Egovernment
elektronizace veřejné správy

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

VIZE 2020

KONFERENCE MIKULOV

www.egovernment.cz

č. 3/2016

Nebudou obíhat lidé, ale data a naše údaje budeme poskytovat veřejné správě pouze jednou. A završíme to v roce 2018, kdy se budeme (konečně) elektronicky identifikovat. Teprve od tohoto okamžiku si budeme plně užívat elektronizace veřejné správy. A možná se díky tomu posuneme i na vyšší příčky evropských hodnocení.

Ne že bychom na tom byli špatně. Jak se shodli představitelé MV ČR, kteří vystupovali na konferenci e-government 20:10 v Mikulově, back end máme skvělý. To jsou především základní registry. Co nám však chybí, je front end, tedy něco, co jde přes úřední přepážku směrem k nám, klientům veřejné správy a umožňuje nám využívat dat v základních registrech. A to by měla být právě elektronická identita, která by nám měla umožnit sedět doma a komunikovat s veřejnou správou prostřednictvím svého počítače.

Pokud se domníváte, že máte v kapse elektronický občanský průkaz i s čipem a že by vám tedy měla veřejná správa poskytovat služby elektronicky, můžete dojít poznání, že tento průkaz Vám neumožní často využívat ani těch klasických, neelektronických služeb. Prostě proto, že na rozdíl od těch předchozích verzí občanského průkazu nemá řadu informací ve viditelné podobě. Například informace o vašem manželovi či manželce, dětech atp, nejsou vidět. Měly by být přístupné ze základních registrů, kam ale zatím, přes tento průkaz nikdo nepřistoupí, protože nemá ani čtečky, které by to umožnily.

Čtěte skvělé vyhlídky do roku 2020, které jsou výstupem z konference v Mikulově. A připravte se na výměnu svých průkazů, abychom konečně ochutnali e-government i jako jeho klienti.

Ing. Michal Jirkovský
šéfredaktor

“Konečně - hybridní cloud, který dokáže

TRANSFORMOVAT

naše fungování bez narušení.”

One **CLOUD.**
Any **APPLICATION.**
Any **DEVICE.**™

VMware představuje nový hybridní způsob využití IT. Diky němu dokážete jednoduše spojit vaše stávající datová centra s cloudovými a můžete tak rychleji inovovat za využití IT které již používáte. Rozšíření IT nebylo nikdy jednodušší.

vmware®

vmware.com/cz/cloud-computing/hybrid-cloud

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.

Accelerating next

Hewlett Packard Enterprise

Blade server HPE ProLiant Gen9 s procesory Intel® Xeon®. Intel Inside®. Znamená výkonné řešení.

Zrychlování automatizované inteligence

Síla jednotného řešení. Jeden zjednodušený pohled na celé vaše datové centrum v akci – HPE BladeSystem se softwarem HPE OneView. Zrychlete virtuální pracovní úlohy a poskytujte své IT služby 66× rychleji.[1] Snižte prostoje o 91 %.[2] Získejte kontrolu nad svými pracovními postupy. To vše vaší firmě přinese větší hodnotu.

Začněte už teď na stránce **hpe.com/info/workload-guide**

[1] Transformace organizace s konvergovanou infrastrukturou HPE pro softwarově definovaná datová centra, IDC Spotlight, leden 2014.

[2] Oficiální dokumentace společnosti IDC, „Obchodní hodnota systému HPE BladeSystem", IDC, leden 2015.

VIZE 2020

VIZIONÁŘSKÝ PROGRAM A PŘEPLNĚNÝ ZÁMEK

Vize vývoje elektronizace veřejné správy v ČR pro příští čtyři roky bylo základní téma letošní konference e-government 20:10, aneb žijem si jak na zámku, ať to trvá věčně. Proběhla ve dnech 6.–7. 9. 2016 tradičně v prostorách zámku Mikulov a navštívilo ji na 700 účastníků. To mimo jiné znamenalo, že v některých chvilkách bylo i ve velkorysých prostorách zámku docela těsno. Program úvodního dopoledne musel být dokonce přenášen do sálu v horní části zámku.

Pod záštitou ministra vnitra **Milana Chovance**, hejtmana Jihomoravského kraje JUDr. **Michala Haška** a starosty města Mikulov **Rostislava Koštiala**, ve spolupráci s Jihomoravským krajem a za podpory řady významných partnerů se vedly diskuze a přednášky nejen na hlavní téma konference, tedy vizi vývoje pro nejbližší období, ale rovněž k dalším souvisejícím otázkám, ať se jednalo o **kyberbezpečnost**, **cloudová řešení** nebo **elektronickou identitu**.

VIZE „VNITRA"

Konferenci zahajoval za MV ČR náměstek ministra vnitra pro informační a komunikační technologie JUDr. **Jaroslav Strouhal**, který ve svém úvodním projevu vyzdvihl především práci ministerstva na nových zákonech souvisejících se zaváděním elektronické identifikace, včetně zákona o službách vytvářejících důvěru. Kromě toho upozornil na současnou výbornou spolupráci mezi MV ČR a ICT UNIÍ pod vedením jejího nového prezidenta Mgr. Zdeňka Zajíčka.

