Egovernment
elektronizace veřejné správy

„Žijem si jak na zámku,
ať to trvá věčně.“

KONFERENCE MIKULOV e-government

Úvodní slovo

Žijeme si jako na zámku, ať to trvá věčně

to je podtitul našeho již pravidelného setkání v Mikulově. Bavíme se tady o tom co je nového, co se nového blíží, co nás čeká a nemine a taky si tady zvolíme nejsympatičtější dámu české veřejné správy pro daný rok. Držíte v rukou magazín, který je určitým průvodcem po našem zámeckém diskutování.

Letos, po informačně poněkud klidnějším období, to vypadá, že český e-government opět dostane konečně určitou dynamiku. Je to dáno především tím, že nás k tomu nutí vnější okolnosti – strukturální fondy, respektive nové už rok běžící programové období a hlavně nařízení EK ohledně zavádění elektronické identity. A tak jsme letos slyšeli konečně znění některých konkrétních výzev a rovněž jsme diskutovali o tom, jaké nároky a v jakém horizontu na nás elektronická identita klade. I o tom byla naše debata v Mikulově.

A tak, pokud jste nebyli s námi na zámku, začtěte se, krom informací o jednotlivých prezentacích jsou zde k dispozici doplňující články a samozřejmě představíme i Miss Egovernment 2015.

Ing. Michal Jirkovský
šéfredaktor

NERISKUJTE A ZÁLOHUJTE FIREMNÍ DATA U NÁS V BEZPEČÍ

Díky zázemí a odbornému know-how velké mezinárodní firmy vám dokážeme garantovat, že vaše data budou vždy v naprostém bezpečí. S individuálním řešením zálohování v našich datových centrech ušetříte náklady na vlastní IT řešení a ke svým datům budete mít přístup kdykoliv a kdekoliv – z počítače, tabletu i mobilu. Zálohujte u jedničky v datových centrech.

Více na www.t-mobile.cz/profirmy

T · ·

GTS

Zdroj: Disaster Recovery Preparedness Council

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
ISSN 1801-9420

Šéfredaktor: Ing. Michal Jirkovský
Korektorka: PhDr. Helena Veverková
Asistentka: Mgr. Kristýna Petrů

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

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.

CETIN
ČESKÁ TELEKOMUNIKAČNÍ INFRASTRUKTURA

JSME TAM, KAM OSTATNÍ NEDOSÁHNOU

- Jsme CETIN – vlastník a provozovatel největší telekomunikační sítě v České republice.
- Naše služby jsou dostupné 99,6 % populace.
- Úřady, podniky i domácnosti propojujeme sítí 20 000 000 km metalických kabelů a 38 000 km optických vláken.
- Poskytujeme fyzické síťové uzly i v zahraničí (např. Londýn, Vídeň, Bratislava, Frankfurt nebo Hongkong).

Obchodní kontakt
Tel.: +420 238 463 819 (9-17 SEČ), E-mail: sales@cetin.cz
www.cetin.cz

TO NEJDŮLEŽITĚJŠÍ, CO NÁS ČEKÁ V PŘÍŠTÍM ROCE:

16. 2. 2016

Jihlava – Jednotné elektronické podání

Konferenční sezonu otevíráme pravidelně v Jihlavě tentokrát aktuálním tématem Jednotného elektronického podání.

1. – 3. 6. 2016

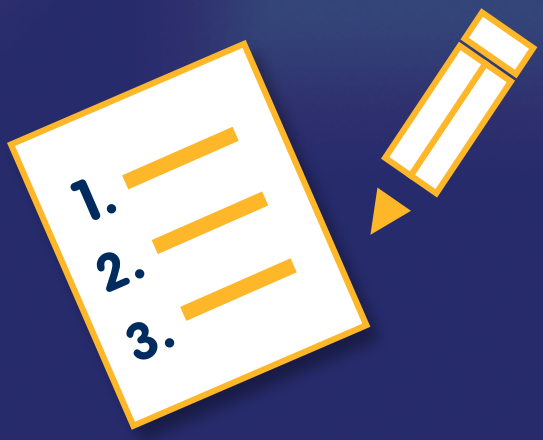
Rok informatiky – Náchod

Pravidelné setkání všech, které zajímá elektronizace veřejné správy se tentokrát odehraje začátkem června v Náchodě.

6. – 7. 9. 2016

e-government 20:10 – Mikulov

V září si opět budeme žít jako na zámku a přitom diskutovat problematiku elektronizace veřejné správy.



Egovernment

elektronizace veřejné správy

Vše o elektronizaci veřejné správy - srozumitelně a zdarma:

www.egovernment.cz

V Mikulově jsme si žili opět jako na zámku

Ve dnech 8. – 9. září proběhl na zámku Mikulov již sedmý ročník konference e-government 20:10, aneb žijem si jak na zámku, ať to trvá věčně. I letos se tradičně hodnotil stav elektronizace veřejné správy v České republice, diskutovalo o strategiích pro nejbližší období a hledaly cesty k financování zajímavých projektů.

Hlavní blok konference byl ve znamení vystoupení **MV ČR**, které zde reprezentovali hned dva náměstci – **Jana Vildumetzová, která řídí sekci veřejné správy,** a **Jiří Zmatlík za sekci ekonomiky, strategií a evropských fondů.**

Mezi ně se „vtlačila" pětice pánů, která reprezentovala Útvar hlavního architekta, respektive sekci informačních a telekomunikačních technologií. Byli jimi **Petr Kuchař, ředitel odboru hlavního architekta eGovernmentu, Roman Vrba, ředitel odboru eGovernmentu**, **Miroslav Tůma, ředitel odboru kyberbezpečnosti a koordinace ICT**, **Tomáš Kroupa, vedoucí oddělení strategie a standardizace z odboru hlavního architekta eGovernmentu, a Roman Fišer, který je věcným gestorem projektu agendy A121.**

Příští rok se v Mikulově sejdeme v termínu 6. – 7. 9. 2016

Účastníci konference, kteří do Mikulova zavítali, tak dostali komplexní informace, které doplnil konkrétními čísly ve vztahu k možnostem financování projektů kybernetické bezpečnosti z IROP **Aleš Pekárek za MMR**.

Odpolední sekce pak nabízely informace k jednotlivým projektům a dávaly větší prostor pro diskuzi. Druhý den konference byl monotematicky věnován problematice elektronické identity, a to jak z legislativního, tak právního, technického i uživatelského pohledu.

Oba dva konferenční dny tradičně propojoval společenský večer, v jehož rámci byla zvolena Miss Egovernment 2015, tedy nejsympatičtější dáma české veřejné správy. I přes chladnější počasí se jednalo o zábavné představení, které v čele poroty bedlivě sledovala náměstkyně ministra vnitra Jana Vildumetzová, spolu se státním tajemníkem Jiřím Kauckým. I díky jejich hlasům se Miss Egovernment 2015 stala Hana Pospíšilová z České pošty Brno, první vicemiss Kateřina Komárková ze Správy základních registrů a na třetím místě a druhou vicemiss se stala Alena Leinweberová z Ministerstva kultury.

Zatímco vítězky soutěže si odvážely hodnotné ceny od partnerů, téměř šest stovek účastníků konference si odváželo dostatek nových informací, případně pak kvalitní moravská vína, která zde byla tradičně, v termínu těsně před vinobraním, v nabídce.

Informace o konferenci naleznete na následujících stránkách magazínu, nebo na **www.egovernment.cz/mikulov**, kde jsou umístěny i jednotlivé prezentace.

VIZE ROZVOJE VEŘEJNÉ SPRÁVY

Náměstkyně ministra vnitra pro řízení sekce veřejné správy v úvodu vystoupení pozdravila účastníky konference e-government 20:10, aneb žijem si jak na zámku, ať to trvá věčně, a to jak jménem svým, tak jménem ministra vnitra Milana Chovance, který dal konferenci svoji záštitu, ale z pracovních důvodů nemohl být přítomen.

Jak náměstkyně Vildumetzová uvedla, připravila si na dnešek téma vize rozvoje veřejné správy. Zdůraznila, že hlavním cílem vize veřejné správy je, aby veřejná správa byla kvalitní, efektivní a transparentní a především byla pro občany. Vrátila se krátce do minulosti, když připomněla rok 1999 a tehdy probíhající reformu veřejné správy. Reforma se týkala územní veřejné správy, ústřední veřejné správy a právě i modernizace a zvýšení efektivity veřejné správy, ale bohužel nebyla dokončena. Jana Vildumetzová připustila, že bylo již připraveno mnoho koncepčních návrhů, které ovšem vždy skončily buď před projednáváním v Poslanecké sněmovně nebo před projednáním ve vládě. Bylo to především zákonné řešení územního členění státu, což je velký problém, kterému se podle náměstkyně budeme muset věnovat i proto, že je to jedna z předběžných podmínek Evropské komise. Do

příštího roku tak musíme předložit věcný záměr harmonizačního členění státu.

Rovněž koncepce dokončení reformy veřejné správy byla zpracována, ale jak uvedla Jana Vildumetzová, v roce 2012 byla stažena z jednání vlády. Zatím tedy nemáme zpracovánu a přijatu ucelenou strategii veřejné správy. Nemáme tedy plán, kam bude dál veřejná správa směřovat. To je podle Jany Vildumetzové náš hlavní úkol, kterým se musíme nyní zabývat.

Jak sama uvedla, mohla by v rámci konference hovořit o mnoha tématech. Například o volbách, o příspěvku na výkon veřejné správy, o zákoně č. 106/1999 o svobodném přístupu k informacím, o matričních úřadech atp. Místo toho chtěla, podle svých slov, na jednom případě ukázat, kam by měla veřejná správa směřovat. Tím příkladem bylo vydávání občanských průkazů a cestovních dokladů, neboť tato problematika je právě v její sekci. Problémem, který v letošním roce řešíme, je totiž nárůst vydávání občanských průkazů. Tento rok uběhla desetiletá lhůta, kdy si všichni občané museli měnit staré občanské průkazy, které byly ještě v podobě červených knížeček. Jana Vildumetzová uvedla, že MV ročně obvykle vydá okolo milionu a půl občanských průkazů. V letošním roce je to, kvůli uvedené skutečnosti, asi o pět set tisíc víc. I proto MV ČR velmi apelovalo na rozšíření úředních hodin úřadů. Občanské průkazy vydávají pouze obce s rozšířenou působností, kterých je na území České republiky jen dvě stě pět. Zároveň byla provedena analýza identifikující existenci vyvolávacích a rezervačních systémů a sledující vytíženost kabin. MV ČR podle slov náměstkyně Vildumetzové eviduje mnoho žádostí o větší počet těchto kabin, které údajně kapacitně nestačí.

Vedle tohoto „krizového" řešení je rovněž nutno uvažovat o systémovém řešení, kterým je rozšíření kontaktních míst, a to ve spolupráci s pověřenými obecními úřady, vydávání občanských průkazů s čipem a samozřejmě jednotnost postupů a následné procesné modelování agend. Cílem by mělo být, aby došlo ke sjednocení tří agend – občanské průkazy, cestovní doklady a řidičské průkazy.

ÚŘEDNÍ HODINY

Úřední hodiny vydávání OP byly jedním ze zásadních témat vystoupení náměstkyně Jany Vildumetzové. Jak uvedla, obce s rozšířenou působností by chtěly zřizovat více pracovišť. Důvodem je údajně stávající nedostatečný počet, velké fronty atp. Jana Vildumetzová si v této souvislosti nechala zpracovat analýzu, ze které vyplývá, že tato pracoviště jsou v současné době využita v některých městech pouze 16 hodin týdně. To je, podle jejího mínění, nepřijatelné. Pokud úřad nemá úřední hodiny nastavené minimálně na 30 hodin týdně, není podle ní možné, v jeho rámci, uvažovat o zřizování dalšího pracoviště.

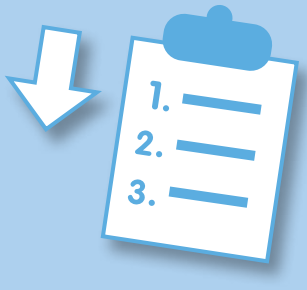
Při své návštěvě Státní tiskárny cenin, která vyrábí Občanské průkazy, zjistila, že nejvyšší odběr nových průkazů se odehrává v pondělí a ve středu (zhruba 20 000). V úterý a ve čtvrtek se jedná o tří tisíce a v pátek pouze tisíc. V tomto směru by podle paní náměstkyně mělo dojít ke změně a vyrovnání stavu.

REZERVAČNÍ SYSTÉM

Z uvedeného průzkumu vyplývá, že z 205 obcí s rozšířenou působností je možné se pouze na sto čtyřiceti obcích objednat prostřednictvím nějaké formy rezervačního systému. Na sedmdesáti devíti to v žádném případě možné není. Objednání je v tomto směru uvažováno telefonicky, smskou nebo elektronicky přes objednávací systém. Jana Vildumetzová možnost objednání zdůraznila jako velice důležitou právě s ohledem na vstřícnost vůči klientům. S tím ovšem souvisí i termín objednání. Problematické je, pokud se jedná o termíny v délce 20 i 30 dní. Je potěšující, že téměř 60 úřadů umožňuje objednání ihned či do druhého dne, ale nemalé množství je těch, které objednávají v horizontu deseti a více dní, a to není pro klienty komfortní.

Analýza, ze které náměstkyně Vildumetzová čerpala pro svoji prezentaci, rovněž sledovala existenci vyvolávacího systému, tedy zařízení, které umožňuje, aby klient po pří-

chodu na úřad nemusel hlídat, zda jej někdo nepředběhne atp. V této souvislosti je zajímavé, že čísla jsou v podstatě shodná s čísly o rezervačním systému přitom se ale nejedná o stejné obce. Tedy ten úřad, který má rezervační systém, nemá zároveň vyvolávací systém a naopak. Cílovým stavem by měl být stav, kdy všechny obce s rozšířenou působností v budoucnosti budou disponovat jak vyvolávacím, tak rezervačním systémem. Kromě toho je podstatná rovněž existence informačního kanálu, nejčastěji webu, na kterém je možné sledovat průběh dané zakázky tak, aby si klient nemusel na úřad opakovaně telefonovat.



ÚŘEDNÍ POSTUPY

V rámci uvedené analýzy považuje náměstkyně Vildumetzová za velice zajímavý rovněž výstup, který se týká sjednocení úředních postupů. Otázkou bylo, zda a jak se liší postupy správních orgánů při vyřizování jednotlivých agend státní správy. Při porovnání toho, zda úřady při vyřizování jednotlivých agend postupují jednotně, byly uvažovány stavební řízení, evidence obyvatel a vydávání občanských průkazů. Bylo zjištěno, že nejvíce se liší postup úřadů při realizaci stavebního řízení. U vydávání občanských průkazů byla odpověď o rozdílném přístupu úřadů jen 20 %, ale i zde považuje za nutné sjednotit náležitá pravidla.

Náměstkyně Vildumetzová se ještě zastavila u tématu Strategického rámce rozvoje veřejné správy, kde je cílem: kvalita, efektivita a transparentnost s důrazem decentralizace, dekoncentrace a subsidiarity. Jak uvedla, dnes máme 205 obcí s rozšířenou působností. Na základě svého dotazování zjistila, že ze 182 pověřených obecních úřadů by minimálně dalších 127 mělo zájem také vydávat občanské průkazy a cestovní doklady.

Jedná se tedy, podle ní, o téma, které bychom měli řešit. Jestliže existuje 7000 Czech POINTů a 5800 měst, kde si můžeme vyřídit výpis z rejstříku trestů či výpis z katastru nemovitostí, pak je zarážející, že máme pouze 205 míst, kde si můžeme vyřídit občanský průkaz a cestovní doklad. Je sice pravdou, že se jedná o agendu, kterou si řešíme 10x za život. Občanský průkaz ale vlastní každý občan a každý si ho jde vyměnit. Je to tedy agenda, která dělá největší obraz veřejné správy. A proto musíme zajistit, aby byla stále zkvalitňována a vylepšována.

Náměstkyně Vildumetzová připomněla, že v současné době je v Poslanecké sněmovně projednáván sněmovní tisk, novela zákona o evidenci obyvatel, rodných číslech, občanských průkazech a cestovních dokladech. Účinnost toho zákona by měla být od 1. ledna příštího roku a měla by právě přinést sjednocení v oblasti občanských průkazů a cestovních dokladů. Nebude nadále platit místní příslušnost ani u občanského průkazu ani u cestovního dokladu a každý občan bude mít možnost si sám rozhodnout, kam si půjde tuto agendu vyřídit. Předpokladem je, že občan se bude rozhodovat podle kvality nabízených služeb, tedy že i obce s rozšířenou působností se budou v uvozovkách muset snažit, aby měly klientelu pro tuto agendu. MV ČR se bude v budoucnosti zabývat i příspěvkem na výkon státní správy, tzv. výkonovým placením. Podle náměstkyně Vildumetzové eviduje apely ze strany starostů, že tento příspěvek je nedostatečný a v oblasti občanských průkazů je to pro ně nejvíc diskutabilní. Je totiž jedno, zda úřad vydá za den velký nebo malý počet průkazů, příspěvek dostane stejný. Přitom se jedná o agendu, která je měřitelná, tedy přesně víme, která obec kolik vydala občanských průkazů a cestovních dokladů. Proto bychom se v budoucnosti měli dát cestou výkonového placení za daný doklad, a jak dodala, myslí si, že by to mělo právě přinést i motivační prvek.

