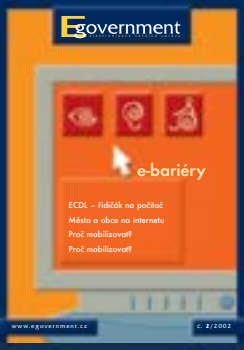
aby vše nebylo jednodušší, než to může být.

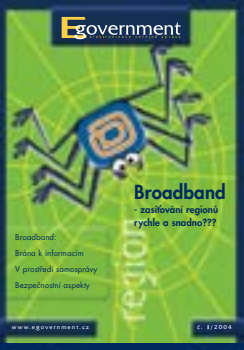
3. Otevřená data jsou významná, neboť jsou prostředkem k:

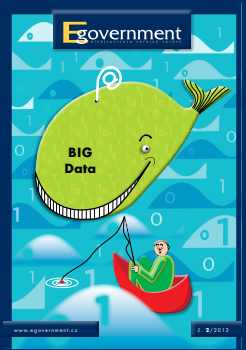
- posilování transparentnosti VS a směrování k otevřenému vládnutí a otevřené společnosti;
- budování e-govenmentu VS ČR (součást architektury VS – Veřejný datový fond);
- vytvoření jednotného digitálního trhu pro podporu a rozvoj hospodářského prostředí EU;
- vybudování sdíleného datového prostoru pro podporu inovací, vývoje a výzkumu v celé EU.

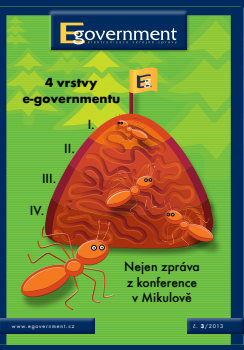
Egovernment

elektronizace veřejné správy









Vše o elektronizaci veřejné správy
- srozumitelně a zdarma:

www.egovernment.cz

e-government 20:10

aneb žijem si jak na zámku, ať to trvá věčně

MIKULOV • 8. - 9. 9. 2020

ZAČNEME ZNOVU

8. - 9. 9. 2020

www.egovernment.cz