Ing. **Roman Vrba**, ředitel odboru e-Governmentu, popsal například spuštění registru smluv a novinky v systému datových schránek. Poznamenal, že Ministerstvo vnitra vyšlo vstříc požadavkům na úpravy od resortů spravedlnosti a financí, a připomněl také, že občané mohou nově díky „datovkám" získat zdarma a z vlastního počítače výpis bodového hodnocení řidiče a výpis z rejstříku trestů.

Ing. **Miroslav Tůma**, Ph.D., ředitel odboru kybernetické bezpečnosti a koordinace informačních a komunikačních technologií, vyzdvihl úkoly, které čekají ministerstvo na poli kyberbezpečnosti. Popsal, jak dohledové centrum e-Governmentu zajišťuje na centrální úrovni bezpečnostní dohledy pro důležité systémy v rámci Ministerstva vnitra. Podle slov ředitele Tůmy se podařilo také udělat několik významných


Ing. Petr Kuchař


JUDr. Jaroslav Strouhal


Ing. Roman Vrba


Ing. Miroslav Tůma, Ph.D.

kroků v oblasti centrálních nákupů. Například rámcovou smlouvu zajištěnou Ministerstvem vnitra na produkty Microsoft využilo 115 úřadů, celková dosažená sleva je zatím cca 700 milionů korun.

Ing. **Petr Kuchař**, ředitel odboru hlavního architekta e-Governmentu, do svého vystoupení, spolu s Ing. **Michalem Peškem**, ředitelem SZR, zařadil ukázku, jak v praxi


Ing. Michal Pešek

funguje digitalizace a autentizace tak, aby přítomní snáze pochopili princip, na němž funguje Národní identitní prostor.

Protože základní registry a elektronická identita jsou pro úspěšný provoz e-Governmentu spojenými nádobami, Michal Pešek je, kromě oblíbených statistik, přiblížil jako základ propojeného datového fondu.


Jan Přerovský

STRATEGIE STÁTNÍCH PODNIKŮ

Ředitel státního podniku Národní agentury pro komunikační a informační technologie **Jan Přerovský** prezentoval roli NAKITu v rámci e-governmentu. Poslání tohoto podniku je být servisní organizací MV ČR pro oblast ICT, která by měla nejen provozovat infrastrukturu, ale rovněž začít poskytovat služby veřejné správě, posilovat roli integrátora a stát se inovačním nástrojem státu pro rozvoj ICT.

Protože NAKIT v těchto snahách bude velice úzce spolupracovat s dalším státním podnikem, SPCSS, Ing. **Vladimír Dzurilla**, generální ředitel Státní pokladny Centra sdílených služeb hovořil o strategii rozvoje služeb tohoto podniku, přiblížil bezpečné datové centrum SPCSS a řešení potřeb zákazníka volbou prostředí SPCSS. Dále prezentoval SPCSS jako subjekt kritické infrastruktury a dodavatele nezbytné dodávky dle číselníku nezbytných dodávek atd.

Ing. Vladimír Dzurilla

INICIATIVA 202020 A EVROPSKÝ POHLED

Ing. **Lucie Šestáková**, zástupkyně státního tajemníka pro evropské záležitosti, prezentovala priority koordinátora digitální agendy, kterým byl jmenován Ing. Tomáš Prouza. V rámci svého vystoupení rovněž upozornila na aktuální spuštění webu digiczech.eu, který je zaměřen na aktuality z oblasti digitální agendy, a rovněž prezentovala participaci Tomáše Prouzy na INICIATIVĚ 202020.

Právě přiblížením INICIATIVY 202020, sdělením důvodů pro její existenci a jejích cílů navázal prezident ICT UNIE Mgr. **Zdeněk Zajíček**, neboť jak uvedl, množství a kvalita on-line služeb veřejné či státní správy jsou takové, že zdaleka neodpovídají pozici, kterou zaujímá ČR v rámci mezinárodních hodnocení. Je proto nutné šířit osvětu a zároveň zvyšovat odborné vzdělávání v oblasti ICT tak, abychom o těchto službách nejen věděli, ale dovedli je rovněž využívat.

Ing. Lucie Šestáková


Mgr. Zdeněk Zajíček

O závěrečné shrnutí celého dopoledního programu se postaral **Patrik Bikar** ze společnosti CISCO, platinového partnera konference e-government 20:10. Jako specialista na digitalizaci ve státní správě regionu Evropy, Středního východu a Afriky hovořil o zkušenostech a doporučeních digitalizace státní správy v Evropě.

Odpoledne se pak program rozdělil na dvě sekce, kdy jedna byla zaměřena především na problematiku kybernetické bezpečnosti a druhá se věnovala problematice cloudu a digitalizace veřejné správy.


Patrik Bikar

Jako neveřejná část programu proběhlo setkání komise informatiků Svazu měst a obcí a komise Rady AK ČR pro informační technologie ve veřejné správě.