Vedle občanských průkazů je tu otázka dalšího sjednocení agend, a to s řidičskými průkazy. U řidičských průkazů platí místní příslušnost, přitom se nejedná o stejné pracoviště jako cestovní doklady a občanské průkazy. Náměstkyně Vildumetzová by si představovala jako ideální získat finanční prostředky z evropských strukturálních fondů na projekt, který by přinesl jedno pracoviště, v jehož rámci by se vydávaly občanské průkazy, cestovní doklady i řidičské průkazy. Jana Vildumetzová se domnívá, že by to přineslo efektivnější a kvalitnější veřejnou správu i spokojenost klientů. Uvedený projekt by byl směřován nejen na 205 obcí s rozšířenou působností, ale samozřejmě i na rozšíření těchto míst, kterými by byly pověřené obecní úřady.

software602®

Formulářové aplikace pro Váš úřad

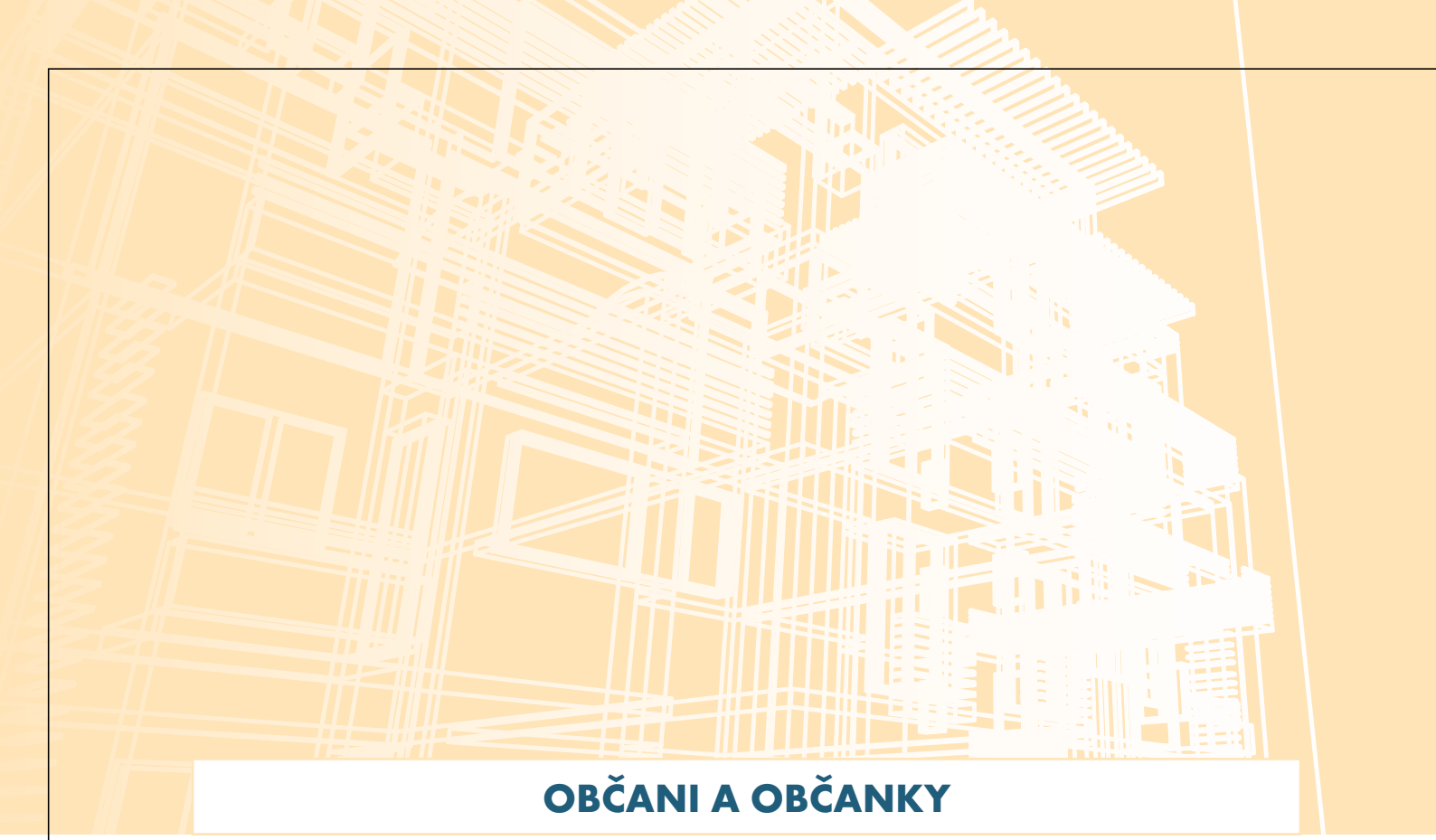
Chytré řešení pro vaše agendy

- CESTOVNÍ PŘÍKAZ
- ELEKTRONICKÁ PODÁNÍ PRO OBČANY
- PŘÍPRAVA MATERIÁLŮ PRO RADU A ZASTUPITELSTVO
- DOVOLENKA, NEPŘÍTOMNOST
- SCHVALOVÁNÍ FAKTUR
- EVIDENCE SMLUV A JEJICH ZVEŘEJŇOVÁNÍ
- EVIDENCE VEŘEJNÝCH ZAKÁZEK
- AGENDY PRO PORTÁL OBČANA A ÚŘEDNÍKA
- OBJEDNÁVKY
- INTERNÍ SDĚLENÍ, KOORDINOVANÉ STANOVISKO
- ELEKTRONICKÁ PODPISOVÁ KNIHA
- ÚKOLY
- AGENDY PRO ZŘIZOVANÉ ORGANIZACE
- MOBILNÍ KANCELÁŘ
- PŘÍSTUP K INFORMACÍM DLE ZÁKONA 106/1999
- ZÁKON O STŘETU ZÁJMŮ DLE ZÁKONA 159/2006
- PŘIDĚLOVÁNÍ UŽIVATELSKÝCH PRÁV
- EVIDENCE A REZERVACE
- ŽÁDOSTI A SCHVALOVÁNÍ ŠKOLENÍ
- HELP-DESK
- ANKETY
- ELEKTRONICKÉ ŽÁDOSTI
- SBĚRY DAT A DOKUMENTŮ
- SBĚR ŽÁDOSTÍ O GRANTY A DOTACE

KONTAKTUJTE NÁS PRO VÍCE INFORMACÍ!

Michal Vejvoda | obchodní ředitel divize Samospráva | +420 725 326 994 | vejvoda@602.cz
Radim Beran | obchodní manažer | +420 702 284 514 | beran@602.cz
Jiří Širek | obchodní manažer | +420 725 036 913 | sirek@602.cz

Software602 a.s. | Hornokrčská 15, 140 00 Praha 4 | +420 222 011 602 | info@602.cz
www.602.cz | www.LongTermDocs.eu | www.FormApps.eu



OBČANI A OBČANKY

Takový název neslo vystoupení pětice mužů, která reprezentovala Ministerstvo vnitra a především Útvar hlavního architekta. Byli jimi Roman Vrba, ředitel odboru eGovernmentu, Petr Kuchař, ředitel odboru hlavního architekta eGovernmentu, Miroslav Tůma, ředitel odboru kyberbezpečnosti a koordinace ICT, Tomáš Kroupa, vedoucí oddělení strategie a standardizace odboru hlavního architekta eGovernmentu, a Roman Fišer, věcný gestor projektu agendy A121 – živnostenské podnikání.

Moderátorem tohoto minibloku Ministerstva vnitra byl Petr Kuchař, který sám hovořil a předával slovo jednotlivým svým kolegům. Jejich společný program uvedl i tím, že doposud bývalo zvykem, že prezentace MV sestávaly z několika dlouhých, doslova naučných vystoupení. Dnes by se mělo jednat o celkově dynamické vystoupení pěti osob s devíti tématy. V krátkosti jednotlivé pány představil, a protože to bylo poprvé, kdy konferenčně vystupoval v pozici ředitele odboru hlavního architekta, v krátkosti uvedl sám sebe a přiblížil svoji dosavadní práci. Ta byla spojena s dlouhodobým vývojem nikoli pro veřejnou správu, ale pro komerčně zaměřený software ABRA. Nyní je ředitelem odboru hlavního architekta, jehož hlavní kompetencí je správa Národního architektonického plánu, který je zhmotněním minulých vizí. Význam Národního architektonického plánu Petr Kuchař přirovnal ke stavebnímu plánu. Je zcela běžné, že nikdo se při stavbě nového domu bezhlavě nesnaží rozkopat celou ulici jenom proto, aby si ke svému domu přivedl plyn. Obvykle se spoléháme na tvz. sdílenou službu, tedy na skutečnost, že v této ulici již někdo poskytuje vedení plynu pro všechny, a my budeme pouze požadovat, abychom měli k dispozici plynovou přípojku u paty svého domu. S ICT je to podle Petra Kuchaře velice podobné a Národní architektonický plán je zhmotněním této vize. Je tedy zakreslením základních systémů, kterými typově jsou základní registry, datové schránky, Czech POINTy atd. Smyslem tohoto zakreslení je možnost posoudit všechny budoucí systémy na shodu s Národním architektonickým plánem. Díky tomuto posouzení pak je možné zajistit, aby se nedělaly další a další „plynovody v jedné a téže ulici“, aby se tak neopakovaly projekty a postupy, které již jsou realizovány a mohou být k dispozici.

eIDAS

Prvním prezentovaným tématem byla elektronická identita. Petr Kuchař zdůraznil, že téma je nejen zajímavé, ale rovněž velice aktuální. Jedná se o směrnici eIDAS, na kterou se podle jeho slov můžeme dívat jako na zářijovou směrnici, neboť spousta jejích milníků se odehrává právě vždy v září. Směrnice byla vyhlášena v roce 2014, její první milník nastává letos 18. září a jedná se dobro-

volné využití elektronického ID. První vážný milník nastane 1. 7. 2016, tedy za necelý rok, kdy vejdou v platnost části směrnice, které řeší služby vytvářející důvěru a elektronický dokument. A patrně nejdůležitějším milníkem bude 18. 9. 2018. Do tohoto data musí mít členské státy EU hotové svoje systémy elektronických identit a rozpoznávání. Petr Kuchař se věnoval tomu, jak MV ČR přistupovalo k implementaci této směrnice. Uvedl, že existuje řídící výbor eIDAS, v jeho rámci pak šest pracovních skupin, které ten výbor řídil. Těchto šest skupin se podle slov Petra Kuchaře dělí na ty, které pracují, a na ty, jež se zatím nesešly, a to v poměru 3:3. Skupiny „elektronické podpisy, elektronická identita a elektronický dokument" se podílely na nové legislativě – zákonu o službách vytvářejících důvěru. V případě těch, které se ještě nesešly (elektronické doporučené doručování, Gateway národního ID, dohledové orgány) se čeká na kroky Evropské komise, konkrétně na Cooperation Network a Expert Group.

CO SE DĚJE AKTUÁLNĚ A CO SE DÍTI BUDE?

Petr Kuchař připomněl, že MV ČR poslalo do vnitřního připomínkového řízení nový zákon o službách vytvářejících důvěru (blíže bude popsán ve vystoupení Romana Vrby). Důležité podle jeho mínění je, že na rok 2016 je chystána realizace Národního identitního prostoru a přípravy elektronického občanského průkazu jako datového nosiče garantované státní identity. Zároveň se počítá s novelou uvedeného zákona, neboť bude nutné jej průběžně upravovat. Na rok 2017 a 2018 jsou podle Petra Kuchaře připraveny realizace Národního ID provozovaného Správou základních registrů, případně příprava Národního systému doporučeného doručování.

RVIS A LEGISLATIVA

Pro přiblížení aktivit Rady vlády pro informační společnost (RVIS) předal Petr Kuchař slovo Romanu Vrbovi. Toto téma bylo zařazeno do bloku konference především proto, že reálně je o aktivitách RVIS malé povědomí. Připomněl, že RVIS začala fungovat na konci roku 2014 a celá rada má 27 členů. Zajímavé je, že tato rada je propojena s Radou vlády pro veřejnou správu (RVVS), a to prostřednictvím společného řídícího výboru pro eGovernment a služby informační společnosti ve veřejné správě. V letošním roce se RVIS setkala 4x a její předsednictvo se pravidelně schází jednou za dva týdny. Nejvýkonnější pracovní skupinou pod RVIS je podle slov Romana Vrby skupina pro jednací řízení bez uveřejnění. Předsedou RVIS je trvale pověřen náměstek IKT Jaroslav Strouhal. Momentálně vznikají další pracovní skupiny, například pracovní skupina pro prostorové informace, která vzniká na základě usnesení vlády, kterým byla schválena geoinfostrategie a v podstatě bude nahrazovat celou řídící strukturu geoinfostrategie.

NEJVÝZNAMNĚJŠÍ ÚKOLY PRO ROK 2015

Roman Vrba informoval o tom, že již byly, ve spolupráci s ostatními resorty, definovány a dokončeny prioritní projektové okruhy, které byly ve spolupráci s RVVS předány vládě na konci července a v průběhu srpna byly schváleny. V současné době je připravena ještě strategie rozvoje ICT služeb veřejné správy (tzv. Voříškova srategie), která se nyní projednává. Podle povědomí Romana Vrby chybí už jen jeden bod na vypořádání, pak bude moci být předložena vládě. Souhrnně se o RVIS dá říci, že se jedná o scelující orgán, který by měl řešit ICT ve veřejné správě ČR. Jeho zásadním úkolem je kontrola strategického rámce cíle 3.

Roman Vrba dále uvedl, že legislativa je základním kamenem veřejné správy. Můžeme mít sebelepší informační systém, který ale bez legislativní podpory nebude fungovat. Proto se věnoval zásadním legislativním mezníkům letošního roku. Jednalo se o novelu zákona o základních registrech, která se podle jeho slov připravovala velmi dlouho a kodifikuje rejstřík orgánů veřejné moci. V podstatě narovnává celý proces fungování informačních systémů datových schránek a působnostního AISu a byla již předložena vládě. Za další zásadní legislativní moment považuje Roman Vrba návrh zákona o službách vytvářejících důvěru. Jak řekl, je to v podstatě nový zákon, který nahrazuje původní zákon o elektronickém podpisu a doplňuje nařízení eIDAS, která budou aplikována k 1. 7. 2016. Posledním důležitým dokumentem je vyhláška o autentizačních certifikátech, která je momentálně ve vnitroresortním připomínkovém řízení. Většina připomínek je v tuto chvíli vypořádána a předpokládaný termín účinnosti je 1. 1. 2016.

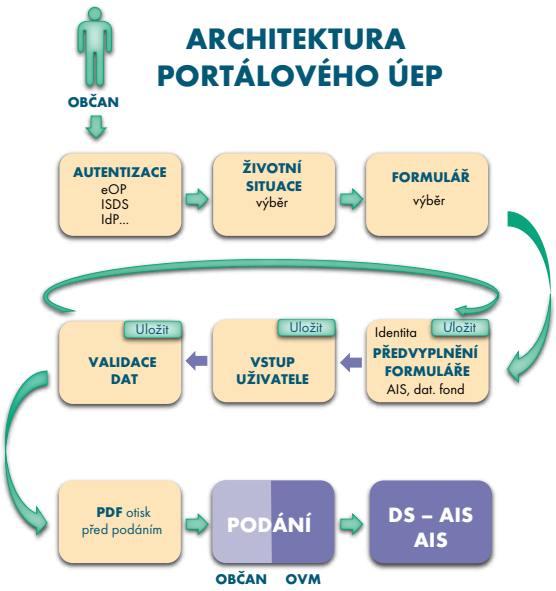
NÁRODNÍ ARCHITEKTONICKÝ PLÁN

Tomáš Kroupa se následně věnoval tématu Národního architektonického plánu (NAP). Jak řekl, jedná se o prostředek pro efektivní řízení informatiky v úřadu a eGovernmentu jako celku. Je to soubor architektur a vzorů, který má dvě části – architektura úřadů a architektura sdílených služeb. Obě tyto části splňují tzv. princip čtyř vrstev. Celý Národní architektonický plán je podle slov Tomáše Kroupy tvořen v notaci jazyku Archimade a snaží se dodržovat metodiku Togaf.

- **Architektura úřadů** zahrnuje samotný úřad a to jak v případě malého úřadu, tak z pohledu úřadu jako korporace, tedy úřadu, který řídí jemu podřízené organizace. K tomu budou vydány vzory, které budou definovat základní strukturu a očekávané komponenty, jak by takový úřad na jednotlivých úrovních měl vypadat. Smyslem je, že ze vzoru bude vidět, jak například městská část z principu vypadá. Následně příslušný úřad pouze zadá, co již má, případně co by měl mít. Úložištěm těchto modelů jsou tzv. centrální depozitory, které udržuje Útvar hlavního architeka. Podstatné podle Tomáše Kroupy je, že ÚHA čeká od úřadů vstupy ve formátu OpenGroup Exchange Format. Jinými slovy je jedno, jaký produkt úřady použijí, jakým nástrojem budou podklady zpracovávat, ale pro ÚHA je podstatné, aby bylo možné tyto informace importovat.
- **Architektura sdílených služeb** je, z pohledu Tomáše Kroupy, především globální architektura eGovernmentu, ve které jsme schopni dohledat, zda konkrétní aplikace již ve veřejné správě náhodou neexistuje, abychom ji nedělali znovu. Vedle toho budou existovat, a jak zdůraznil, z části již existují povinné architektonické vzory. To jsou pravidla, kterými ÚHA bude vynucovat, aby jednotlivé úřady své projekty a systémy stavěly správně. Mezi takové architektonické vzory patří například propojený datový fond, kontaktní místa, nebo centrální místo služeb.

Než předal Petr Kuchař slovo dalšímu vystupujícímu, ještě u architektury zůstal. Jak řekl, jedna z prvních výzev na IROP bude totiž na tzv. úplné elektronické podání. Na základě analýzy toho, co je v rámci jednotlivých resortů již dnes realizováno, je podle něj možné říci, že skutečně není podání jako podání. Proto by chtěl demonstrovat, jak vypadá architektonický model úplného elektronického podání. Problém je podle Petra Kuchaře v tom, že podíváme-li se na to, co a jak funguje na webu generálního finančního ředitelství a porovnáme to s tím, co funguje na webu MPO a případně ČSSZ, pak zjistíme, že každá z těchto institucí realizovala podání jinak. Petr Kuchař proto prezentoval schéma, které vysvětluje, že úplným elektronickým podáním se myslí toto (v případě portálového řešení, protože i nadále je možné podání realizovat listinnou podobou prostřednictvím klasické pošty, e-mailu či datovou schránkou):

1. na začátku musí být vždy autentizace, to znamená, že člověk přistoupí na portál a autentizuje se prostřednictvím datových schránek, v budoucnu pak díky eIDAS i například elektronickým občanským průkazem, časem možná i prostřednictvím identitních providerů dalšího typu (to je ale otázkou dalšího jednání);
2. po přihlášení si občan vybere životní situaci, pro kterou potřebuje konkrétní podání realizovat;
3. v rámci životní situace si vybere konkrétní formulář a začne vyplňovat;
4. jako přihlášenému se některé údaje předvyplní automaticky, následně jako uživatel doplní, či upraví některé informace;
5. následuje část validace dat, a protože některá podání se zpracovávají dlouho, je možné tuto část kdykoliv uložit, znovu otevřít a pokračovat;
6. PDF otisk toho, co občan vyplnil – vizuální porovnání;
7. v případě, že souhlasí občan s vizuální formou, realizuje podání – odeslání OVM (DS nebo prostřednictvím AIS, to je v případě, že občan nemá svoji datovou schránku).



Všechna nová podání by měla být již postavena podle tohotu schématu.

Microsoft Azure

Microsoft Azure sdílené služby

Efektivní nástroje pro váš úřad

Zjednodušte správu a provoz IT ve vašem úřadu! Využijte cloudové služby Microsoft Azure pro efektivnější práci. Rychle vytvářejte, nasazujte a spravujte aplikace, využívejte obrovské úložiště pro svá data. Přitom platťte pouze za to, co využíváte.

Výzvy současného IT pro veřejnou správu

- **Vysoké požadavky na rychlost a kapacitu IT služeb** bez nárůstu nákladů.
- **Omezený rozpočet** navzdory rostoucím nárokům úřadů.
- **Přísné požadavky legislativy** při správě a provozu osobních údajů.
- **Potřeba rychle implementovat informační systém**.
- **Omezené možnosti veřejné právy na zaměstnání IT odborníků.**

Řešení s využitím cloudových služeb Microsoft Azure

- Platťte pouze za to, co využijete. Neinvestujte do nevyužitého hardwaru.
- Díky automatickému škálování běží vaše aplikace neustále i v čase extrémních zátěží.
- Splňte požadavky bezpečnostních politik a buďte v souladu s EU legislativou.
- Využijte stejné nástroje pro správu a monitoring napříč cloudem, HW i aplikacemi.
- Snadno přiřazujte kapacitu a optimalizujte náklady.