DOPROVODNÝ PROGRAM

Účastníci konference mohli navštívit prostory zámku v rámci večerní prohlídky a pak už následoval raut a společenský večer. Jeho nedílnou součástí je volba **Miss Egovernment 2016**. Letos byla situace do poslední chvíle napjatá, neboť ještě v úterý dopoledne byly nad zámkem v Mikulově mraky a sprchlo. Spolehli jsme se však na elektronické předpovědní prostředky, dle kterých měl být večer vlahý a příjemný a pódium postavili na nádvoří zámku. Opět jsme si tak mohli vychutnat soutěžení sympatických dam pod hvězdnou oblohou s projekcí na zámeckou zeď. Pro zlepšení nálady nás do 80. let přenesly **Děti ráje** svými nestárnoucími písněmi, které v současnosti zažívají úspěch ve stejnojmenném muzikálu, a hlavně nás zaujaly samotné soutěžící svým šarmem, humorem a pohotovostí.

Porota, které předsedala náměstkyně ministra vnitra pro řízení sekce veřejné správy Mgr. **Jana Vildumetzová**, spolu s Miss Egovernment 2015 **Hanou Pospíšilovou** za vydatné podpory náměstka ministra vnitra pro státní službu RNDr. **Josefa Postráneckého** a zástupců hlavních partnerů konference, společností CISCO a GORDIC, určila nakonec, že **Miss Egovernment 2016** se stala **Karolína Doskočilová** z České pošty s.p. Letovice. Na druhém místě byla vyhlášena **Jana Lengálová** z České pošty s.p. Brno a druhou vicemiss se stala **Michaela Boušková** z České pošty s.p. Praha 2.

Úspěch Jany Lengálové ještě podrthla skutečnost, že byla vyhlášena rovněž Miss Sympatie, tedy že kromě poroty si získala také přízeň přítomných diváků. Tyto výsledky mimo jiné znamenají, že reprezentantky České pošty tentokrát drtivě porazily zástupkyně úřadů veřejné a státní správy. Měla by to tedy být pro příští roky určitá výzva jak pro ministerstva, kraje, města, tak obce, aby nominovaly své sympatické pracovnice do soutěže.

Zábava po vyhlášení pokračovala romantickou diskotékou na nádvoří pod taktovkou zkušeného DJ **Martina Hrdinky**, který si tu a tam na pomoc přizval na živo Děti ráje.

ELEKTRONICKÁ IDENTITA NA ZÁVĚR

Závěrečný den konference e-government 20:10 již tradičně naplňuje monotematický workshop. Jeho tématem pro letošní rok byla **elektronická identita – eIdas**. Prezentovali zde a s přítomnými diváky diskutovali zástupci MV ČR, právní experti, certifikační autority, dodavatelé IT služeb v oblasti elektronické identity atd. Závěrečné shrnutí tohoto programu bylo na řediteli rozvoje produktů a služeb státního podniku Státní tiskárna cenin.

Program, prezentace a fotografie z konference e-government 20:10 naleznete na www.egovernment.cz/mikulov.

Informace o soutěži Miss Egovernment, profily jednotlivých soutěžících a fotografie ze slavnostního večera naleznete na www.egovernment.cz/miss.

Souhrn informací z MV ČR

Náměstek ministra vnitra pro řízení sekce informačních a komunikačních technologií JUDr. Jaroslav Strouhal pozdravil přítomné účastníky jménem ministra vnitra i jménem svým a vyjádřil potěšení, že může právě v Mikulově vystupovat. Nejdříve referoval o zlepšených vztazích mezi MV ČR a ICT Unií. Jak řekl, vztahy mezi ministerstvem a tímto odborným sdružením nebyly vždy úplně korektní, ale nyní, pod vedením nového prezidenta ICT Unie Zdeňka Zajíčka, se podařilo spoustu věcí nastartovat. Jaroslav Strouhal to považuje za dobrý základ pro budoucí spolupráci státu s odbornými sdruženími.

CO SE POVEDLO?

Pokud by měl Jaroslav Strouhal vyzdvihnout, co se MV ČR, případně státu v rámci elektronizace veřejné správy podařilo, upozornil by především na legislativu. Jak řekl, stát funguje na bázi zákonů a dobrá legislativa je tedy základem toho, že věci budou fungovat správně. I proto upozornil na schválení **zákona o službách vytvářejících důvěru**, který je první částí implementace nařízení eIDAS. Uvedený zákon upravuje elektronické podpisy, elektronická časová razítka a pečetě, prošel Senátem a nyní se čeká na podpis prezidenta republiky.

Jak dále náměstek Strouhal referoval, byla na jaře tohoto roku schválena **novela zákona o základních registrech**. Ta by podle něj měla, mimo jiné, umožnit lepší komunikaci občanů se státem, využívání agregovaných údajů, které má stát k dispozici, a to podle hesla „stát vyžaduje údaje od občanů pouze jednou".