Vyšší bezpečnost za nižší náklady

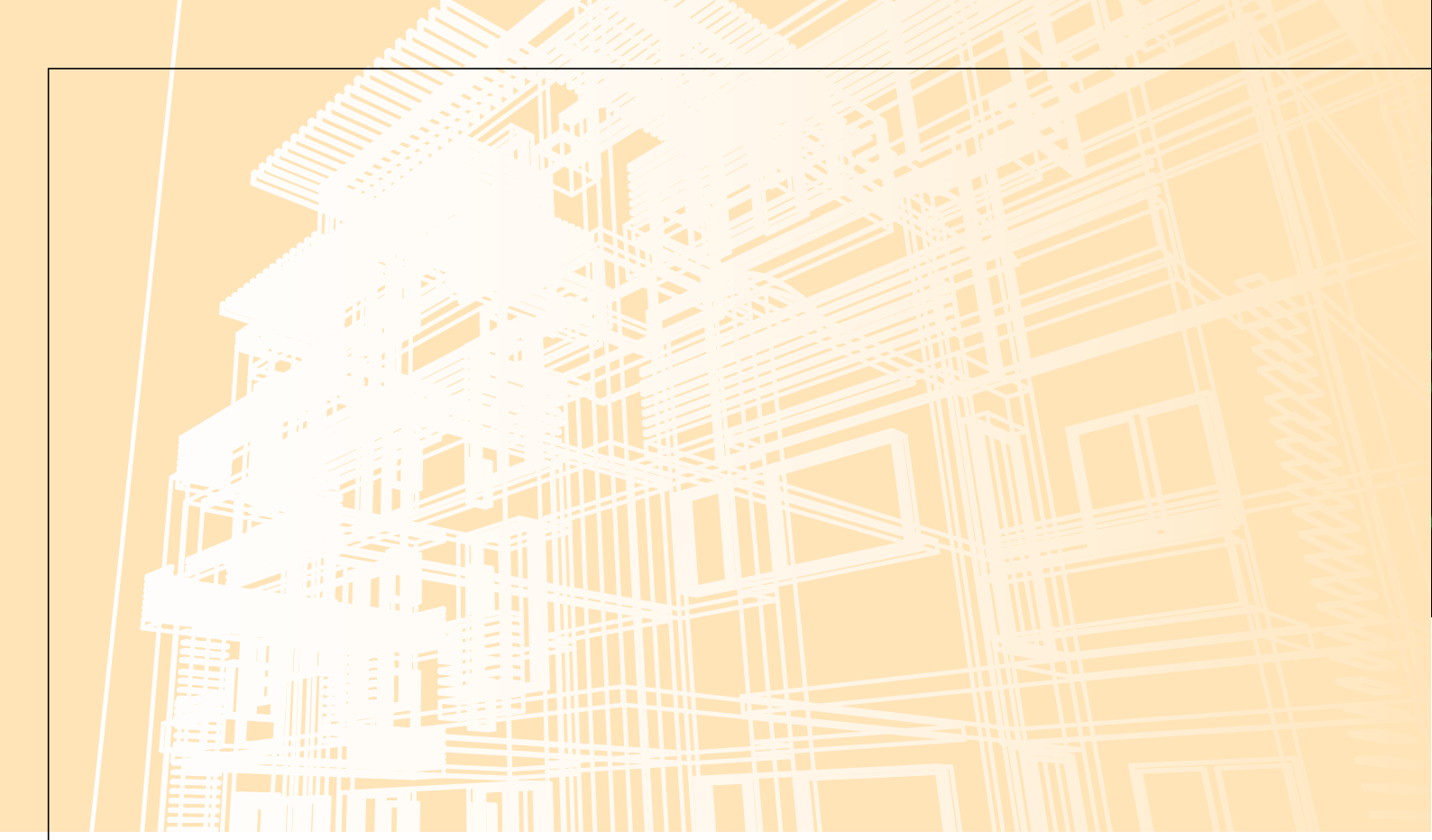
- Zajistěte bezpečný přístup k vašim aplikacím odkudkoliv, i z mobilních zařízení.
- Získejte automaticky 6 kopií geograficky oddělených dat.
- Využijte levné úložiště pro archivní a méně využívaná data.
- Díky řízenému a automatizovanému disaster recovery udržujte vaše aplikace neustále v chodu.
- Zrychlete nasazování nových služeb. Pracujte v multiplatformním prostředí.

Soulad s předpisy a certifikace

Cloudové služby Microsoft Azure získaly maximum možných certifikací a svým zákazníkům nabízí takové smluvní podmínky včetně „Smlouvy o zpracování dat" se zahrnutím standardních smluvních doložek („EU Model Clauses"), které podpoří splnění podmínek zákona č. 101/2000 Sb. o ochraně osobních údajů.

Výhody otevřené platformy a služeb

CentOS · openSUSE · ubuntu · Java · Node.js · Hadoop · OpenLogic · ORACLE · cleardb · Python · CANONICAL · mongolab · php



PERSONÁLNÍ PORTÁL

Roman Vrba přiblížil svým vystoupením Interaktivní personální portál (PePo). Je to jeden z projektů, který zažil mnoho kotrmelců, ale nyní se dá říci, že se blíží k úspěšnému dokončení. Projekt je striktně určen pro samosprávu, tedy obce 1., 2. a 3. typu, a zejména pro starosty, tajemníky a personalisty. I když se jedná o projekt, který nabral velké zpoždění, může podle Romana Vrby výrazně pomoci v případě, že budou umístěny správné informace na jednom místě na jednom portále. Konkrétně se jedná o informace typu akreditace, vzdělávání, hodnocení, zaměstnanecké záležitosti a platy, katalog prací a burza práce atp. Cílem tohoto projektu je totiž vytvoření metodického nástroje a podpory efektivity rozvoje a řízení lidských zdrojů ve veřejné správě.

PROCESNÍ MODELOVÁNÍ VE VEŘEJNÉ SPRÁVĚ

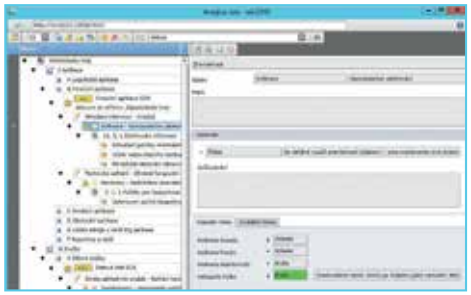
Bylo téma pro Romana Fišera. Pokud má použít již řečený příměr o přístupu k budování ICT a běžné stavby, pak v oblasti procesního modelování jsme dle jeho mínění začali ten dům stavět od střechy, ale nyní již naštěstí máme ponětí o tom, jaké budou základy. A právě o tom bylo jeho vystoupení. Jak Roman Fišer uvedl, umíme modelovat agendy na vysoké úrovni, dělat sofistikované standardy agend, ale důležité je, co se stane ve chvíli, kdy se takový standard dostane na úroveň úřadu. Tedy, jak se bude chovat úředník, zda přijme takto definovanou práci. Bude schopen ji překlopit do skutečně efektivního výkonu a v dobré služby občanovi? Aby toto bylo možné zjistit, bylo nutné najít úřad, který by umožnil celý postup ověřit a který by byl schopen absorbovat takový standard již dnes. Tím úřadem je MÚ Břeclav, který v letošním roce zavedl integrovaný systém řízení, který je zaměřen na procesy, kompetence a ukazatele. Jak Roman Fišer řekl, vypadá to, že celý standard agendy nebude problém do Břeclavi implementovat. Základním východiskem je Strategický rámec rozvoje veřejné správy. I na úrovni konkrétního obecního úřadu je nutno řešit řadu problémů, které ani dnes ještě nejsou obsahem PMA, ale vždy je možné najít takový bod v jednom z pilířů globální strategie. Podle Romana Fišera jsou rovněž velice důležité výsledky PMA, které sice mají sice různou pověst, ale metodika modelování agend je plně použitelná. Momentálně se využívá k pilotnímu projektu agendy 121 – živnostenské podnikání a podle této metodiky jsou rovněž upřesňovány požadované ukazatele výkonnosti a prováděny pilotní měření na třiceti vybraných městských a obecních úřadech. Výsledkem by měl být standard agendy, který by měl mít procesní část (co má být děláno a v jaké podobě) a výkonovou část (jak bude měřeno, že skutečně pracujeme dobře). Smyslem měření na jednotlivých úřadech je podle Romana Fišera stanovit požadované hodnoty, které potom budou doporučovány pro jednotlivé typy úřadů tak, abychom byli schopni posoudit, jestli jejich výkon je efektivní a také jaké náklady agenda vlastně stojí.

SAAR SP

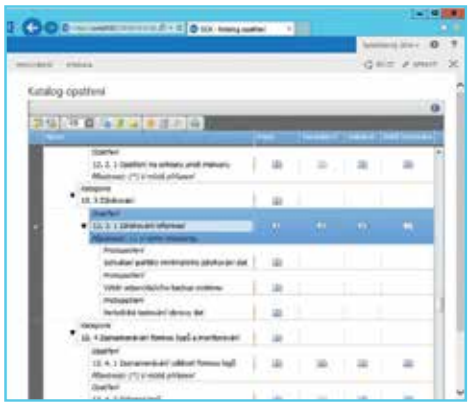
Softwarový nástroj pro správu bezpečnostních rizik a informací

Softwarový nástroj **SAAR SP** je určen k řízení bezpečnosti informací. Podporuje přípravu, zavedení a provoz ISMS dle normy ČSN ISO/IEC 27001:2014 a je plně v souladu s Kybernetickým zákonem. Základní koncept **SAAR SP** vychází z potřeb dvoustupňového řízení informační bezpečnosti.

Stupeň **Globální řízení** usnadňuje celoplošné zavedení politik informační bezpečnosti, uplatňuje principy jednotné identifikace, ohodnocení a zvládání rizik, zavádí jednotný způsob řízení dokumentace, plánování a vyhodnocování interních auditů a zpětně ověřuje účinnost přijatých opatření.



Stupeň **Lokální řízení** umožňuje vlastní výkon řízení rizik a informační bezpečnosti v konkrétních podmínkách jednotlivých organizací nebo jejich částí, v rozsahu uplatněných globálních pravidel a podmínek.



Nástroj **SAAR SP** je provozován na platformě Microsoft Sharepoint 2013 (od verze Foundation a vyšší).

Hlavní výhody

- jednotná politika řízení rizik a bezpečnosti informací
- možnost plošného řízení s uplatněním lokálního řízení
- víceúrovňová kontrola a grafické výstupy
- online přehled o rizicích a jejich vazbách na sdílená aktiva
- podpora ISMS, auditů a na jejich základě přijatých opatření

Kontakt

Luboš Nejedlý, lubos.nejedly@ts.fujitsu.com, tel. +420 724 592 231

fujitsu.cz

shaping tomorrow with you

FUJITSU

CO SE DĚJE V BŘECLAVI?

V Břeclavi byly převedeny procesní standardy (diagramy) z PMA do interních procesů úřadu. Zároveň byly částečně upraveny, protože každý úřad má svoje specifika. Následně byly tyto standardy propojeny přímo do pracovních náplní úředníků. Přitom bylo, jak řekl Romana Fišer, nutno zohlednit skutečnost, že jeden úředník neřeší vždy pouze jednu agendu, ale více agend, a to jak v přenesené, tak v samostatné působnosti. Bylo tedy nutno provést systemizaci rolí, která umožní identifikovat konkrétní výkon vůči agendě a následně jej i ocenit ve vazbě na alokovaný úvazek. Ve spolupráci s vedením úřadu diskutoval ÚHA o sestavě ukazatelů, tedy o tom, co je vhodné měřit a reportovat. Nakonec byla původně zamýšlená sestava podělena třemi. Jde tedy víceméně jen o třetinu původně navrhovaných úřadů, aniž by přitom bylo ovlivněno to, jakým způsobem agendu měříme, nebo hodnotíme. Podle Romana Fišera bylo ověřování těchto modelů na nižší úrovni přínosem.

V současnosti jsou již zaváděny výkonnostní modely úředníků. Ze standardních ukazatelů bylo vybráno pět, které jsou uplatnitelné na úrovni výkonu jednoho jediného úředníka. Ty budou navázány i na aplikaci dobrý úřad. V jejím rámci se občané přímo vyjadřují ke kvalitě práce konkrétních lidí – úředníků. Nad rámec PMA byly realizovány kompetenční modely úředníků, což jsou vlastně sady znalostí a dovedností, které úředník potřebuje k výkonu agendy. Byly do nich zahrnuty i tzv. měkké dovednosti, například zvládání konfliktních lidí atp. Toto podle Romana Fišera vzniklo nad rámec standadru a cílem je, aby se tzv. měkké dovednosti staly jeho součástí. Tím, že na základě rolí bylo možné alokovat přesný díl pracovního času na agendu, vznikl podle Romana Fišera dobrý základ pro vytvoření procesního nákladového modelu agendy a tím i pro výpočet úhrady.

CO NAS ČEKÁ?

Jak Roman Fišer uvedl, nyní bude nutné realizovat modelování 60 agend a také standardizace. Pokud se vžijeme do kůže a situace úřadů, pak pro ně to patrně znamená až desítky agend, které budou muset ročně implementovat do svého života. Pro pracovníky ÚHA je podstatné, jak vypadá systém řízení úřadu jako celku, ne jenom jedné agendy. Proto ÚHA chce úřadům pomáhat systémy vytvářet, radit jim, jak postupovat a ukazovat řešení a současně zprostředkovat komunikaci mezi gestory, metodiky a úředníky, respektive úřady jako takovými. To je vlastně výzvou do budoucna. V současné době chybí sice sdílený systém kvality, ale pracuje se na něm. Cílem přitom je, aby nebyl zaměřen jen jednu úzkou oblast, ale aby šel napříč všemi pilíři Strategického rámce rozvoje veřejné správy.

CENTRÁLNÍ NÁKUP SOFTWAROVÝCH PRODUKTŮ

Miroslav Tůma, jehož odbor se na MV ČR věnuje dvěma klíčovým oblastem – kybernetické bezpečnosti a koordinaci ICT, se nevěnoval důležitosti bezpečnosti, ale soustředil se na centrální nákupy, kde je rozhodně čím se pochlubit. Miroslav Tůma uvedl, že je nutné, aby projekty, které zde byly již prezentovány, na něčem fungovaly a na něčem byly vytvářeny. Právě proto je důležité zajistit správný software a zajistit jej efektivně. A jak uvedl, když už je ministerstvo zajišťuje, tak pokud možno pro celou veřejnou správu, nikoli pouze pro MV ČR.

Jedním z prvních bodů v tomto směru bylo podepsání rámcové smlouvy na dodání produktů Microsoft. Ta byla podepsána 1. 12. 2014. Po devítiměsíčním zkoušení a běhu je možné prezentovat výsledky, kterých bylo dosaženo v oblasti úspor a které vycházejí z řešení rámcové smlouvy. Ta, jak zdůraznil, navazuje na strategické smlouvy podepsané na úrovni vlády a je zaměřena na základní oblasti, to znamená na oblast nákupu select enterprise, potažmo software assurance, a rovněž i poskytování bezplatných služeb, které jsou doprovodné k předmětům smlouvy. Jak Miroslav Tůma řekl, rámcová smluva v sobě definuje prováděcí smlouvu, následně bylo vybráno pět dodavatelů, mezi kterými pak pro pozici konkrétního poskytovatele probíhají minitendry na úrovni jednotlivých dodávek. Tyto minitendry jsou automaticky realizovány v rámci elektronického portálu navázaného na elektronické tržiště, jehož prostřednictvím dochází ke konkrétní soutěži na zadavatele.

Podle Miroslava Tůmy je podstatné, že rámcová smlouva garantuje slevy pro program enterprise ve výši 19–22%, pro select 17–25%, což jsou základní slevy vysoutěžené v rámci rámcové smlouvy. Pro jednotlivé minitendry jsou dosahovány slevy ještě vyšší – v oblasti enterprise 26 %, v oblasti select 25 %. Jak Miroslav Tůma zdůraznil, jedná se o necelou stovku minitendrů, které proběhly za uplynulých devět měsíců. Z toho vyplývá i to, že MV je připraveno a nyní představilo celý portál pro jednotlivé

zadavatele tak, aby si oni mohli tyto minitendry provádět sami, a to nejen pro smlouvu a dodávku produktů Microsoft, ale jsou připravovány i další smlouvy. Konkrétně se jedná o dodávku VMware (měla by být vyhlášena v polovině září) a následně Oracle, který bude vyhlášen patrně na počátku roku. Znamená to tedy, že jsou připraveny další rámcové smlouvy na dodávku produktů jednotlivých dodavatelů tak, aby bylo možno stavět správné projekty. V případě zájmu o informace k tendrům a smlouvám uvedl Miroslav Tůma následující kontakty:
pro Microsft: **cnsw.ms@mvcr.cz**,
pro Oracle: **cnsw.or@mvcr.cz**
a pro VMware: **cnsw.vm@mvcr.cz**.

CO JSME UDĚLALI?

Roman Vrba se ještě v závěru tohoto prezentačního bloku ptal, co bylo uděláno nejen pro veřejnou správu, ale především pro lidi, tedy pro koncové klienty. Jak řekl, jedná se o taková drobná, malá vítězství. Ve spolupráci s Ministerstvem dopravy byl vydán nový formulář pro czechpoitn@home, a to výpis z bodového hodnocení řidiče. Je to zcela nový formulář, který byl spuštěn 2. 9. 2015 a který funguje pouze pro držitele datových schránek. Výpis pořízený touto cestou je ovšem zdarma oproti fyzickému vyřízení na Czech POINTu.
Další zajímavou aplikací je mobilní aplikace Co dělat, když? Oproti jarnímu představení byla nyní rozšířena a snaží najít cestu k lidem poněkud přístupnější formou tak, aby jednotlivé životní situace nebyly popisovány strohým úřednickým jazykem. Aplikace je rovněž schopna nabídnout nejbližší kontaktní místo i s otevírací dobou, popřípadě mapou, jak se k němu dostat tak, aby bylo možné vše potřebné vyřídit.
Podle Romana Vrby se na aplikaci stále pracuje. Budoucností by měl být stav, kdy bude k dispozici databáze úřadoven, tedy skutečných míst, kde se daná agenda vykonává. Problém je v současnosti podle Romana Vrby v tom, že nyní nám aplikace sice nabídne informaci o tom, že určitou agendu je možné vyřídit na konkrétním úřadě, ale získáme pouze adresu sídla tohoto úřadu, ale nikoli například konkrétní budovu v rámci úřadu. To bývá leckdy, především ve větších městech, dosti problematické.
Poslední, na co chtěl Roman Vrba upozornit, je skutečnost, že nyní je na Czech POINTu, kromě výpisu z katastru nemovitostí, možné získat i ověřený snímek katastrální mapy (je tomu tak od srpna), je to vlastně první grafický výstup v rámci CZP.

Role MV v oblasti eGOVERNMENTU v programovém období 2014 – 2020

Jak v úvodu svého vystoupení řekl náměstek ministra vnitra pro řízení sekce ekonomiky, strategií a evropských fondů Mgr. Jiří Zmatlík, slyšeli jsme, jaké jsou plány do budoucna, co by se mělo realizovat a jakým způsobem, ale zůstává otázka, z čeho bude taková realizace placena. Plány jsou podle jeho mínění úžasné, ale protože v reálném světě všechno něco stojí a systémy IT a obecně oblast informačních technologií je poměrně nákladná záležitost, hovoříme o realizaci velice drahé. K jejímu financování nám mohou pomoci evropské fondy. Jak zdůraznil, pomáhají nám již v dalším programovém období. Nyní, v tomto roce, již končí programové období 2007 – 2014 a navazuje na něj nové programové období 2014 – 2020.

V minulém programovém období mělo podle Jiřího Zmatlíka Ministerstvo vnitra, o něco silnější pozici ve vztahu k fondům. Bylo zprostředkujícím subjektem a jako takové v podstatě bylo i poskytovatelem dotace. Nyní se ale jedná o nové programové období, a tedy i novou funkci nebo činnost Ministerstva vnitra, kterou v jeho průběhu bude vykonávat. Jde tedy o to ujasnit si, že se role MV ČR změnila a že mnohdy jsou jeho pracovníci kontaktováni s dotazy kvůli realizaci projektů, ale dotazy by měly být směrovány na jiný subjekt.

Pokud jde o operačních programy, ze kterých bude možné financovat e-government, tak stejně jako v minulém programovém období i nyní jsou k dispozici dva fondy. Jedním z nich je operační program zaměstnanost (OPZ) a druhým z nich je integrovaný regionální operační program (IROP). IROP je zaměřen na tzv. tvrdé projekty. Operační program zaměstnanost se věnuje tzv. měkkým projektům. Jiří Zmatlík považuje za velice důležitou existenci určité vize toho, co je možné z těchto fondů financovat. Takovým dokumentem je Strategie rozvoje veřejné správy a e-governmentu, která byla schválena minulý rok. Letos v létě k němu přibyly implementační plány, které v podstatě rozpracovávají jednotlivé činnosti v rámci strategického rámce. V souvislosti s e-governmentem je zejména důležitý implementační plán číslo 3, který obsahuje karty projektových záměrů, okruhů, které lze v rámci strategického rámce realizovat a na které je vhodné se při snaze čerpat dotace z těchto fondů zaměřit.

INTEGROVANÝ REGIONÁLNÍ OPERAČNÍ PROGRAM (IROP)

Řídícím orgánem IROP je Ministerstvo pro místní rozvoj a to má jeden zprostředkující subjekt, kterým je CRR – Centrum pro regionální rozvoj. V minulém programovém období tímto subjektem bylo právě MV ČR, CRR, dále i Ministerstvo zdravotnictví a Ministerstvo kultury. MMR tedy na sebe nyní bere obrovskou odpovědnost, neboť bude realizovat a vypisovat výzvy na odborná témata, s nimiž v zásadě nemá ani podle kompetenčního zákona nic moc společného. Jiří Zmatlík se domnívá, že to bude pro MMR velice obtížná situace. I proto by mělo být zřetelně zviditelněno, že nyní leží tato odpovědnost na MMR.

Na specifický cíl 3.2, prioritní osy 3, který se v rámci IROP týká tématu e-governmentu je k dispozici 8,9 miliardy, což je 7 % z celého IROPu. Podle analýzy celkových požadavků je absorbční kapacita v této oblasti zhruba 18 miliard. I když částka, která je k dispozici, není malá, zdaleka podle Jiřího Zmatlíka nepokrývá současné potřeby.

První výzvy v rámci IROPu budou vypisovány v září, zřejmě na úplné elektronické podání. V říjnu pak bude následovat výzva na kybernetickou bezpečnost.

Jiří Zmatlík následně uvedl příklady projektů, které mohou být v rámci IROP realizovány:

- Projekty z oblasti e-governmentu, infrastruktury a informačních a komunikačních systémů veřejné správy v rozsahu rozšíření, propojení, konsolidace systémů, aplika-

cí a datového fondu (včetně jeho publikování) veřejné správy (včetně cloudových řešení);
- Modernizace informačních a komunikačních systémů pro specifické potřeby subjektů veřejné správy a složek IZS;
- Vznik a vybavení orgánů veřejné moci pro ochranu infrastruktury IKT a zajištění řízeného a bezpečného sdílení dat veřejné správy v souladu se standardy kybernetické bezpečnosti, včetně komunikační a radiokomunikační infrastruktury státu.

Především poslední odrážka je velmi závažné téma, kterému se zřejmě budeme věnovat následujících pár let – kybernetická bezpečnost, tedy zajištění infrastruktury tak, aby nebyla napadnutelná.

OPERAČNÍ PROGRAM ZAMĚSTNANOST (OPZ)

Řídícím orgánem operačního programu zaměstnanost je MPSV, které nemá žádný zprostředkující subjekt. Poskytovatelem dotace je tedy přímo MPSV. Alokace je v tomto případě o něco nižší, konkrétně 3,5 miliardy a směřuje do tzv. měkkých projektů. Tedy zejména do zlepšení lidského kapitálu, lidských zdrojů. Dále, v případě úřadů, do zlepšení komunikace uvnitř i navenek, případně zkvalitnění různého strategického řízení. Z tohoto programu je možné financovat různé evaluace a analýzy, které by měly být podkladem například pro další realizování projektů v rámci IROPu.

První výzva v rámci OPZ již byla vypsána, nicméně tato první výzva se nevztahuje vůbec k e-governmentu. E-governmentu se bude věnovat druhá výzva, která bude soutěžní a měla by podle Jiřího Zmatlíka být vypsána v září. Jedná se ovšem o výzvu, která bude mít určité limitující parametry. Tím limitem je maximální výše dotace – 50 milionů Kč. Podle náměstka Zmatlíka to bude pro některé žadatele o dotace velmi kritické. MPSV k tomu ovšem má poměrně logický důvod, protože v minulosti byly naopak realizovány velké projekty, které byly velmi komplexní. Realizovala se sice v rámci nich celá řada aktivit, ale projekty nebyly dokončeny. Tím vznikl problém, že nebyla vyčerpána poměrně velká alokace. Proto se nyní MPSV snaží nasměrovat žadatele tak, aby nedělali velký komplexní projekt, ale jednotlivé aktivity samostatně.

SPOLUFINANCOVÁNÍ

Oproti minulému programovému období se rovněž poněkud změnila míra spolufinancování, především u organizačních složek státu a dalších státních organizací, státních podniků. Nedosahuje nyní oněch 85 %, na které jsme byli zvyklí, ale necelých 81%. U územních samosprávních celků oněch 85 % zůstalo zachováno s výjimkou Prahy, která je dle Evropské komise bohatá. Územně samosprávní celky mohou ještě počítat s 5% příspěvkem od státu a vlastními prostředky tak budou muset zajistit pouze zbylých 10 %. MV ČR má v tomto směru roli tzv. věcného garanta. Jak náměstek Zmatlík uvedl, dlouhodobě si s jednotlivými řídícími orgány vyjasňovali, co to vlastně bude znamenat, jak se budou moci podílet na jednotlivých operačních programech a jakým způsobem budou moci zasahovat do rozdělování finančních prostředků na jednotlivé projekty. Nakonec podle jeho slov k určitým dohodám došlo – s MMR existuje dohoda, která byla schválena usnesením vlády, s MPSV byla podepsána dohoda o spolupráci v červnu. Ta obsahuje podmínky, práva a povinnosti, které jako věcný garant MV ČR má. Ministerstvo vnitra se tak u obou programů bude věnovat především nastavování výzev, případně bude dávat i u OPZ nezávislá stanoviska. U IROPu zůstává jako zásadní stanovisko hlavního architekta.

Role hlavního architekta e-governmentu je podle Jiřího Zmatlíka jednou z nejdůležitějších věcí. Organizační složky státu musí žádat o stanovisko ÚHA. Územní samosprávy musí žádat o stanovisko v případě, že se jedná o projekt nad 15 milionů korun. Architekt pak posuzuje zejména, zda je projekt v souladu se strategických rámcem a zda je v souladu s architektonickým plánem.

KONTAKTY

Na závěr svého vystoupení Jiří Zmatlík uvedl kontakty, na nichž je možné získat informace týkající se role Ministerstva vnitra jako věcného garanta:

Informace k IROP naleznete na:
http://www.strukturalni-fondy.cz/cs/Microsites/IROP/Uvodni-strana

Informace k OPZ naleznete na:
http://www.esfcr.cz/op-zamestnanost-2014-2020

V případě dalších dotazů se obracejte na:

1) ŘO IROP/OPZ, irop@mmr.cz/esf@mpsv.cz
2) Samostatné oddělení strategií a ESIF Ministerstva vnitra
   Mgr. Jana Menšíková, vedoucí oddělení
   E-mail: jana.mensikova@mvcr.cz, tel.: 974 833 324
   Sekretariát:
   E-mail: olga.vikturnova@mvcr.cz

Možnost financování e-governmentu a kybernetické bezpečnosti z integrovaného regionálního operačního programu v programovém období 2014 – 2020

Podle Aleše Pekárka je současná situace poněkud schizofrenní, neboť MMR je sice zodpovědné za program, ale následně jej uvádí MV a s tím bude nutné se v průběhu celého programového období poprat. Jak ale doufá, obě ministerstva spolu budou úspěšně spolupracovat na tom, aby se neopakovala situace v IOPu, kde vznikly určité problémy právě s čerpáním dotací. Aleš Pekárek představil IROP, který byl schválen v červnu 2015, tedy docela pozdě, a tak času není skutečně nazbyt. Celková alokace v tomto programu činí přes 4,5 mld. EUR, což je i s kofinacováním skoro 150 mld. Kč. Jedná se skutečně o velké množství peněz, za jejichž rozdělování je nyní zodopovědné MMR. Řídicím orgánem je Ministervo pro místní rozvoj, odbor řízení operačních programů. Kofinacování těchto projektů je většinou ve formátu 85% z evropských fondů a 15% financuje stát. Jediný rozdíl bude ve specifickém cíli 3.2.

IROP se dělí na čtyři prioritní osy:

1. **infrastruktura** (doprava silnice, ekologické autobusy);
2. **lidé** (mateřské školy, sociální služby, ale i paradoxně zateplování bytových domů atp.);
3. **dobrá správa území a zefektivnění veřejných institucí** – krom e-governmentu, což je specifický cíl 3.2, obsahuje rovněž podporu kulturního dědictví a podporu územně plánovací dokumetace u obcí s rozšířenou působností;
4. čtvrtá prioritní osa jde v podstatě napříč celým operačním programem a budou z ní podporovány místní akční skupiny, ty však budou mít trochu jiný režim kofinancování.

Role MMR ČR a Centra pro regionální rozvoj

Jedná se o řídicí orgán programu, který připravuje výzvy a pravidla pro žadatele i příjemce a je poskytovatelem dotace. Evropská komise žádala zjednodušení programového období. Minulé jsme si nastavili poněkud složitě – měli jsme příliš mnoho operačních programů, podle slov Aleše Pekárka patrně nejvíce z evropských států. Jak uvedl, tomu odpovídal i vývoj, když jsme minulé programové období prožívali dosti chaoticky. Na základě přání EK i našich zkušeností byl nyní určen pouze jeden zprostředkující subjekt, a to právě Centrum pro regionální rozvoj. CRR bude konzultovat jednotlivé projektové žádosti, přijímat, hodnotit, kontrolovat a administrovat veškeré změny i celé projekty. CRR už nyní disponuje poměrně velkým množstvím odborníků, kteří rozhodně zvládnou tyto projekty administrovat lépe, než tomu bylo v uplynulém programovém období.

PRAVIDLA

Pro žadatele a příjemce dotací je k dispozici následující model: existují obecná pravidla, která jsou závazná pro všechny specifické cíle a pro všechny výzvy. Zároveň bude ale pro každou výzvu vydán samostatný dokument, který je stručnější (specifická pravidla) a v něm budou upřesněny náležitosti konkrétní výzvy. Jedná se o krok směrem ke zjednodušení.

SPECIFICKÝ CÍL 3.2

V rámci tohoto cíle jde o e-government. Alokace v rámci cíle 3.2 činí 330 mil. EUR, tedy téměř 9 mld. Kč. Tento cíl má tři následující pilíře:

- **rozvoj e-governmentu** (e-justice, e-kultura ...);

- **specifické informační systémy pro IZS** a takové, které nepatří k těm e-systémům. Zde bude ještě dořešeno, jaké specifické informační systémy by mohly být do této oblasti zahrnuty;
- **kybernetická bezpečnost** zahrnuje zhruba třetinu uvedené alokace. Budou se zabezpečovat především významné a kritické informační systémy veřejné správy.

Příjemci jsou organizační složky státu, příspěvkové organizace organizačních složek státu, obce, organizace zřizované nebo zakládané obcemi, kraje, organizace zřizované nebo zakládané kraji, státní organizace. U akciových společností a s.r.o., pokud je kraj nebo obec mají založené, platí, že taková organizace nemůže dostat ze státního rozpočtu kofinancování. To znamená, že 85% dostane z evropského regionálního fondu a 15% si musí organizace zaplatit sama.
Důležité je, že posuzování v rámci specifického cíle 3.2 je navázáno na indikátory. Nejdůležitějším indikátorem je pořízení informačního systému, jakýkoliv podaný projekt musí tedy mít náležitost informačního systému. Může se jednat o nový – nově pořízený, nebo upravený stávající IS. Rozhodně nebude podporován pouze nákup hardware bez vazby na nějaký nový či upravený informační systém. Informační systém sám o sobě ovšem nebude stačit. Dalším indikátorem je nová funkcionalita. Přitom je důležité, aby tento informační systém měl minimálně tři nové funkcionality.

Například se jedná o:

- samoobslužný proces veřejné správy;
- propojování datového fondu veřejné správy;
- zajištění provozní spolehlivost a bezpečnosti;
- dostupnost služeb veřejné správy;
- interoperabilita na území státu s přesahem v rámci EU;
- celoplošná dostupnost.

Všechny funkcionality jsou uvedeny v tzv. metodickém listu indikátoru. Zároveň je možné vymyslet i novou funkcionalitu. Tu by pak posuzoval Útvar hlavního architekta, a pokud dá souhlasné stanovisko, je možné takový projekt posunout do další fáze hodnocení.
Projekty musí být v souladu se Strategickým rámcem rozvoje veřejné správy České republiky 2014+ a jeho implementačními plány a okruhy. Těch projektových okruhů je celkově 15 a je to docela široký záběr. Je tedy, podle Aleše Pekárka, dobré se při přípravách podívat na projektové okruhy, jak jsou v projektových kartách rozepsány, a navázat na ně svůj projekt. Krom toho bude ještě nutno doložit souhlasné stanovisko hlavního architekta. To se týká všech projektů nad 15 milionů korun celkových způsobilých výdajů, všech projektů organizačních složek státu a pak všech projektů pod 15 milionů korun, které jsou vázány na centrální systémy státní správy. Je to v podstatě většina projektů z 3.2, ale je možné si představit projekt, u kterého takové stanovisko nebude potřeba.

KONKRÉTNÍ VÝZVY

17. září – výzva Aktivity vedoucí k úplnému elektronickému podání

Jedná se o výzvu, na které spolupracovalo MMR a MV a byla doporučena RVIS. Podle rady vlády je toto téma velice prioritní. MMR doporučení rady vyslyšelo a vyhlásilo výzvu, která bude průběžná a otevřená až do roku 2017. Alokuje zatím 0,5 mld. Kč, neboť není zcela jasné, kolik takových projektů vlastně bude. Odhadovaná absorbční kapacita je skutečně pouze určitým odhadem úředníků. Jako řídicí orgán se na výzvu MMR musí dívat objektivně a po zkušenostech z IOPu víme, že řada projektových záměrů nakonec nebyla realizována, ať již z důvodu voleb, fluktuace zaměstnanců či řady dalších. Pokud by o tuto výzvu byl zájem a projekty byly smysluplné, není podle Aleše Pekárka problém ji navýšit. Výzva je v souladu s projektovými okruhy 3.1 a 3.2 úplné elektronické podání a kontaktní místa a příjemci jsou všichni, kteří jsou obsaženi ve specifickém cíli 3.2., tedy organizační složky státu, příspěvkové organizace organizačních složek státu, obce, organizace zřizované nebo zakládané obcemi, kraje, organizace zřizované nebo zakládané kraji, státní organizace.

Podporované aktivity v rámci výzvy jsou zatím rozepsané MV ČR, MMR se je bude snažit ještě zpodrobnit, tak, aby se úkoly/aktivity více upřesnily:

- vytvoření podpůrných služeb pro úplné elektronické podání;

- vytvoření samoobslužného místa pro subjekt práva v české i anglické verzi, prostřednictvím kterého bude možné realizovat úplné elektronické podání;
- elektronizace formulářů veřejné správy a zajištění anglické verze;
- zajištění úplného elektronického podání;
- implementace identifikace a autentizace pomocí identifikačních prostředků ve smyslu nařízení eIDAS pro využívání služeb e-governmentu prostřednictvím kontaktních míst;
- podpora sdílení identitních služeb na národní a regionální úrovni;
- vytvoření bezpečného mechanismu poskytování a využívání údajů jako součást referenčního rozhraní ISVS z jednotlivých agendových systémů v návaznosti na referenční údaje základních registrů s využitím funkcionality EgonServiceBus;
- vytvoření mechanismu pro odstraňování nekonzistencí nereferenčních údajů o subjektech práva v jednotlivých agendových systémech.

Další velice důležitá výzva, která by měla být vyhlášena v říjnu (cca 21. 10.), je **výzva Kybernetická bezpečnost.**
Opět se bude jednat o průběžnou, nesoutěžní výzvu, otevřenou až do roku 2017. Její alokace činí 1,5 mld. Kč. Předložené projekty musí být v souladu s projektovým okruhem č. 7 Strategického rámce, ale musí být rovněž v souladu se zákonem o kybernetické bezpečnosti. MMR jednalo s NBÚ a podle všeho bude muset mít každý projekt, který bude chtít být z této výzvy financován, i souhlasné stanovisko NBÚ. Nejpozději v momentě vyhlášení výzvy by měla být k dispozici metodika hodnocení i samotné stanovisko NBÚ. Projekty předložené v této výzvě musí být zaměřeny na systémy významné a kritické.
Jaké budou podporované aktivity? V zákoně o kybernetické bezpečnosti se píše o tzv. technických opatřeních. Opět je zde monitorovací indikátor a každé z těchto opatření je hodnota jedna monitorovacího indikátoru. Pokud si budeme chtít zabezpečit nějaký informační systém, můžeme se rozhodnout pro jedno až deset těchto technických opatření.

Podporované aktivity (technická opatření):

- fyzická bezpečnost;
- nástroj pro ochranu integrity komunikačních sítí;
- nástroj pro ověřování identity uživatelů;
- nástroj pro řízení přístupových oprávnění;
- nástroj pro ochranu před škodlivým kódem;
- nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů;
- nástroj pro detekci kybernetických bezpečnostních událostí;
- nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí;
- aplikační bezpečnost;
- kryptografické prostředky, které nejsou určeny k ochraně utajovaných skutečností;
- nástroj pro zajišťování úrovně dostupnosti informací
- bezpečnost průmyslových a řídicích systémů.

Poslední výzvu **Zvyšování efektivity a transparentnosti veřejné správy prostřednictvím rozvoje a kvality systémů IKT** opět doporučila RVIS. Tato výzva bude omezena na projekty e-legislativy a e- sbírky, které má již MV připraveny, a bude vyhlášena v prosinci. Zároveň byla k uvedeným projektům přiřazena archivace. Příjemci dotace zde budou organizační složky státu, včetně Národního archivu. Je to opět průběžná výzva, ale vzhledem k jejímu zaměření je otevřena pouze do června 2016. Její alokace je 700 mil. Kč a je zde nutný soulad s projektovými okruhy 3.3 (e-sbírka) a 3.11 (NDA).
V závěru svého vystoupení Aleš Pekárek uvedl kontakty, pokud budete mít projektový záměr a potřebu k němu získat informace:

PhDr. Aleš Pekárek, řídicí orgán IROP
E-mail: ales.pekarek@mmr.cz
Telefon: +420 224 861 571.