CO NÁS ČEKÁ?

Při pohledu dopředu upozornil Jaroslav Strouhal na to, že MV ČR má nyní připravenu **novelu zákona o občanských průkazech**. Její ambicí je zavést jednotný identifikátor – nosič elektronické identity, a to formou občanského průkazu s čipem. Bude se jednat o základní platformu pro ověřování identity vůči službám veřejné správy, nebo jakýmkoliv elektronickým službám.

V polovině září by měla v Poslanecké sněmovně vstoupit do prvního čtení poměrně zásadní **novela zákona č. 365/2000 Sb., o informačních systémech veřejné správy**. Jak řekl náměstek Strouhal, jedná se o velkou novelu po 5 či 6 letech fungování zákona. Předmětem této úpravy má být promítnutí zásad, které vláda schválila v loňském roce v rámci usnesení vlády č. 889. Jedná se především o **zvýšení transparentnosti**. Novela tedy směřuje k efektivnímu a transparentnímu vydávání finančních prostředků na IT. To je i jeden z důvodů, proč byl i v rámci MV ČR zřízen odbor hlavního architekta, který dozoruje a koordinuje budování informačních systémů v rámci celé veřejné správy.

VIZE 2020

stát má. Především s využitím informačního systému správy základních registrů a samozřejmě i identity, které vznikly v rámci činnosti jednotlivých soukromoprávních korporací.

To byl podle náměstka Strouhala stručný přehled aktuálních legislativních kroků. V závěru svého zahajovacího slova upozornil na některé body programu konference, které jsou zajištěny ze strany MV ČR jako jejího odborného partnera. Tyto prezentace představují projekty, které mají dopad do života nás všech. Měli bychom tedy e-government vnímat jako institut, který má zkrátit či ulevit nám všem při vyřizování jakékoliv agendy. Zároveň upozornil na představení nového státního podniku, který byl založen k 1. 7. 2016 – Národní agentury pro komunikační a informační technologie jako servisní organizace MV ČR. Ambicí tohoto podniku je poskytovat IT služby celé veřejné správě, pokud to samozřejmě legislativa umožní.

Jak Jaroslav Strouhal uvedl, v loňském roce žil celý úřednický aparát implementací služebního zákona, který se po dlouhých letech podařilo, díky současné vládě, uvést v život. Ta část, která se týká úseku, jejž vede náměstek Strouhal, je **informační systém o státní službě**, který se podařilo realizovat v rekordně krátké době (v průběhu 4 měsíců). Jak zdůraznil, stalo se tak, mimo jiné, i díky zmíněnému NAKITu. V současné chvíli tento systém standardně funguje a je v něm zahrnuto zhruba 80 000 úředníků se všemi atributy, které předvídá zmíněný zákon o státní službě. Dále uvedl, že byl rovněž postaven také registr smluv a od 1. 7. 2016 tento informační systém funguje a všechny povinné subjekty do něj standardně přispívají. Těch projektů, které MV ČR realizuje, ať dovnitř úřadu, nebo směrem ven, je celá řada. V závěru svého vystoupení proto náměstek ministra vnitra Jaroslav Strouhal pozval účastníky konference na jednotlivé přednášky s přesvědčením, že i ty mohou přispět k našemu lepšímu vnímání toho, co stát v oblasti elektronizace dělá.

eIDAS

Jak Jaroslav Strouhal uvedl, v tuto chvíli je dokončen draft návrhu **zákona o elektronické identitě**. Podle jeho mínění se jedná se o nutný základ, který navazuje na již schválený zákon o službách vytvářejících důvěru a má sjednotit prokazování elektronické identity vůči službám, které buď nabízí stát, nebo jsou realizovány na základě soukromoprávních subjektů. Tato norma podle slov Jaroslava Strouhala počítá s využitím stávajících platforem, které

Letem světem e-governmentem

Další vystupující, ředitel odboru eGovernmentu MV ČR, Ing. Roman Vrba řekl, že nazval své vystoupení Letem světem e-governmentem, protože je velmi mnoho témat, o kterých by chtěl referovat, a jen málo času.

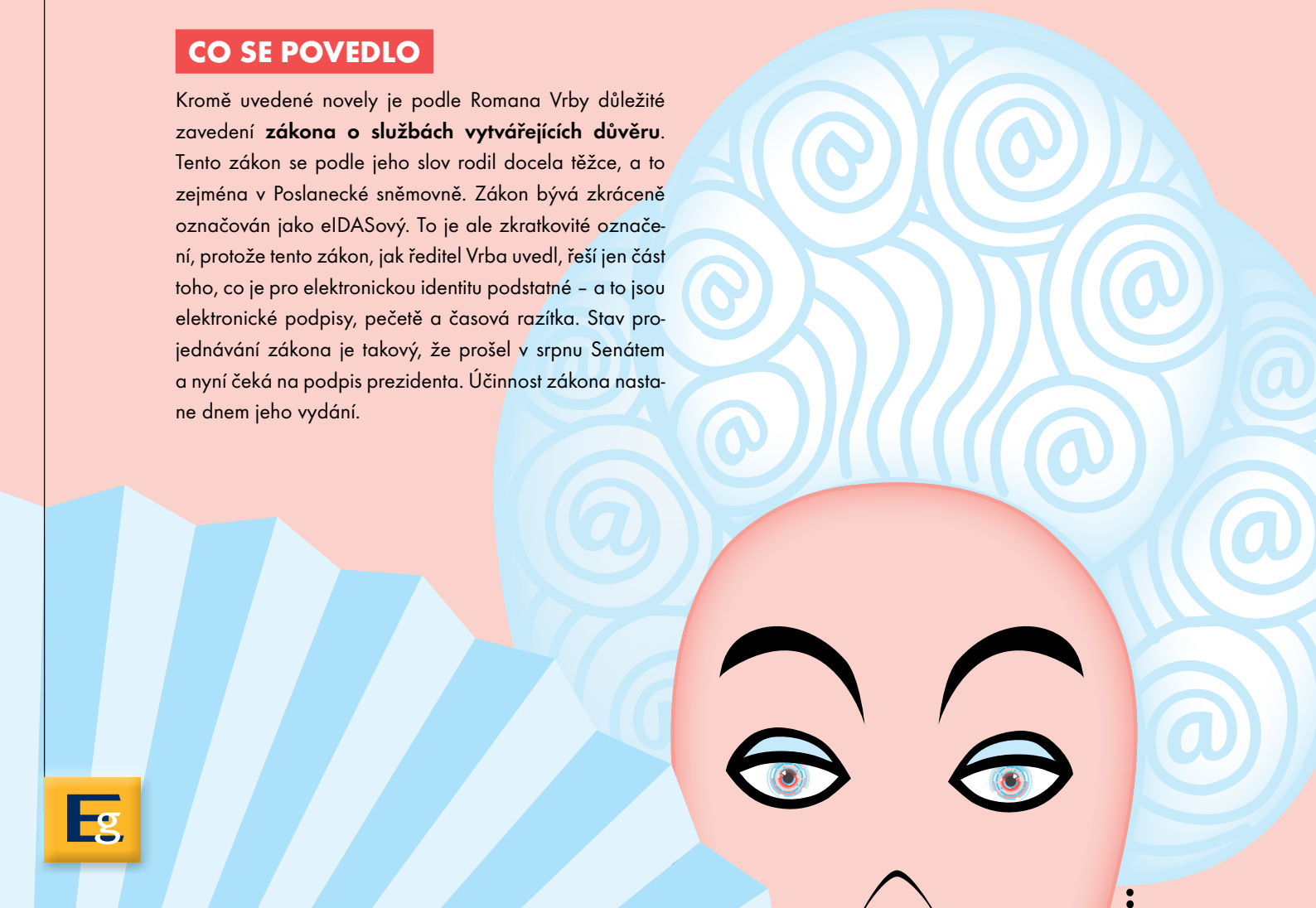
Z pohledu legislativy je velice důležité, že nyní dochází na první technickou novelu od spuštění zákona o základních registrech. A jak zdůraznil, jedná se o novelu zcela zásadní, neboť umožňuje vstup do základních registrů orgánům veřejné moci. Konkrétně se jedná o **zákon č. 192/2016 Sb.** ze dne 25. května 2016, kterým se mění zákon č. 111/2009 Sb., **o základních registrech**. Novela obsahuje právní ukotvení JIP KAS pro OVM, které mohou využívat systém pro autentizaci svých uživatelů v agendách. Datum nabytí účinnosti je 1. 7. 2017, s výjimkou některých ustanovení.

CO SE POVEDLO

Kromě uvedené novely je podle Romana Vrby důležité zavedení **zákona o službách vytvářejících důvěru**. Tento zákon se podle jeho slov rodil docela těžce, a to zejména v Poslanecké sněmovně. Zákon bývá zkráceně označován jako eIDASový. To je ale zkratkovité označení, protože tento zákon, jak ředitel Vrba uvedl, řeší jen část toho, co je pro elektronickou identitu podstatné – a to jsou elektronické podpisy, pečetě a časová razítka. Stav projednávání zákona je takový, že prošel v srpnu Senátem a nyní čeká na podpis prezidenta. Účinnost zákona nastane dnem jeho vydání.