Zároveň ale jasně upozornil, že MMR nebudeme platit vedlejší aktivity typu projektové řízení a osobní náklady. Ta podpora je tentokráte zaměřena hlavně na HW/SW, případně nějaké stavební úpravy pro serverovny atp.

eLearning

Zítřek patří připraveným

Vzdělání odvážně vstoupilo do 21. století. Digitální didaktické pomůcky, interaktivní výuka a další inovativní nástroje zvyšující efektivitu vzdělávání jsou díky řešením společnosti Atos přístupné nejen pro školy, ale i pro firmy.

cz.atos.net

Your business technologists. **Powering progress** Atos

Z pískoviště k obraně státu. Kybernetické útoky nejsou imaginární hrozbou

V éře internetu věcí a ve stále propojenějším světě se mění i přístup ke kybernetické bezpečnosti, která už totiž dávno není jen záležitostí odborníků na IT. Současní kyberzločinci se profesionalizují, jejich útoky si hledají nové cíle a využívají nové pokročilé metody napadení. Pro státní správu i samotný stát se tak mohou stát skutečně zásadní hrozbou! Jaké jsou nové způsoby boje v kybernetické válce a jak se vyvíjejí nové bezpečnostní mechanismy a produkty, sdělil na letošním ročníku konference e-government 20:10 Petr Somol, ředitel výzkumu ve výzkumném a vývojovém centru pro oblast kybernetické bezpečnosti společnosti Cisco v Praze.

Zkuste si představit, že by kyberútočník dokázal například napadnout semafory na jedné z hlavních pražských ulic. Jak obrovské komplikace by dokázal způsobit? Jak dlouho by se z toho Praha mohla vzpamatovávat? A co kdyby se mu podařilo nějakým způsobem napadnout například spisovou službu? Kdyby dokázal změnit informace v úředních dokumentech?

Dnes se stále častěji setkáváme s pokročilými typy útoků, proti kterým je potřeba postavit i sofistikovanou obranu. Ta už nemůže spoléhat na to, že se škodlivý software podaří odhalit porovnáváním jednotlivých souborů s existujícími vzorky. Je nezbytné detailně analyzovat síťový provoz a dokázat tak rozpoznat útoky, které byly doposud neznámé, a žádný „vzorek" na ně tedy neexistuje. Vývoj přesně takových bezpečnostních nástrojů má na starosti výzkumné a vývojové centrum společnosti Cisco v Praze, které vzniklo akvizicí české start-upové firmy Cognitive Security.

Neubráníme se, ale musíme to vědět

John Chambers, který stál v čele společnosti Cisco více než 20 let, nedávno prohlásil, že firmy se dělí na ty, které již byly napadeny, a ty, které o tom prozatím nevědí. Zní to jako bonmot, ale výzkumy Cisco skutečně ukazují, že najít dnes firmu, v jejíž síti by se nějaký škodlivý kód nenacházel, je prakticky nemožné. Není třeba si dělat iluze, že by situace ve státní správě byla radikálně odlišná. Problém ale je, že pokud firma či instituce napadení nezjistí, má útočník obrovské možnosti, jak svého úspěchu využít. Nedávno publikovaná studie Cisco Midyear Security Report uvádí, že detekce takovéhoto útoku může s tradičním přístupem trvat až 200 dní. To znamená více než půlrok, kdy může útočník s napadenými počítači nakládat podle libosti. Vraťme se nyní k příkladu s napadením spisové služby, či jakéhokoli jiného elektronického archivu dokumentů.

Tradiční přístup se snažil zabránit proniknutí škodlivého kódu do sítě. Ochrana proti pokročilým hrozbám musí

ale fungovat na zcela jiném principu. Strategie společnosti Cisco hovoří o tom, že je potřeba chránit se ve všech fázích kybernetického útoku, před ním, během něj i po něm. V první fázi je důraz kladen na maximální prevenci, ve druhé na co nejrychlejší zjištění probíhajícího útoku a jeho zastavení, ve třetí pak na zjištění škod a přijetí nápravných opatření.

Zjistěte rozsah škod

V minulosti byly kybernetické útoky často dobře zaznamenatelné. Cílem útočníků bylo často i zviditelnit sami sebe a své možnosti. Profesionální útočníci dnes již ale mají značné finanční prostředky, špičkové vybavení a jejich cílem není vlastní propagace, ale čistě finanční zisk. Proto jsou jejich útoky často velmi důmyslně skryté tak, aby bylo pro bezpečnostní systémy velmi obtížné je identifikovat. Během první fáze se tak často snaží jen získat přístup k určenému počítači a instalovat do něj škodlivý kód, který jim do budoucna umožní provést další fáze útoku či přesněji samotný útok.

Tady právě přichází ke slovu ochrana před útokem, kdy se systémy snaží analyzovat běžný provoz v síti a zjistit, jestli například některé programy či aplikace nekomunikují se servery, se kterými by komunikovat neměly, nebo neodesílají nějaká data jinam, či v jiné formě, než by měly. Zkrátka, je třeba zachytit podezřelé chování.

Obvykle v okamžiku, kdy se napadený počítač podaří zpeněžit na černém trhu, zahájí kyberzločinci samotný útok. Může jít například o snahu získat data ze serverů, ke kterým je počítač připojen a využít ho jako jakéhosi trojského koně. Právě v tomto okamžiku již může být ohrožena kritická infrastruktura. A je vlastně trochu jedno, na jakém místě se útočníci rozhodnou udeřit. V této chvíli je proto potřeba útok v síti okamžitě detekovat a – pokud možno automaticky – určit příslušná opatření k zamezení jeho šíření. V podstatě to znamená, že během útoku by měl být systém schopen například odpojit konkrétní počítače či celý segment počítačů od zbytku sítě, či jim zabránit v přístupu na servery, na něž je útok veden.

I v případě, že útočníci sami svou činnost v síti ukončí, nebo zafungují bezpečnostní systémy a dokáží ho přerušit, práce ani zdaleka nekončí. Nyní musí nastoupit velmi důkladná analýza způsobených škod. Jde samozřejmě o to zjistit, k jakým datům kyberzločinci získali přístup, jaká data poškodili, případně jaká mohli pozměnit. Napadené firmě, či instituci totiž vždy hrozí ztráta důvěryhodnosti jejích dat. To může být skutečně velké riziko.

I proto se stává, že týmy bezpečnostních analytiků, jako ty, které působí ve výzkumném a vývojovém centru Cisco, jsou povolány do firem, které si útok uvědomí až po jeho skončení, případně jej zaznamenají, ale již mu nedokážou zabránit. Zjištění rozsahu škod a obnovení důvěry je totiž naprosto klíčovým momentem. I v tomto případě přicházejí ke slovu sofistikované bezpečnostní mechanismy a behaviorální analýza, které dokáží objevit i drobné stopy po kybernetickém útoku a nabídnout příslušná opatření.

Učení se na pískovišti

Ač se to může zdát paradoxní, bojovníci s kybernetickým zločinem hledají inspiraci v přírodních a společenských vědách. Pokud má být obrana proti pokročilým hrozbám opravdu účinná, musí z velké části fungovat automaticky. Není totiž v lidských silách analyzovat tak obrovské množství dat, které je k takovéto detekci třeba. To otevírá prostor k vývoji systémů využívajících principů umělé inteligence a strojového učení. Změnu přístupu ke kybernetické bezpečnosti umožnil také fenomén zpracování tzv. velkých dat (big data). V minulosti se totiž tyto systémy „učily" jen na malém datovém vzorku a byly odkázány na lidské zásahy. Dnes naopak učení probíhá na masivním vzorku dat a je v podstatě automatické, přičemž vychází z různých úrovní detailu.

Zkušenosti pražských výzkumníků společnosti Cisco ukazují, že kybernetické „viry" se chovají velmi podobně jako viry biologické. A stejně tak jako v lékařské vědě mohou lékaři předpovědět potenciální nádorové bujení či šíření nemoci v organismu z nestandardního chování jednotlivé buňky (byť ona sama se může jevit jako zcela v pořádku), učí se bezpečnostní systémy bránit proti pokročilým hrozbám snahou zachytit chování, které na první pohled vypadá jako logické a bezpečné, a identifikovat ho jako potenciální hrozbu. Během několika let tak budou schopny pokročilé síťové bezpečnostní systémy automaticky rozlišovat lidmi nerozeznatelné události v síti a spolehlivě automaticky reagovat při objevení jediného příkladu doposud neznámé hrozby. To znamená, že bez nutnosti lidského zásahu zajistí zabezpečení a vyčištění napadeného systému, včetně zajištění reportingu celé události.

Při vytváření takovýchto systémů se ke slovu dostává dokonce i teorie her, která umožní umělé inteligenci naučit se rozpoznávat cíle a záměry případných útočníků. Dnes se do centra pozornosti dostává testování aut schopných pohybovat se bez řidiče. V podobných projektech je potřeba se vyrovnat s celou řadou překážek a snad každý si umí představit, že auto bez řidiče musí být schopno zvládnout jak předvídatelné situace – reakci na dopravní značky, pokyny policisty či chování jiných účastníků provozu, tak i ty obtížně předvídatelné, jako jsou například neoznačené silnice, extrémně komplikované dopravní situace či například vliv počasí, poruchy a podobně.

Stejně tak se musí bezpečnostní systémy v souboji s pokročilými hrozbami nastavit za pomoci kombinace celé řady analytických metod a zjištění tak, aby byly schopny rozeznat kybernetický útok i v případech, kdy jde o útoky zcela nové. Právě na tyto případy lze aplikovat teoretické modely chování, které známe třeba ze sociálních věd. Ať již je to zmíněná teorie her či různé modely chování. V praxi tak jak za auty bez řidiče, tak za ochranou proti kybernetickým hrozbám stojí vlastně podobné analytické stroje snažící se rozpoznat konkrétní chování či situaci a automaticky na ni zareagovat. Na rozdíl od aut, která jsou hudbou spíše vzdálené budoucnosti, na poli boje s kybernetickým zločinem jsou odborníci Cisco již dnes schopni nabízet nástroje, které umělou inteligenci a strojové učení využívají v reálném prostředí.

Ze start-upu pod křídla Cisco

Společnost Cognitive Security se zrodila na půdě pražského ČVUT a brzy získala zakázky od americké armády, námořnictva a dalších státních i soukromých subjektů. Nápady v boji s kyberzločinci zaujaly i společnost Cisco, která celou firmu odkoupila v roce 2013. V roce 2015 již produkt Cisco Cognitive Threat Analytics chrání více než půl milionu síťových uzlů na celém světě.

cisco™

Fortinet – víme jak vás ochránit

S příchodem zákona o kybernetické bezpečnosti si řada státních institucí klade otázku, jak naplnit literu tohoto zákona.

Potenciálním cílem kybernetických útoků se dnes může stát kterákoli společnost – bez ohledu na její velikost nebo obchodní zaměření a tradiční síťová ochrana se často ukáže jako nedostačující.

Fortinet působí na trhu již 15 let a přináší komplexní, vícevrstvé bezpečnostní řešení, které kombinuje řadu nejmodernějších technologií a nabízí inteligentní ochranu všem zařízením, uživatelům a aplikacím připojeným k internetu.

Rádi vám pomůžeme zorientovat se v současném světě IT bezpečnosti a vždy být o krok napřed.

Kontaktujte nás na **csr_sales@fortinet.com**.

FORTINET®

www.fortinet.cz

Nový datový sklad Středočeského kraje zvýší přehled o hospodaření úřadu

Středočeský kraj pokračuje v modernizaci svých ICT nástrojů za účelem zvýšení efektivity a transparentnosti svého hospodaření. Napomáhají tomu akce kraje realizované v rámci projektu „Rozvoj e-governmentu ve Středočeském kraji" spolufinancovaného z Evropského fondu pro regionální rozvoj na základě Integrovaného operačního programu.

Nový ERP: přísnější kontrola hospodaření

V roce 2013 kraj dokončil rozsáhlý projekt Vnitřní integrace úřadu. Jeho klíčovou součástí byl nový ERP systém GINIS®, pokrývající všechny důležité ekonomické agendy. Spolu se zprovozněním nových modulů byla nastavena přísnější pravidla provádění ekonomických operací, a to striktně podle zákona o finanční kontrole ve veřejné správě ve smyslu prováděcí vyhlášky č. 416/2003 Sb. Nastavené procesy a informační systém zabezpečují, aby všechny plánované a připravované operace byly v souladu s právními předpisy, schválenými rozpočty, programy, projekty, uzavřenými smlouvami nebo jinými rozhodnutími o nakládání s prostředky kraje.

Mezi další významné celky dodaného řešení patřily mzdy a personalistika, majetek a skladové hospodářství s vazbou na ERP a Asset management (správu hmotných i nehmotných aktiv) nebo softwarová podpora pro vedení správních řízení či procesů spojených s rozhodováním orgánů kraje (usnesení). Důležitou část projektu představovala také integrace se systémem základních registrů a s dalšími informačními systémy. Díky novému Identity managementu disponuje nyní úřad centrální řízenou správou účtů a přístupových údajů k jednotlivým aplikacím.

Významnou roli pro sdílení dat v rámci celého systému hrají portálová řešení pro využití konsolidovaných a personalizovaných informací, a to s vazbami na personální portál nebo objednávkový systém. Požadavky uživatelů, události a incidenty jsou směřovány na nový centrální Service Desk, postavený na technologii CA.

Jak využít získaná data?

V první polovině letošního roku byl projekt Vnitřní integrace úřadu následován dalším, nyní už můžeme říct úspěšným projektem Implementace datového skladu kraje. Tato posloupnost má svoji logiku. Datový sklad je příležitostí,

jak optimálně využít získanou kvalitní a konsolidovanou základnu dat.

Středočeský kraj tím získá možnost hlubších analýz a hledání vzájemných souvislostí v datech. Datový sklad slouží jako jediné centrální úložiště, jehož data využívá manažerský informační systém a obsahuje datová tržiště ekonomika úřadu, ekonomika obcí, školství, zdravotnictví, registry, metadata, vnitřní věci a provoz (v jejich rámci jsou obsahem data z oblastí např. správního řízení a personalistiky.) Například u ekonomiky úřadu tak může nyní kraj lépe sledovat a odhalovat pohyby na příjmových a výdajových účtech a analyzovat je až do úrovně jednotlivých rozpočtových dokladů.

Díky specializovaným tržištím školství a zdravotnictví pak zase úředníci získají větší přehled o činnosti svých školských a zdravotnických zařízení. Součástí dodávky je začlenění datového skladu do informačního systému kraje – realizováno bylo napojení především na ekonomické agendy příspěvkových organizací.

Poskytované informace budou sloužit jak managementu pro jeho rozhodování, tak budou představovat veřejnou informační službu organizacím, obcím kraje i samotným občanům. To by mělo přinést nejen zvýšení transparentnosti a důvěryhodnosti kraje, ale v dlouhodobé perspektivě také přímé finanční úspory.

Dotace tlačily na rychlost

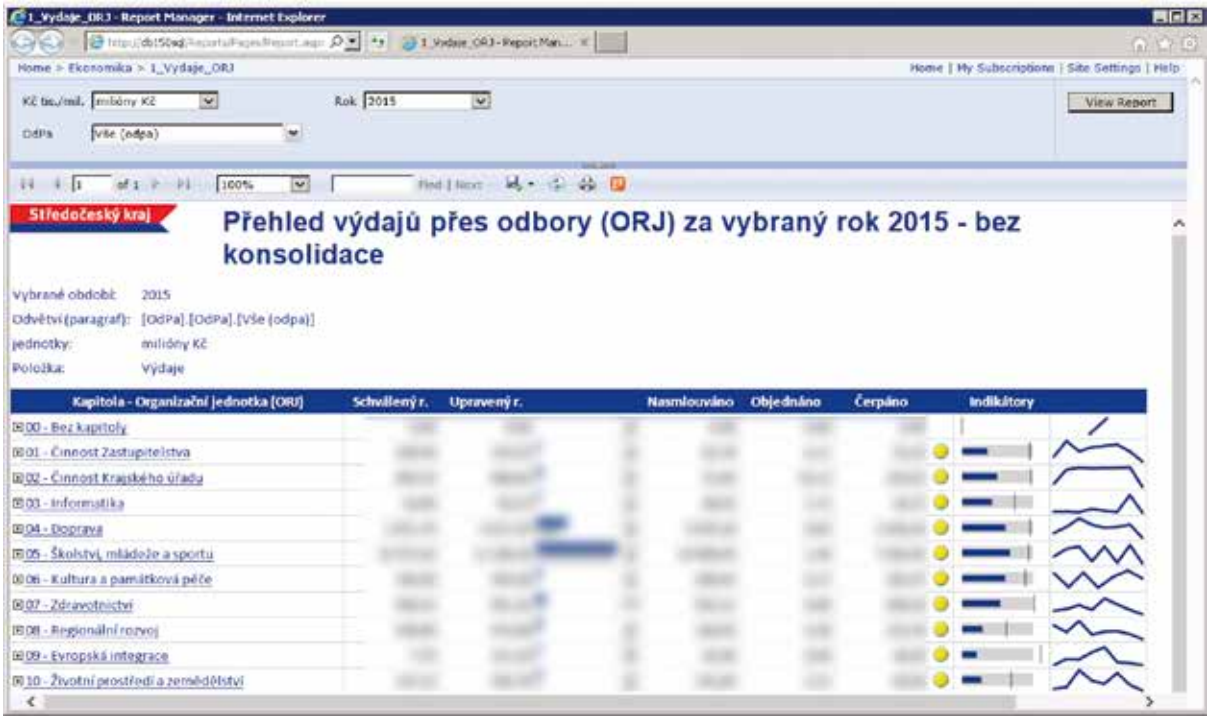
Specifikem tohoto projektu byl požadavek na rychlost jeho realizace. Vzhledem k termínům vycházejícím z celého dotačního projektu na rozvoj e-governmentu byl Středočeský kraj nucen již v zadávací dokumentaci požadovat dodání datového skladu jako hotové aplikace, která se bude „pouze" přizpůsobovat pro potřeby uživatelů Středočeského kraje. Harmonogram projektu se podařilo dodržet, řešení bylo akceptováno 22. července a uvedeno do rutinního provozu. Doba udržitelnosti projektu je 5 let, po kterou bude poskytována (záruční) technická podpora v garantované úrovni služeb.

Pro dodávku a implementaci spolupracoval Středočeský kraj s ověřenými a akreditovanými dodavateli, odborníky a specialisty na datové sklady, manažerské informační systémy a nástroje Business Intelligence a na veřejnou správu. Dodavatelem řešení byla společností GiST a v roli subdodavatele společnost GORDIC.

Václav Pávek, GORDIC spol. s r. o.

GORDIC®

Přehled výdajů za rok 2015



Při rozvoji elektronických služeb je bezpečnost tématem číslo 1

Informační technologie jsou nedílnou součástí moderní společnosti, rozvoj zažíváme ve zdravotnictví, vzdělávání, v komunikaci se státní správou a tak dále. Technologie přináší významný pokrok a zvyšují efektivitu a komfort, ale přinášejí také obrovské množství rizik a hrozeb. Vládní strategie proto klade důraz i na oblast kyberbezpečnosti, na změnu v systému zabezpečení informačních technologií, speciálně v oblasti kritické infrastruktury. Kolem Strategie kybernetické bezpečnosti ČR na období let 2015 až 2020 probíhá řada nejrůznějších diskuzí, každopádně je potřeba zmínit, že v oblasti zabezpečení musí být organizace proaktivní a především ve vlastním zájmu musí dbát na svou ochranu.