CO JE V PROCESU

Krátce po konání konference v Mikulově vstoupí do prvního čtení ve Sněmovně **novela zákona č. 365/2000 Sb., o informačních systémech veřejné správy** (na programu je 14. září). Novela modifikuje pravidla pro řízení, ekonomickou efektivitu a funkční vlastnosti informačních systémů. Dále upravuje koordinační roli MV ČR v oblasti dlouhodobého řízení informačních systémů veřejné správy. Předpokládá se nabytí účinnosti 1. ledna 2017.
Velmi důležitým zákonem do celé mozaiky elektronické identity je **zákon o občanských průkazech**. Zákon zavádí nové elektronické občanské průkazy, a to pro



všechny bez poplatku. Elektronickou identitu si může držitel aktivovat při převzetí OP, nebo kdykoliv později. Zákon nyní posuzuje legislativní rada vlády. Předpokládáme, že během září by se měl dostat na jednání vlády a na 50. schůzi PSP by měl být zařazen do prvního čtení. **Účinnost je stanovena prvním dnem dvanáctého kalendářního měsíce následujícího po jeho vyhlášení.**
Dalším z důležitých zákonů je podle Romana Vrby **zákon o elektronické identifikaci**. Je klíčovým proto, aby identifikace fungovala, neboť jeho hlavním cílem je položit základy státem garantované identity osob prokazované elektronicky. Za zajímavou považuje skutečnost, že se jedná o první zákon, který byl nejdříve modelován procesně, a pak teprve navazovala práce na paragrafovém znění. Roman Vrba předpokládá, že jak veškerá legislativa, tak technická řešení by měla být účinná a funkční k 1. 1. 2018.

REGISTR SMLUV

V případě registru smluv Roman Vrba nejprve upozornil na řadu webových adres:
provozní prostředí je na www.smlouvy.gov.cz;
testovací prostředí je na www.isrs.cz;
metodika je na www.mvcr.cz/clanek/registr-smluv.aspx;
dotazy je možné klást na adrese registrsmluv@mvcr.cz.

Zákon o registru smluv byl publikován ve Sbírce 14. 12. 2015. To znamená, že čas na vytvoření registru byl skutečně minimální. V průběhu května a června proběhla Roadshow k registru smluv (jedno zastavení bylo natočeno na YouTube a podle statistických údajů mělo zatím přes 6000 zhlédnutí). Zároveň bylo 1. 5. 2016 spuštěno interní testování a 1. 6. 2016 veřejné testování tohoto registru. Ostrý provoz naběhl 1. 7. 2016 a první smlouva zde byla zveřejněna v 00:17 min., tedy čtvrt hodiny po půlnoci a začátku ostrého provozu.
Jedná se o systém, který sdílí a využívá služeb e-governmentu – příjem smluv je řešen pře ISDS, správa rolí přístupu využívá JIP/KAAS, CMS přístup do internetu a řízení zátěže. Celý tento systém běží ve dvou krajských datových centrech, a to Kraje Vysočina a Plzeňského kraje.
Jak dále Roman Vrba uvedl, celkový počet doposud přijatých smluv (k 6. 9. 2016) je 45 000, platných smluv je 44 153, počet publikujících subjektů je 1965. Podle jeho slov je počet subjektů, které musí povinně zveřejňovat, cca 7–8 000. To znamená, že většina subjektů zatím nezveřejnila žádnou smlouvu.

TEST eIDENTITY V CHYTRÉM MOBILU

Při obhajování zákona o službách vytvářejících důvěru bylo ve Sněmovně Ministerstvu vnitra ČR vyčítáno, že se nevěnuje mobilní identitě. Proto spustili pilotní ověření identity v chytrém mobilu. Hlavním důvodem je podle slov Romana Vrby prudký nárůst právě mobilních zařízení. V krátké budoucnosti se očekává, že až 70% těch, kteří budou využívat elektronických služeb v kontaktu s veřejnou správou, bude k tomu používat právě chytré telefony, tablety a další obdobná zařízení. Proto je důležité, aby tady vznikal další ID provider v tomto smyslu.
Celý test prokázal, že proces je velmi jednoduchý a v budoucnu by mohl vypadat tak, že by využíval například stávající Czech POINTy. Konkrétně se zájemce o možnost elektronické identifikace prostřednictvím svého mobilu dostaví na Czech POINT s konkrétním aparátem, zde se identifikuje pomocí OP a díky QR kódu dojde ke spárování identity této osoby a jejího mobilního telefonu. Následně může využívat elektronickou identitu v mobilu například k autentizaci mobilních aplikací.

CO DALŠÍHO?