Podívejme se na pár faktů, proč je potřeba nebrat zabezpečení jen jako nějaký doplněk a nadstavbu, ale jako nedílnou součást implementace nových technologií. Čísla hovoří jasně a jsou velmi alarmující. Rok 2014 přinesl dramatický nárůst škodlivého kódu a neustále se vyvíjí také rafinovanost jednotlivých útoků. Každou hodinu zasáhne organizaci 106 neznámých typů škodlivého kódu, což je 48krát více než v roce 2013.

Tradičně slabým místem v organizacích jsou mobilní zařízení. Pokud se bavíme o skutečně efektivní elektronické komunikaci, je mobilita klíčová. Například stále častěji budou mít lékaři k dispozici data o pacientech na nějakém mobilním zařízení už přímo v sanitce, zásadním způsobem se tak zrychlí a zkvalitní poskytovaná péče. Ale vše má své pro a proti. Mobilní zařízení jsou oblíbenějším a oblíbenějším terčem kyberzločinců, protože se v podstatě jedná o plnohodnotné počítače s nepřeberným množstvím citlivých, a tedy velmi hodnotných dat. Check Point v rámci svého průzkumu zjistil, že organizace s více než 2000 zařízeními v síti mají až 50procentní riziko, že existuje nejméně 6 infikovaných nebo pro útok vytipovaných mobilních zařízení.

Také 81 procent analyzovaných organizací má nepříjemnou zkušenost se ztrátou dat, což je alarmující nárůst o 41 procent oproti roku 2013. Data mohou nevědomky unikat jakékoli organizaci z různých důvodů, většinou je zde ale spojení na současné nebo bývalé zaměstnance. Většina bezpečnostních strategií se sice zaměřuje na ochranu dat před hackery a útoky zvenčí, ale je úplně stejně důležité chránit data uvnitř organizace i jejich pohyb směrem ven.

Rozvíjí se také stínové IT, tedy neoficiální aplikace nepodporované centrálním IT dané organizace. Výzkum ukázal, že 96 procent organizací použilo v roce 2014 alespoň jednu vysoce rizikovou aplikaci a každou hodinu dojde téměř ke 13 incidentům spojeným s těmito aplikacemi, což je skoro dvojnásobný nárůst oproti roku 2013.
V rámci rozvoje elektronických služeb je bezpečnost jednoznačně tématem číslo jedna. A zatímco vládní strategie se větší měrou soustředí na reakci a vyhodnocování bezpečnostních incidentů, tak organizace by měly rizikům předcházet. Preventivní technologie pomohou vyhnout se možným postihům a problémům.

Elektronické zdravotnictví zajistí přístup ke kvalitnější a rychlejší péči, elektronické bankovnictví zvýší komfort, elektronické vzdělávání otevře studentům zcela nové obzory výuky a komplexní elektronická komunikace se státní správou bude splněným snem mnoha občanů. Nadějné vyhlídky, myslíte si. Ale jen pokud je vše součástí bezpečného prostředí, jinak se naopak takový propojený živý organismus stane noční můrou.

Speciálně ve zdravotnictví nebo bankovním světě je důvěra posvátnou věcí a jedno klopýtnutí může být osudné. Nejvyšší prioritu musí mít i soulad s nejrůznějšími předpisy a nařízeními, například jak dlouho a jakým způsobem lze uchovávat zákaznická data a podobně. Sledování shody musí být automatické a jednoduché a bezpečnostní manažeři musí mít kdykoli k dispozici ucelený přehled o stavu zabezpečení. Zároveň musí být bezpečnostní řešení flexibilní a přizpůsobovat se měnícím se podmínkám a velikosti organizace. To v žádné vládní strategii nenajdete a je na každém, jak dobře si svou instituci zabezpečí. Následky jsou potom už jasné.

Při dnešní síle médií a sociálních sítí se jakákoli kauza rychle dostane na veřejnost a následky způsobené ztrátou důvěry a poškozením pověsti mohou dosáhnout obřích rozměrů. A nemusí se jednat jen o únik citlivých informací. Zásadní je i dostupnost služeb a jejich spolehlivost. Jakékoli výpadky sítě nebo služeb způsobené kyberútoky mají kritický dopad na samotný chod organizace.

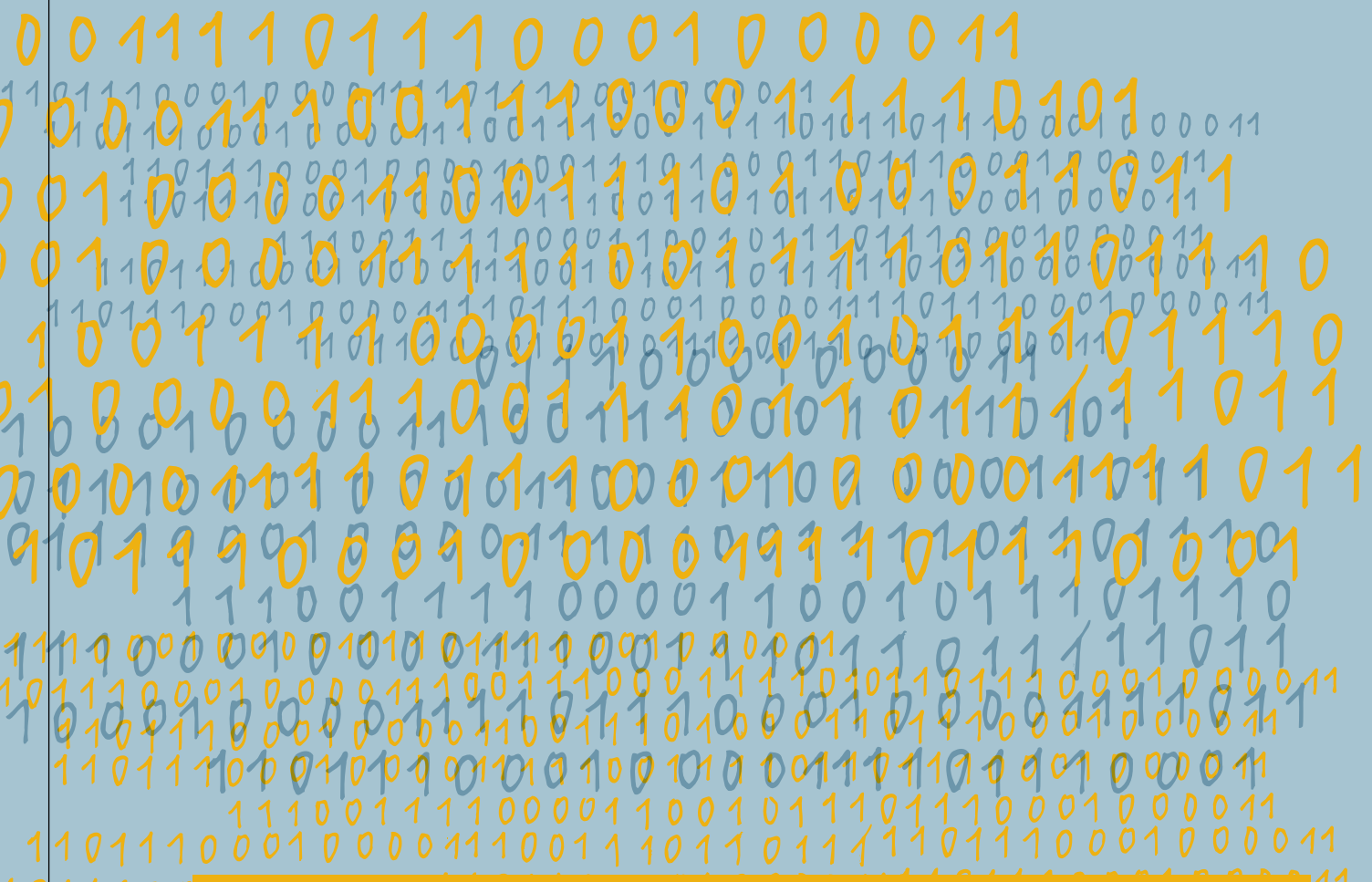
V oblasti zdravotnictví se nebavíme jen o zabezpečení záznamů o pacientech, musí se jednat o komplexní bezpečné prostředí, například zdravotní organizace shromažďují, zpracovávají a uchovávají darovanou krev a orgány. Důležitým prvkem takového projektu je aplikace, která dává zaměstnancům bez ohledu na polohu přístup k údajům, což zrychluje poskytování orgánů pacientům čekajícím na transplantaci. Umíte si představit, co by se stalo, kdyby takový systém někdo napadl a získal k němu neoprávněný přístup?

A rizika se postupem času budou ještě zvyšovat s příchodem internetu věcí. Vyděračské, ransomwarové útoky známe z počítačů a mobilních zařízení, ale můžeme se spolehnout, že postupem času se objeví podobné techniky i u dalších zařízení s připojením k internetu, což u zdravotnických přístrojů může přímo ohrožovat životy lidí, pokud nepřijmeme dostatečná bezpečnostní opatření. Zločinecké skupiny nebudou muset unést živého člověka a požadovat výkupné, stačí získat přístup k nějakému unikátnímu přístroji nebo ovládnout IT v nemocnici a požadovat výkupné za odemčení a zpětné zpřístupnění technologií. Proto jsou jakékoli snahy ze strany vlády o zlepšení kyberbezpečnosti obzvlášť vítané.

Speciální kategorií je potom ochrana kritické infrastruktury. Elektřina, plyn, doprava, jaderná energie... Pro útočníky velmi lákavé oblasti. Check Point je proto velmi aktivní i v oblasti zabezpečení SCADA/ICS systémů, kde pomáhá eliminovat případná rizika. Jakákoli hrozba v této oblasti může způsobit ochromení nebo přímo ohrožení regionu nebo celého státu.

Moderní technologie zkrátka musí jít ruku v ruce s bezpečností. Není možné řešit jen hlášení incidentů, ale zaměřit se především na preventivní technologie. Rychlý a bezpečný internet může otevřít nový svět i studentům. Pomocí videokonferencí se podívají na vesmírnou stanici nebo si prohlédnou podmořský svět očima potápěče. Bezpečnost ale především. Jedno slabé místo v systému umožní útočníkům dostávat se postupně k dalším cílům. A s rozvojem elektronické komunikace a propojením systémů se rozšiřují možnosti, kam se takové útoky mohou posouvat. Zabezpečte proto svou budoucnost.

Miloslav Lujka
Check Point Software Technologies
Czech Republic s.r.o.



eIDAS

Otázka elektronické identity nabývá stále většího významu. V kyberprostoru se nachází stále více našich citlivých dat, s nimiž potřebuje pracovat stále větší počet subjektů. Je tedy podstatné vědět, kdo, kdy s nimi, jak a proč nakládal a zároveň mít možnost zpřístupňovat, či uzavírat svoji elektronickou identitu konkrétním institucím pro konkrétní úkony. Jde tedy o to, mít svoji identitu pod kontrolou v prostředí elektronické veřejné správy (případně elektronického komerčního světa) alespoň tak „dobře", jako tomu je v běžném životě.

Otázkou elektronické identity je nutno se zabývat nejen z důvodu její důležitosti, případně možnosti usnadnění řady úkonů občanů vůči státu a státu vůči občanům, ale rovněž z prostého důvodu, že nám to nařizuje zákon, respektive nařízení Evropského parlamentu. Podle něho například, již ani ne za rok, konkrétně **1. 7. 2016**, vstoupí v platnost **nařízení pro služby vytvářející důvěru a elektronický dokument.**

Času tedy není nazbyt. Proto jsme se tématu elektronické identity věnovali i workshopem v rámci konference e-government 20:10 v Mikulově. Podstatné informace z této diskuze naleznete na následujících stránkách. Zdaleka jsme zde téma eIDAS nevyčerpali, a tak si Vás dovolíme pozvat na seminář, který na toto téma připravujeme na 10. 11. 2015 do Poslanecké sněmovny Parlamentu ČR.

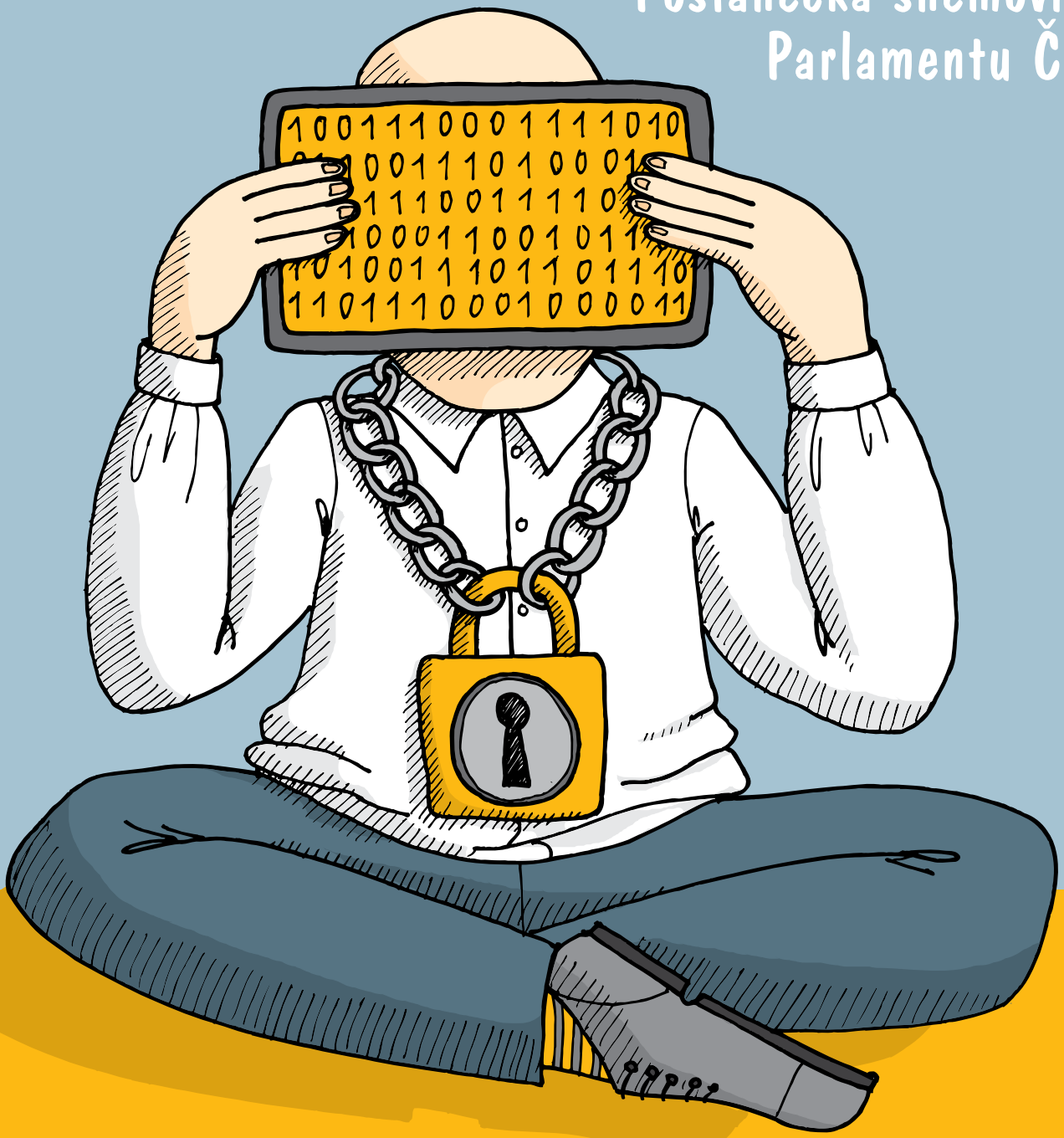
Proč? Protože čas běží, a 1. 7. 2016 musíme mít svoji eIdentitu.

eIDAS

- do roka a do dne

10. 11. 2015

Poslanecká sněmovna
Parlamentu ČR



www.egovernment.cz/eldas

eIDAS – aktuální situace

Robert Piffl v úvodu vystoupení ubezpečil posluchače, že nebude zabíhat do rigidního výkladu práva, ale spíše by je chtěl seznámit s principy eIDAS, časovou osou jeho zavádění a pracovními skupinami MV ČR, které mají s tématem eIDAS přímou souvislost, a s jejich úkoly.

Nařízení eIDAS (Nařízení) je formalizováno od roku 2014, kdy je přijal Evropský parlament a Rada Evropy, a konkrétně od 17. 9. 2014 je toto nařízení platné. Jak Robert Piffl připustil, jeho čtení není úplně jednoduché. Některé pasáže tohoto Nařízení je nutno přečíst několikrát, než je možné pochopit strukturu služeb, o kterých pojednává. Podstatné ale je, že Nařízení eIDAS poprvé řeší právní rámec služeb vytvářejících důvěru napříč Evropou a zároveň definuje nástroje a jejich pravidla, a to jak legislativní, tak technologické (tzv. prováděcí akty). Je zřejmé, že se v rámci tohoto Nařízení vše točí kolem elektronického dokumentu. Sama definice elektronického dokumentu je dána i v našem právním řádu, a to v zákoně č. 499/2004 Sb. Zjednodušeně se všechny tyto definice dají vyložit tak, že elektronickým dokumentem je téměř cokoliv v digitální podobě, tedy jakýkoliv elektronický obsah, dokonce i elektronický certifikát je možné považovat za elektronický dokument.

Velice důležité je, že nařízení EU č. 910/2014 o eIDAS skutečně stanoví právní rámec pro tyto služby:

- elektronické podpisy;
- elektronické pečetě;
- elektronická časová razítka;
- elektronické dokumenty;
- služby elektronického doporučeného doručování a certifikační služby pro autentizaci internetových stránek.

Celé Nařízení vzniklo na základě snahy Digitální Evropa 2020. Zásadním datem je 17. 9. 2014, kdy bylo přijato EK. Dalšími klíčovými termíny jsou:

18. 9. 2015 Od tohoto data je teoreticky možné, aby jednotlivé členské státy dobrovolně začaly používat systém elektronické identifikace. Teoreticky proto, že prováděcí akty, které definují jednotlivé stupně a úrovně atp., byly přijaty 14. 9. 2015. K jejich formalizování a uveřejnění v Evropském věstníku došlo o pár dní později, a tak by zřejmě jen těžko někdo mohl od 18. 9. 2015 skutečně provozovat systém elektronické identifikace. Ale od tohoto data běží lhůta až do roku 2019.

1. 7. 2016 Jako vedlejší důsledek Nařízení se zruší směrnice č. 93, na jejímž základě vznikl zákon o elektronickém podpisu. K tomuto dni se na území ČR ruší zákon o elektronickém podpisu a věci s ním související a místo toho bude vydán nový zákon o službách vytvářejících důvěru při elektronických transakcích. Tento termín je tedy jakousi tlustou čárou, která zavádí určitou právní jistotu. Od tohoto dne některé pojmy, které byly napříč Evropou roztříštěné, budou sjednoceny a všechny evropské státy je budou vnímat, používat a vyhodnocovat naprosto stejně.

18. 9. 2018 Ačkoliv to není uvedeno přímo v Nařízení eIDAS, Evropská komise ve všech svých materiálech uvádí, že by členské státy měly být povinny od tohoto data rozpoznávat elektronickou identifikaci. Souvisí to s tzv. tříletou přechodnou lhůtou navazující na přijetí prováděcích aktů.

CO NÁM eIDAS PŘINESE?

Více času. Jak Robert Piffl uvedl, eIDAS je vystižen heslem „vracíme vám čas". Tím, že budou definovány právní rámce, může se elektronizace podle jeho slov více rozhýbat. To znamená, že bychom ve všech důsledcích měli především ušetřit čas – každému z nás by eIDAS měl přinést více volného času díky tomu, že budeme schopni vyřešit více úředních věcí elektronicky.

Zvýšení právní jistoty. To je patrně nejpodstatnější. Se zvýšením právní jistoty souvisí i tzv. zavedení odpovědnosti za škodu. Podle Roberta Piffla je to nejlepší možný katalyzátor, který něco prosadí. Na úrovni Nařízení je totiž jednoznačně stanoveno, že od určitého data všechny členské státy musí akceptovat elektronické dokumenty. Nemohou je tedy odmítnout ani jako důkazní prostředek u soudu ani u správních řízení atp. A především, pokud tak učiní, mají odpovědnost vůči subjektu, kterému akceptaci odmítly.

CO SE DĚJE?

Do poloviny září došlo ke schválení posledních prováděcích aktů, které se týkají zejména prokazování stupně důvěry. Zároveň zahajuje činnost Coopertaion Network, což je v podstatě skupina expertů jednotlivých členských států, kteří budou navzájem posuzovat jednotlivé systémy jak identifikace, tak ostatních služeb vytvářejících důvěru. Na základě tohoto posuzování budou stanovovat hodnoticí kritéria a v návaznosti na ně pak budou jednotlivé členské státy ohlašovat své systémy. Zásadní datum bude 1. 7. 2016, kdy veškeré důsledky tohoto Nařízení vstoupí plně v účinnost. Zároveň by měl v ČR vstoupit v platnost nový zákon, který MV ČR v současné době dává do vnějšího připomínkového řízení – zákon o službách vytvářejících důvěru při elektronických transakcích. První etapa eIDAS by pak měla být dořešena v roce 2020.

PRINCIP

V našem právní řádu existovaly podle Roberta Piffla „berličky" odstavce vsunuté do zákonů, které řešily vše, co bylo potřeba, a přitom to nebylo v našem právním řádu zakotveno. V tomto směru nejsme patrně výjimkou. Různé členské státy situaci řešily ve svých právních řádech odlišným způsobem a teprve nyní je napříč Evropou skutečně jednotný názor, co obsahují konkrétní služby, jaký mají význam, a to s jasnou vymahatelností.

Konkrétní pravidla, která Nařízení přináší:

- identifikace slouží pouze k identifikaci. Identifikací nelze nahradit žádný projev vůle či jiné kroky, identifikace je pouze identifikací daného subjektu;
- doručování slouží k doručení datové zprávy od odesílatele k příjemci. Nic víc od toho úkonu nelze očekávat.

Komise se shodla na tom, že teprve v případě realizace některé z forem podpisu – vlastnoruční či elektronický – bude občan projevovat svoji určitou vůli. Nařízením se v této souvislosti zavádějí elektronické pečetě, což jsou vlastně speciální formy elektronických značek (ty, které byly zavedeny naším zákonem, se nově ruší). Elektronická pečeť je tedy vhodná pro právnické osoby, které je možné označit jako původce a nejsou svázány s konkrétní fyzickou osobou.

Protože toto vše vyplývá z Nařízení eIDAS, je podle Roberta Piffla vhodné hledět na Nařízení jako na příručku, která popisuje určité životní cykly a stavy elektronického dokumentu a z toho je pak možné odvozovat důsledky a využitelnost Nařízení.

DOPADY eIDAS

Konečně tedy máme napříč Evropou jasný právní rámec, který říká, co se stane, když se elektronický dokument doručí z bodu A do bodu B. Je jasně definováno, co znamená, když dokument bude podepsán kvalifikovaným elektronickým podpisem, co znamená, když bude opatřen kvalifikovaným časovým razítkem, a co znamená, když bude opatřen pečetí, případně doručen systémem elektronického doporučeného doručování. Máme tedy k dispozici skutečný právní rámec.

Podstatné ovšem podle Roberta Piffla je, že bychom nikdy neměli zaměňovat primární účely elektronických služeb. Pokud navštívíme web, který bude označen jako důvěryhodný a bude využívat služby pro důvěryhodné weby, tak máme pouze a jedině jistotu, že jsme se přihlásili tam, kam jsem se přihlásit chtěli. Například navštívíme-li web FÚ, budeme mít jistotu, že je to web FÚ a že tedy například čísla účtů, která jsou zde uvedena jako ta, na něž bychom měli poslat daně, jsou skutečně správná. Teprve další rovina je situace, kdy protistrana potřebuje vědět, kdo jsem, tedy situace, kdy použiji důvěryhodnou identifikaci a jsem identifikován. A teprve v momentě, kdy učiním nějaký úkon, v jehož důsledku se vytvoří libovolný dokument podepsaný elektronickým podpisem či opatřený pečetí, nastává doručování a je vyjádřena má vůle.

To je základní princip eIDAS – přináší jasné cykly, jasné postavení služeb a jasné dopady do právního prostředí.

Grafické provedení značky důvěry

JAK JSME NA TOM V ČR?

Odbor hlavního architekta e-governmentu koordinuje některé z důležitých činností v této oblasti a postaral se rovněž o to, že vznikl tzv. řídicí výbor eIDASu. Ten je jednak poradním orgánem ministra a zároveň se jedná o poradní orgán RVIS. Výbor tedy spojuje odborníky i úředníky a vytvořil šest pracovních skupin:

1. elektronické podpisy, elektronické pečetě, časová razítka a autentizace webů;
2. elektronické doporučené doručování (v rámci služeb vytvářejících důvěru);
3. elektronická identita a prostředky pro elektronickou identifikaci;
4. gateway národního ID systému a dalších služeb vytvářejících důvěru do EU a vice-versa;
5. elektronický dokument;
6. dohledové orgány, hodnocení ID systémů.

Zatím se nesešly skupiny, jejichž práce souvisí s přeshraničním uznáváním. Podle Roberta Piffla je to tím, že ani v Bruselu ještě nebyly ujasněny tzv. dobrovolné prováděcí akty. Teprve nyní se poprvé schází Cooperation Network a uvedené skupiny začnou pracovat následně (jedná se o skupiny číslo 2,4,6).

Pracovní skupina jedna se spolupodílela na přípravě nového zákona o službách vytvářejících důvěru. Jednalo se především o podpisy, časová razítka a pečetě atp. Pracovní skupina 3 se zabývala aspekty eletronické identifikace, zejména s dopadem na nové využití občanského průkazu - v rámci celé Evropy začíná převládat jakýsi většinový názor, jak s tímto naložit.

V současné době bude MV ČR dávat do vnějšího připomínkového řízení nový zákon o službách vytvářejících důvěru při elektronických transakcích. Ten zákon je zcela nový. Původní zákon o elektronickém podpisu a všechny související záležitosti budou tedy zrušeny.

Od 1. 7. 2016 jak Nařízení, tak i zákon vytvoří základní stavební kameny, které budeme moci využívat.
Jak Robert Piffl uvedl, Nařízení eIdas postupuje v určitých vlnách. Nyní se vyřešila identifikace, elektronický dokument, následně se začnou řešit přeshraniční uznávání, Gateway atp. Z toho je zřejmé, že nový zákon se bude každý rok upravovat. Zcela nepochybně Ministerstvo vnitra bude mít již pro příští rok v legislativním plánu prací novelu tohoto zákona, neboť se budou muset přidat pasáže o elektronické identifikaci a věci související. Dá se očekávat, že v této souvislosti se změní i řada dalších právních předpisů, to znamená, že pro několik příštích let je možné v této oblasti očekávat legislativní smršť.

JAKÝ JE VÝVOJ V EU?

EU jde podobným směrem jako ČR. Leckde jsou nyní aktuální úvahy o tom, kdo a jakým způsobem by měl být nositelem národní identity, která bude garantovaná státem, přičemž stát v tu chvíli přebírá zmiňovanou odpovědnost za škodu. Zvažují se tedy alternativy, zda se bude jednat o státní národní autoritu, nebo zda bude do této oblasti vpuštěn soukromý sektor. V roce 2016 očekáváme, že bude formalizován a definován tzv. národní identitní prostor, který bude základním stavebním pilířem pro evropské ID a bude určovat, jak a u koho budeme žádat o ID v České republice. Kdoliv si může zřídit identitu v rámci jiného členského státu a využívat digitální služby jiného než českého státu. A právě v digitálně spojené a sjednocené Evropě spočívá podle Roberta Piffla hlavní význam eIDAS.
Probíhají pravidelná jednáních nejen orgánů EK, ale zároveň se čím dál tím více rozdělují jednotlivé členské státy na skupiny, a to jak na základě historického vývoje, tak na základě geopolitického uspořádání a setkávají se při bilaterálních jednáních. Zde se dohadují o tom, jaké jsou představy tvůrců e-governmentu v jednotlivých státech, a snaží se předpřipravit cestu k dohodám o přeshraničním uznávání.

Robert Piffl,
poradce náměstka ministra vnitra

Studie eID kde již využívají – duben/květen 2015

Většina států používá státní národní eID schéma garantované státem a dle ohlasů v eIDAS Expert Group je toto nejvíce podporovaná cesta, nosič většinou čipová karta (zpravidla průkaz totožnosti).

V závěru vystoupení Robert Piffl ukázal, jakým směrem se jednotlivé státy ubírají právě v otázce poskytovatele národní identity. Studie EK, kterou prezentoval, zahrnuje spíše západoevropské státy:

Červené – v nich se vydali cestou, kdy poskytovatel národní identity bude státní, tedy garantován státem.

Zelené – služby budou garantovány státem, ale budou připuštěni i soukromí poskytovatelé, nicméně odpovědnost za škodu přebírá stát.

Modré – je Dánsko, které má privátní útvar, jenž poskytuje národní identitu s tím, že uvažují, jestli přece jen nepřeskočí do státního modelu.

Puntíkované – Británie a Francie, které v současné době ještě nesplňují národní autority plně, tedy model nejvyššího stupně důvěry, který bude v rámci Nařízení eIdas vyžadován. Když je pole červeně puntíkaté, je řešení založeno spíše na státní autoritě, když modře, tak převažuje soukromý sektor.

TAK UŽ NÁM TO ZAČALO!

Ano, přesně 18. 9. 2015 začalo dobrovolné používání elektronické identifikace (eID). A co se stalo? Nic. Je to obrovská škoda, protože se mohlo stát skutečně hodně. Ale to by musel stát něco začít dělat. Tentokrát chyba skutečně není na IT firmách, zde musí zafungovat stát. Jak jsme vyslechli na konferenci v Mikulově, stát začal pracovat na eID, resp. začal se zabývat nařízením EU č. 910/2014 o eIDAS. Na Ministerstvu vnitra byly vytvořeny pracovní skupiny, rozděleny úkoly a? Některé skupiny se zatím ani nesešly. Třeba taková skupina č. 2 zabývající se problematikou elektronického doporučeného doručování.

Je to paradoxní, protože celé nařízení eIDAS se netýká pouze nás, ale všech členů Evropské unie. To nám přece dává obrovskou příležitost nabídnout naše e-governmentové systémy dalším členům Unie, kteří jsou v zavádění e-governmentu ještě za námi. Naše e-governmentové systémy jsou nezpochybnitelně na velmi dobré úrovni, elektronizace v naší zemi rázně pokročila, pouze svá řešení nedovedeme (stát to nedovede) marketingově prodat. Raději budeme pořád dokola obhajovat a přít se, co se kde nepovedlo. Tím, co se skutečně daří, nemá cenu se asi chlubit...

Ale vrátím se k pracovní skupině č. 2. Čím by se měla dle mého názoru zabývat (až se sejde)? Rozhodně využitím toho, co už máme, tedy Informačního systému datových schránek. Vždyť, v čem spočívá elektronické doporučené doručování? Naše datové schránky úspěšně pracují už několik let, neztratily jedinou zprávu, prostě perfektně fungují. Tak proč je nevyužít jako vývozní artikl? Čím více států EU by využívalo podobný systém jako ISDS, tím snadnější by pak bylo řešení problému přeshraničního doručování. Nejlépe poslouží vlastní příklad a jasně deklarovat, že ISDS je připraveno na eIDAS. (A pokud ještě není, tak je na tuto podobu upravit. A neschovávat se za to, že nevíme, jak to bude. Koneckonců, v Česku bude takové řešení, jak řekne české MV.)

Proč čekat na výsledky setkání Cooperation Network nebo Expert Group? Co od nich můžeme očekávat? Buď to bude snaha protlačit myšlenky „někoho většího" nebo „nicneříkající" standardy přeshraničního doručování. Dovolil jsem si tuto troufalost, protože si nedovedu představit, že by mohl mít v současné chvíli někdo představu, jak bude předávat obsah našich datových zpráv například do systému třeba v Portugalsku a naopak. Vždyť se v krajním případě jedná o řešení úlohy s 27 proměnnými. Nebylo by lepší začít konečně propagovat náš systém a skutečně ho vyvézt do ostatních členských zemí? Já říkám, rozhodně! Vždyť, co si myslíte, že budou dělat takoví Estonci? Využijí první možnost vnutit ostatním svůj systém občanských průkazů a státní certifikační autority.

A jsem u dalšího okruhu otázek. Rozumím tomu, proč zástupci státu lpějí na eOP s čipem a pokud možno rovnou s podpisovým certifikátem fyzické osoby. Je to racionální krok, aby byly využity již investované prostředky do systému na vydávání občanských průkazů. Méně už rozumím interní certifikační autoritě, která by měla monopol na vydávání těchto certifikátů. Proč potom MV autorizovalo 3 certifikační autority? Neměly by to být právě ony, kdo by měl vydávat i podpisové certifikáty, když to umí?

Dále se nemohu ubránit pocitu, že stát zde úplně zapomíná, komu má vlastně eID sloužit. V první řadě občanovi, až v druhé řadě jde o stát, který bude mít nepopiratelně identifikovaného a autentizovaného občana hlásícího se k nějakému ISVS.

Tak proč se stát chystá nabídnout uživateli pouze jeden prostředek pro elektronickou identifikaci, tedy již zmíněný eOP? Zřejmě si neuvědomil, že eIDAS otevírá konkurenční prostředí napříč prostorem EU a přitom poskytovatelů identitních služeb bude minimálně 27, spíše více. Obstojí v této konkurenci eOP za pětistovku? Ani náhodou!

Je třeba myslet v první řadě na uživatele, v jakých situacích se může vyskytnout, co bude/může v různých situacích potřebovat, aby se mohl elektronicky identifikovat. Pak lze jednoduše dojít k závěru, že hmotným prostředkem pro elektronickou identifikaci by mohl být třeba i chytrý telefon nebo bankovní karta. Každý takový prostředek může být snadno registrován u poskytovatele identitních služeb a záznam o jeho držiteli propojen s identitou konkrétní fyzické osoby v registru obyvatel. Vždyť jsme na to prakticky připraveni.

Uvedu příklad. *Jako občan České republiky mám eOP, a to dokonce s čipem (pominu, že až dosud mi byl k ničemu). Nyní tedy na něj hypoteticky dostanu, zdarma nebo opět za poplatek, případně za čas strávený cestou na úřad, svůj podpisový certifikát. K tomu mi stát přibalí třeba čtečku čipových karet.(Opravdu to chce stát v současném konkurenčním prostředí financovat?) Dobře, jsem vybaven a mohu použít svoje eID pro přihlášení k nějakému ISVS. Pokud budu sedět doma u svého počítače, jsem schopen čtečku připojit a využít identifikace a autentizace pomocí eOP. Dejme tomu, že čtečku můžu využít i v práci, pokud ji nezapomenu doma.*

Ale co udělám, budu-li například na chalupě (bez počítače, a tedy i bez čtečky), kde ulehnu s chřipkou, nebudu schopen jet zpátky do města a přitom budu potřebovat učinit nějaký úkon vůči státu? Neudělám nic. Třeba i nedodržím nějaký termín určený zákonem. Rodině zavolám, stejně tak do práce, abych se omluvil, ale to je tak všechno. Pokud bych mohl použít svůj mobil jako další hmotný prostředek pro elektronickou identifikaci, měl bych po problému. Potřebný úkon vůči státu bych byl schopen vyřešit.

Nebo jiný případ. *Budu na dovolené v „daleké" cizině. S sebou budu mít veškeré cestovatelské vybavení, včetně plavek a třeba i svůj notebook. Ale budu bez čtečky a bez občanky. Vycestoval jsem prostě s pasem, mobilem a kreditkou a zapomněl, že musím učinit v průběhu dovolené opět nějaký úkon vůči státu. Co s tím? Budu-li v EU, mohl bych zajít na místní kontaktní místo veřejné správy. Co když ale nebudou mít aplikovaný systém eOP, ale dají přednost třeba bankovní kartě? Pokud bych mohl jako další hmotný prostředek elektronické identifikace použít svoji kreditní kartu, mám vyhráno. Podání učiním na kontaktním místě a k identifikaci a autentizaci použiju kreditní kartu.*

Ještě je čas zvolit více hmotných prostředků pro elektronickou identifikaci.

Vraťme se nyní zpět k 18. září 2015. K tomuto datu je dle informací MV vydáno zhruba 26 000 eOP. Žádný z nich (kromě několika „šílenců z IT", kteří systém testují) nemá na čipu elektronický certifikát. Tohle nevypadá na první dobrovolníky používající eID dle eIDAS. Co ale skupina fyzických osob (FO), tedy občanů, kteří mají už svoji osobní datovou schránku? Stačilo, kdyby 3. pracovní skupina včas učinila rozhodnutí, že jednou identifikovaný občan vlastnící osobní datovou schránku může jako svoje eID (než dojde ke změně legislativy kvůli podpisovým certifikátům) používat přístupové údaje k datové schránce!

Pak bychom mohli hrdě do světa, resp. na celou EU hlásit, že my v České republice od 18. září používáme již reálně eID! Stačilo opravdu tak málo.... ale jsem optimista, ještě se vše dá dohnat!

Ing. Martin Řehořek,
jednatel NEWPS.CZ s.r.o

NEWPS.CZ

EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

IROP se aktuálně zaměřuje také na rozvoj informačních systémů pro veřejnou správu

Jedním z cílů Integrovaného regionálního operačního programu (IROP) za přispění Evropských strukturálních a investičních fondů (ESIF) je dosáhnout vysoké kvality služeb veřejné správy prostřednictví propojení a sdílení informací a dat, dále pak dokončit proces elektronizace agend veřejné správy a zavést úplné elektronické podání pomocí rozvoje služeb nad základními registry. V této souvislosti řídicí orgán IROP vyhlásil dne 17. 9. 2015 výzvu s názvem Aktivity vedoucí k úplnému elektronickému podání a dále chystá v druhé polovině října tohoto roku vyhlásit výzvu na podporu kybernetické bezpečnosti. Na co se obě výzvy zaměřují a kdo v nich může předložit žádost o podporu?

Aktivity vedoucí k úplnému elektronickému podání

V rámci této výzvy jsou podporovány projekty zaměřené například na vytvoření podpůrných služeb pro úplné elektronické podání, na vytvoření samoobslužných míst, prostřednictvím kterých bude možné realizovat úplné elektronické podání. Další možné zaměření projektů je mimo jiné na implementaci identifikačních prostředků pro využívání služeb eGovernmentu prostřednictvím kontaktních míst nebo na vytvoření bezpečného mechanismu poskytování a využívání údajů v návaznosti na referenční údaje základních registrů. Oprávněnými žadateli jsou v tomto případě organizační složky státu, příspěvkové organizace organizačních složek státu, státní organizace a státní podniky. Dále také kraje a obce (kromě Prahy a jejích částí) a organizace zřizované nebo zakládané kraji nebo obcemi. Žádost o podporu je možné předkládat již v této chvíli a termín ukončení příjmu žádostí o podporu je 30. 6. 2017.