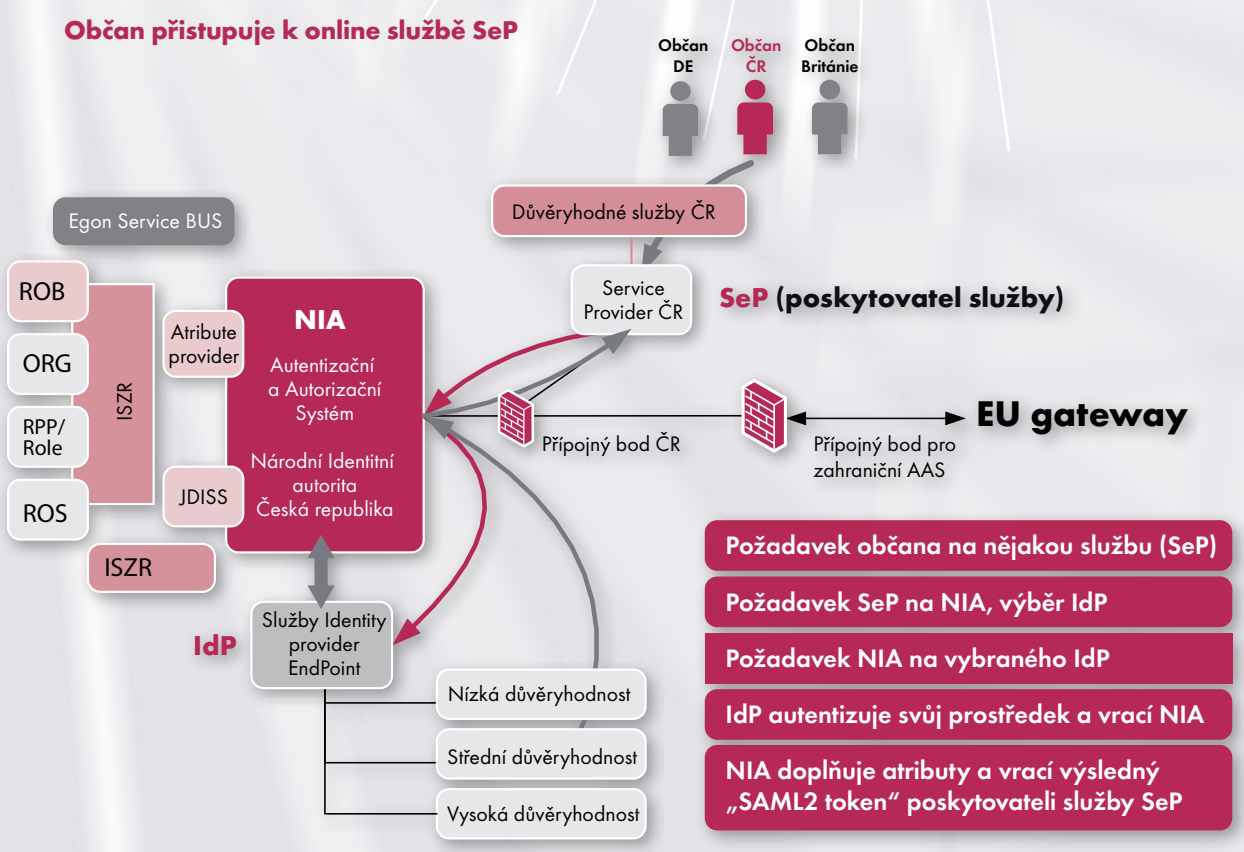
Kromě těchto hlavních kroků považuje Roman Vrba rovněž za důležité upozornit na některé další aktivity v rámci MV ČR. Jednou z nich je Geoinstrategie. Jak uvedl, nyní se bavíme o jednotné digitální technické mapě, o standardech pro výměnu geodat atp. Je ale především důležité upozornit na to, že se jedná o důležité téma, neboť geodatům se podle jeho mínění vždy věnovalo poněkud málo pozornosti.
A úplně na závěr svého vystoupení upozornil na dvě velká témata, která získávají na důležitosti, a to aplikaci procesního modelování do veřejné správy, dále Portál občana a ISDS, především jeho další vývoj po roce 2018.

Národní identitní prostor

Aby celý e-government fungoval a bylo skutečně možné nasadit elektronické prostředky, je potřeba dořešit elektronickou identitu tak, aby občan byl schopen elektronicky doložit, že se jedná právě o něj a že tedy všechny úkony, o které žádá, se skutečně mohou činit jeho jménem. To byla základní teze, s níž Ing. Petr Kuchař, hlavní architekt eGovernmentu MV ČR začal své vystoupení. Jak řekl, prostor, v němž se děje prokazování a kde se pracuje s touto identitou, nazýváme Národní identitní prostor (NIP).

NIP sestává v zásadě ze tří skupin subjektů, proto se nazývá federací. Jednak se jedná o skupinu **kvalifikovaných poskytovatelů** on-line služeb. Z technického pohledu se jedná o servis providery, tedy například portály jednotlivých rezortů (například portál České správy sociálního zabezpečení). Jak Petr Kuchař upozornil, může se ale jednat i o portály soukromoprávní, neboť do budoucna se počítá s rozšířením NIP i na soukromoprávní uživatele. Aby systém fungoval, potřebuje tato skupina provozovatelů služeb dostat identity službu od druhé skupiny, tzv. IdP providerů, což jsou kvalifikovaní správci kvalifikovaných systémů. Pro dodržení pravidel je nutné, aby byl přítomen třetí subjekt, který dohlíží na jejich dodržovaní, kterým bude Národní identitní autorita (Národní bod identifikace). Provozovatelem systému by měla být Správa základních registrů.

Pro dokumentaci fungování identitního systému zařadil Petr Kuchař, spolu se svými kolegy a za pomoci Michala Peška, ředitele SZR, scénku, která přibližovala, jak v budoucnu zareaguje portál ČSSZ v roli poskytovatele on-line služby na požadavek o přihlášení uživatele zaručenou elektronickou identitou.