Kybernetická bezpečnost

Ve výzvě zaměřené na kybernetickou bezpečnost budou podporovány projekty zaměřené na zvýšení odolnosti tzv. významných a kritických informačních systémů veřejné správy proti kybernetickým hrozbám. V těchto projektech budou podporovány například tyto aktivity: fyzická bezpečnost, nástroje pro ochranu integrity komunikačních sítí, nástroje pro ověřování identity uživatelů, nástroje pro řízení přístupových oprávnění, nástroje pro ochranu před škodlivým kódem, nástroje pro detekci, sběr a vyhodnocení kybernetických bezpečnostních událostí, bezpečnost průmyslových a řídicích systémů apod. Oprávněnými žadateli jsou stejné typy institucí vyjmenované u výše uvedené výzvy. Předpokládané datum vyhlášení výzvy je 21. 10. 2015 a žádosti o podporu bude možné předkládat do 30. 5. 2017.

Více informací o obou uvedených výzvách je možné získat na webových stránkách IROP http://www.dotaceeu.cz/IROP, kde jsou zároveň zveřejněny důležité metodické dokumenty a pravidla pro žadatele a příjemce. Pro detailnější informace je možné se obrátit na příslušného specialistu pro absorpční kapacitu Centra pro regionální rozvoj České republiky. Seznam těchto pracovníků naleznete na http://www.crr.cz/cs/ nebo také na webových stránkách IROP v sekci „Kontakty". Další možností, jak získat potřebné informace, je účast na seminářích pro žadatele, které jsou k výzvám organizovány. V této souvislosti doporučujeme sledovat na webových stránkách IROP kalendář akcí a v případě zájmu se na daný seminář přihlásit.

zdroj: Ministerstvo pro místní rozvoj

INTEGROVANÝ OPERAČNÍ PROGRAM

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

ICZ

SPRÁVNÉ INFORMACE A SEHRANÝ TÝM VÁS VŽDY BEZPEČNĚ PŘIVEDOU DO CÍLE.

STEJNĚ JAKO V OSOBNÍM, TAK I V PROFESNÍM ŽIVOTĚ SE PODMÍNKY ČASTO MĚNÍ. SPRÁVNÉ INFORMACE VÁM UMOŽNÍ ZVOLIT IDEÁLNÍ SMĚR. PROTO JSOU ZDE INFORMAČNÍ SYSTÉMY ICZ.

[VÝROBA] [OBRANA] [FINANCE] [DOPRAVA] [ENERGETIKA] [ZDRAVOTNICTVÍ] [VEŘEJNÁ SPRÁVA] [TELEKOMUNIKACE]

www.i.cz

Finanční řízení územně samosprávních celků

Školy, nemocnice, domovy seniorů, technické služby a mnoho dalších. To jsou organizace zřizované územně samosprávním celkem (ÚSC). Mají právní subjektivitu a jejich vedení je za svá rozhodnutí odpovědné. Vnímají je však takto i občané? Obec i kraj má v rámci své působnosti tyto služby zajišťovat, a pokud s nimi občané nejsou spokojeni, bývají to v jejich očích právě političtí představitelé, kdo selhal.

ÚSC jsou veřejnoprávními korporacemi, které poskytují svým občanům veřejné služby. Za tímto účelem mohou zřizovat a zakládat organizace. Tyto celky, společně se svými zřizovanými a zakládanými organizacemi (ZZO), tvoří spletitý organismus, v němž rozhodnutí jedné organizace může ovlivnit fungování všech ostatních. Je důležité, aby byl tento organismus usměrňován, koordinován a monitorován, tedy **systematicky řízen**. Oblastí, u které je zvlášť nezbytné fungující řízení, je nakládání s veřejnými prostředky, neboť hospodaření ZZO je napojeno na rozpočet svého zřizovatele.

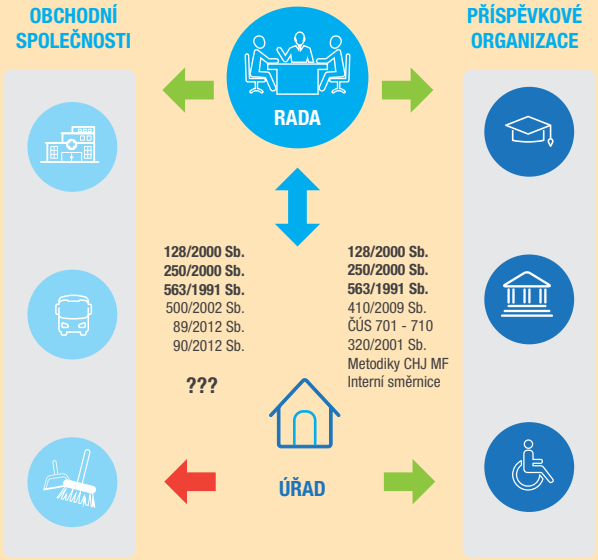
Častým argumentem proti zvýšené míře řízení ze strany ÚSC je právě fakt, že ZZO jsou samostatné organizace s právní subjektivitou a vlastní odpovědností. Co se však stane, pokud organizace bude vykazovat ztrátu a nebude schopna dostát svým závazkům? Na koho se v případě problémů obrátí? Pravděpodobně to bude její zřizovatel. A nenajde-li se jiný způsob, bude to opět tento ÚSC, kdo bude muset vynakládat další prostředky ze svého rozpočtu. Z toho důvodu se v praxi objevují stále častější tendence směřující k zavádění jednotného finančního řízení celé veřejnoprávní korporace, aby se předcházelo nehospodárnému, neefektivnímu a neúčelnému vynakládání veřejných prostředků a aby se přispělo ke zvýšení transparentnosti.

Legislativní rámec finančního řízení

Právní řád umožňuje obcím a krajům zakládat a zřizovat organizace, aby byl zajištěn efektivní výkon veřejné služby. Musí jim tedy také poskytnout určité nástroje, prostřednictvím kterých mohou následně své ZZO řídit. Právní úprava této problematiky sice existuje, ale co se týče její použitelnosti v praxi, není dostatečná a vyvážená. Základem problematiky finančního řízení jsou ustanovení zákona č. 128/2000 Sb., o obcích, zákona č. 250/2000 Sb., o rozpočtových pravidlech územně samosprávních celků, a zákona č. 563/1991 Sb., o účetnictví. Tyto zákony vymezují legislativní rámec vztahu obce vůči jejím ZZO. Úkoly zřizovatele a zakladatele ZZO plní rada obce. Ta zároveň zadává úkoly obecnímu úřadu, který se pak významně podílí na přípravě podkladů potřebných k řízení ZZO.

Základním nástrojem kontroly zřizovatele vůči příspěvkové organizaci je přezkum hospodaření, který spadá pod režim zákona č. 320/2001 Sb., o finanční kontrole. A právě zde se projevuje nevyváženost nástrojů řízení daných zákonem. Obchodní společnosti zakládané obcemi totiž do působnosti zákona o finanční kontrole nespadají. Řízení obchodních společností je postaveno na smluvní volnosti a principech soukromého práva. Finanční řízení obchodních společností je obzvláště složitou oblastí, neboť není vymezeno v žádném speciálním zákoně, naopak je roztříštěno do několika zákonů a při jeho realizaci se neobejdeme bez kombinování prvků z komerční sféry a veřejnoprávní oblasti.

Porovnání legislativy upravující výkon finančního řízení u PO a OS zřizovaných a zakládaných ÚSC



Nástroje finančního řízení nad rámec zákona

Aby bylo možné celou veřejnoprávní korporaci koordinovaně a efektivně řídit, je potřeba jít nad rámec legislativních nástrojů. V dnešní době je možné hledat inspiraci v dobré praxi jiných subjektů veřejné správy, neboť veřejná správa se stále častěji nechává inspirovat sektorem soukromým. Příkladem může být koncepce New public management, která usiluje o zavádění moderních nástrojů do sektoru veřejné správy. K dispozici je také nepřeberné množství mezinárodních standardů, např. COSO 2013, INTOSAI, PIFC, standardy IIA a další.

ÚSC si pro sebe a pro své ZZO musí umět vhodně vybrat ty nástroje finančního řízení, které budou nejlépe vyhovovat jejím potřebám a které vhodným způsobem navážou na to, co je již v praxi používáno. K implementaci jednotného finančního řízení je třeba přistupovat systematicky a organizovaně. Nejedná se o jednoduchý, ani o krátkodobý proces. Vždy je třeba vycházet ze současného stavu, který musí být jasně popsán, nejlépe na základě Analýzy stávajícího stavu nastavení vnitřního řídicího a kontrolního systému, společně s Analýzou nastavení finančního řízení příspěvkových organizací. Na základě takto exaktně doložitelného popisu je možné identifikovat procesy, které je nutné zefektivnit. Teprve poté se mohou hledat řešení a nástroje, které toho pomohou dosáhnout. Může se jednat o nové přístupy k finančnímu plánování – v současné době se stále častěji přistupuje ke **střednědobému finančnímu plánování a k plánování investic**. Důraz se klade na správné nastavení a fungování **vnitřního řídicího a kontrolního systému**, který by měl vést k efektivnímu nakládání s veřejnými prostředky a ke snižování rizik. Častým krokem je též nastavení **jednotného vedení účetnictví** (výkaznictví), které umožňuje ÚSC získávat od všech ZZO data ve stejném rozsahu.

Klíčovým prvkem celé implementace v ZZO je metodická pomoc jejich zřizovatele a zakladatele.

Využití ICT nástrojů

Mluvíme-li o nástrojích usnadňujících a zefektivňujících finanční řízení, nelze opomenout nástroje z oblasti informačních technologií. Provádění některých činností, jako vedení účetnictví, sestavování rozpočtů apod., si dnes již bez těchto nástrojů nedovedeme představit. Softwarové nástroje umožňují organizacím zefektivnění a automatizaci procesů a jejich fixaci oproti nastaveným pravidlům.

Pro komplexní podporu finančního řízení dnes nestačí zavedení ICT nástrojů pro podporu vedení účetnictví. Aby měl zřizovatel co nejpřesnější a aktuální informace o nakládání s veřejnými prostředky u svých ZZO, je zapotřebí elektronizovat a automatizovat další procesy, jako jsou výkon finanční kontroly, finanční plánování, řízení rizik či nastavení průběžného monitoringu. Jedním z nástrojů, který uvedené procesy automatizuje, je HELIOS CROSEUS. Tento nástroj finančního řízení umožňuje zaznamenání provedené předběžné i následné finanční kontroly k jednotlivým finančním a majetkovým operacím. Výsledkem schvalování je detailní auditní stopa, která obsahuje úplnou časovou posloupnost provedených kroků a všech příslušných dokumentů formou přílohy. Vedení ÚSC pak může být průběžně ujišťováno o finančním zdraví celé veřejnoprávní korporace.

Dosažení výsledku

Přínosy zavedení ICT nástrojů jsou mnohé. Vedle usnadnění výkonu daných procesů umožňují získávat aktuální ekonomická data. Ta pak mohou být předmětem analýz a umožňují včasnou identifikaci problémů.

Zavedení nových nástrojů finančního řízení bývá dlouhodobý, komplexní proces, na jehož uskutečnění musí mít zájem jak ÚSC, tak i jeho ZZO. Pokud se však zvolí správný způsob implementace, mělo by finanční řízení představovat komplexní nástroj, který obci umožní zajistit dlouhodobou finanční stabilitu celé veřejnoprávní korporace.

Kristýna Honzů,
konzultantka společnosti DYNATECH s.r.o.

Alžběta Křídlová,
produktová manažerka společnosti
Asseco Solutions, a.s.

MISS EGOVERNMENT 2015

Magazín Egovernment i letos pořádal soutěž o nejsympatičtější dámu české veřejné správy – Miss Egovernment 2015. Již tradičně se finále této soutěže odehrává na zámku Mikulov na společenském večeru konference e-government 20:10, aneb žijem si jak na zámku, ať to trvá věčně. I letos tedy deset finalistek usilovalo o přízeň diváků a poroty. V té zasedli sami na slovo vzatí odborníci, většinou reprezentující hlavní partnery konference: Jakub Fiala za společnost GORDIC, Petr Stiegler za Českou poštu, Dan Šafář za společnost Check point, Květoslav Štrunc za společnost CISCO a Jan Forbelský za Jihomoravský kraj. Předsedkyní poroty byla náměstkyně ministra vnitra pro řízení sekce veřejné správy Jana Vildumetzová, které pomáhal státní tajemník Jiří Kaucký a loňská Miss Egovernment Martina Filipcová. Počasí v Mikulově bylo letos chladné, na zámeckém nádvoří to však při volbě pěkně vřelo.

Nejvíce hlasů poroty a titul **Miss Egovernment 2015** si odnesla **Hana Pospíšilová z České pošty Brno**. Ta zaujala už svým profilem, který do soutěže poslala, když formou básničky popsala samu sebe. Je jí tedy téměř čtyřicet, z toho dvacet let pracuje na poště, ráda hraje squash, píše básničky, hraje na klavír a miluje svoji dceru. Podle vítězky letošní soutěže Miss Egovernment byla atmosféra na zámeckém nádvoří výborná a její trému zastínilo chladné počasí. Jak řekla, znovu by se do soutěže nepřihlásila, ale jen proto, aby dala šanci ostatním vyzkoušet si na vlastní kůži, jaké to je stát se MISS Egovernment. Domnívá se, že každá, která ji bude chtít následovat, by si měla nachystat přirozenost a důvtip.

V rodině a na pracovišti Hance všichni fandili a jak sama připustila, bez jejich podpory by pro ni tato soutěž neměla smysl. „Do příštích let bych organizátorům akce doporučila zajistit lepší počasí, případně finálový večer přemístit do vnitřních prostor zámku.... jinak to byla opravdu skvělá atmosféra a velmi vydařená akce," dodala vítězka...

První vicemiss a zároveň Miss sympatie se stala **Kateřina Komárková ze Správy základních registrů**. Ve svém profilu napsala, že volný čas ráda tráví sportem, tancem a cestováním, ale nebrání se ani klidnějším aktivitám, jako je např. vaření. Nejvíce ji ale baví společenský život a kultura - divadlo, kino, výstavy a historie. Ve volbě Kateřiny se sešel vkus poroty se vkusem diváků, kteří jí udělili titul Miss sympatie.

Podle Kateřiny se celá volba nesla ve slavnostní a velmi přátelské atmosféře. Počáteční nervozita z ní záhy opadla a finálový večer si skvěle užila. Ať už se budoucí soutěžící s odvahou přihlásí samy, nebo je nominuje jejich úřad či organizace, zažít finálový večer podle ní stojí opravdu za to. Je to, dle jejího mínění, zajímavá výzva a báječná příležitost. Příprava na soutěž samotnou nemusí být nutně náročná. Důležitější je spíš přirozené vystupování a osobní kouzlo než například důkladná příprava na volnou disciplínu.

Největší radost Kateřině i jejímu okolí udělalo ocenění Miss sympatie. I proto je vděčná svým kolegům ze Správy základních registrů, kteří si při fandění téměř vykřičeli hlasivky, i všem ostatním, kteří ji v soutěži podpořili. Po

návratu čekaly v práci milé úsměvy a spousta gratulací – to všechno příjemný pocit ze soutěže ještě prodloužilo. Organizátorům by do dalších ročníků popřála hojnou účast a samé pozitivní ohlasy.

Na třetím místě se umístila a **titul druhé vicemiss** získala **Alena Leinweberová z Ministerstva kultury**. Ve státní správě pracuje už 20 let ze svých 40. Svůj volný čas tráví nejraději s rodinkou cestováním. Miluje historii, památky starověkého Řecka, Říma i Egypta a všechny staré věci, které mají duši. Má ráda svoji rodinu, svoji práci, veselé lidi, knížky, květiny a cvičení pilates.

Alena finálový večer prožívala velmi ojediněle a slavnostně. Atmosféra mikulovského zámku a velmi příjemná spolupráce techniků a pozornost moderátora udělaly podle ní své. Všechny z přítomných soutěžících dam se tak, alespoň na chvíli, cítily jako princezny. Protože Miss Egovernment 2015 byla pro Alenu první zkušeností tohoto druhu, uchová si na tuto soutěž jen ty nejkrásnější vzpomínky. I když už opravdu nic podobného neplánuje, po zkušenostech z Mikulova by se do takové soutěže určitě přihlásila znovu. Velmi se jí líbilo, že byla připravena pro široký okruh dam, dívek či slečen, kde jediným společným jmenovatelem byla veřejná správa. Opravdu nikdo neřešil věk, počet dětí či kilogramů... Pro budoucí soutěžící je, podle jejího mínění, důležité, aby se dámy soustředily na svou volnou disciplínu. V té se totiž mohou nejvíce představit, oslovit či zaujmout porotu a přítomné publikum. A neměly by se zbytečně stresovat, zůstat po celou dobu klidné, samy sebou a hezky si finálový večer v Mikulově užít. Reakce rodiny byla bezprostřední a krásná, neboť byli v Mikulově s Alenou, a tak vše společně intenzivně prožívali.

Dodejme jen, že vítězka obdržela nový iPhone 6 od společnosti CISCO, víkendový wellness pobyt v hotelu Galant pro dvě osoby, broušený pohár ze sklárny Rückl, vůz SEAT k zapůjčení na víkend i s plnou nádrží a samozřejmě spoustu gratulací a květin.

Další fotografie a informace k Miss Egovernment 2015 naleznete na **www.egovernment.cz/miss**.

Spolupracujeme. A díky tomu jsme propojili obyvatele města s radnicí.

Šéfům IT oddělení, jako jste třeba právě vy, se díky spolupráci s námi daří zlepšovat veřejné služby a zároveň šetřit peníze daňových poplatníků. Naše moderní mobilní aplikace tak například radikálně mění způsob propojení obyvatel města s radnicí, která díky ní může rychle odstranit nelegální graffiti.

Občanům teď už na oznámení graffiti vandalismu stačí jen mobilní telefon. Během jednoho roku díky této aplikaci vyjely úklidové graffiti čety ke 2851 případu. A to je skvělý způsob, jak přispět ke kvalitě života ve městě.

Zanechte svou vlastní stopu v novém stylu IT. Má to smysl.

Prozkoumejte své možnosti s HP Enterprise Services prostřednictvím stránky Business Value Exchange.
www.bvex.com

GORDIC®

GINIS+

Interaktivní úřad

Intuitivní prostředí

Úplné elektronické podání

» **Inteligentní asistent**

Kybernetická bezpečnost

Facility Management

Portálová a mobilní řešení

Inteligentní asistent

» učí se z chování uživatele

» pomáhá od rutinních činností

» šetří čas a zvyšuje komfort práce

Inteligentní asistent je průřezově zabudován v celém nadstavbovém systému GINIS+. Jak už jeho název napovídá, učí se z chování uživatele a průběžně ho vyhodnocuje. Následně uživateli usnadňuje jeho stále se opakující činnosti.

Čas pro inteligentního asistenta nastává ve chvíli, kdy má smysl s jeho pomocí předvyplňovat dané pole, aby uživatel nemusel provádět samotný výběr ze seznamu. Příležitostí, kdy lze tento nástroj využít, je například výběr předkontací, sestav nebo osob pro předání dokumentů. Systém již dnes disponuje více jak stovkou inteligentních asistentů.