OBECNÉ PRINCIPY FEDERACE NIP

Petr Kuchař zdůraznil, že úkolem NIA je vést evidenci kvalifikovaných subjektů a oddělovat je od sebe.

NIA tedy odděluje skupinu identity providerů od skupiny IdP providerů. Servis provider totiž nesmí vědět, jakým kvalifikovaným prostředkem se uživatel přihlásil, potřebuje pouze informaci, že toto přihlášení bylo kvalifikované a že bylo realizováno na určité úrovni důvěry. Opačně identity provider nemá, podle slov hlavního architekta, proč vědět, pro jakého poskytovatele služeb poskytoval svoji službu. Neměl by tedy shromažďovat informace, k jakým portálům se ten který uživatel hlásil, koho je klientem atd. Uvedená federace je tedy navržena právě proto, aby od sebe oddělovala tyto dvě skupiny.

V této souvislosti Petr Kuchař znovu připomněl zákon o elektronické identifikaci, který vznikal tak, že odbor hlavního architekta předložil věcný záměr, pracoval na metodickém materiálu a odbor eGovernmentu koordinoval psaní toho zákona. Odbor legislativy pak pořídil jeho paragrafové znění. Podle Petra Kuchaře by měl být zákon předložen do konce tohoto roku, nyní ještě proběhnou nějaká interní připomínkovací kolečka.

PRINCIP ZoEI

Samotnému zákonu a především některým jeho pojmům se Petr Kuchař věnoval podrobněji. Zákon, jak řekl, předvídá použití tzv. kvalifikovaného systému elektronické identifikace, a to za dvou podmínek:

1. vyžaduje-li právní předpis vůči osobě prokázání totožnosti jednajícího;
2. umožní-li osoba, o kterou se jedná, prokázání totožnosti elektronickým způsobem.

Kvalifikovaný systém elektronické identifikace je systém, jehož správcem je identity provider. Musí splňovat rámec interoperability, systém musí umožnit komunikaci s Národní identitní autoritou. V rámci tohoto systému je pak vydáván nějaký prostředek (občanský průkaz, mobilní průkaz identity v telefonu, jméno a heslo do datové schránky atp.).

Povinnosti kvalifikovaného správce – IdP provider musí zejména poskytovat svoji službu nepřetržitě, vést evidenci prostředků, které vydal, musí tyto prostředky nahlásit Národní identitní autoritě, musí umět přijímat žádosti o zneplatnění prostředku. Pokud by subjekt IdP providera přestal z jakéhokoliv důvodu existovat, je jeho povinností poskytnout součinnost státu při předání toho identitního kmene.

Kvalifikovaná on-line služba – poskytovatel služby (portálu) musí být kvalifikovaným poskytovatelem, musí být tedy nahlášen u NIA a splňovat její technické podmínky připojení. Samotná služba musí dopředu sdělovat klientovi, jaká data bude o něm od Národního identitního systému požadovat.

Národní identifikační autentizační bod NIA je informační systém veřejné správy, který slouží k identifikaci prostřednictvím kvalifikovaného systému. Jedná se o agendový informační systém, tzn., že má přístup do základních registrů. Z hlediska regulace eIDAS je to rozhodně národní uzel, jenž je místem, které bude v budoucnu napojeno na ostatní uzly dalších členských států Evropské unie. Nařízení eIDAS nám totiž ukládá od září 2018 rozeznávat elektronické identity přišlé z jiných států, tedy od IdP providerů nahlášených v jiných státech. Národní identitní autorita vede konkrétní údaje – identifikátor prostředků, AIFO držitele, BSI pro obě strany kontaktu, případně další údaje, které si o sobě vyplní daný klient veřejné správy.

Jak v závěru Petr Kuchař slíbil, bude se MV ČR spolu se svými partnery snažit toto vše splnit do roku 2018 tak, aby systém skutečně fungoval.

Základní registry a eIDAS

Ředitel SZR Ing. Michal Pešek otevřel své vystoupení výčtem statistických údajů a především upozornil na skutečnost, že v rámci základních registrů bylo učiněno 1 080 000 000 transakcí. Jak uvedl, v přepočtu to znamená, že na údaje o každém z nás, uložené v základních registrech, se „šáhlo".

Michal Pešek zdůraznil, že je nutné stavět na datovém fondu a vycházet ze skutečnosti, že zde již takový existuje, a to v rámci celého státu. Jedná se přitom o záležitost, kterou nemá v rámci EU vyřešenu mnoho zemí. Jako problematickou vidí skutečnost, že v současné době je velmi mnoho novel zákonů, ve kterých určitě není jednoduché se vyznat. A je docela dobře možné, že to novelizační tempo je až zbytečně vysoké. Určitě je nutné se trochu zastavit a dát prostor technickému řešení. Ke každé legislativě je podle jeho slov potřeba udělat a nastavit určité konkrétní technologie a je pravdou, že ty se ve státní správě nevytvářejí zrovna závratným tempem. Musíme si uvědomit, že v této souvislosti hovoříme o pěti novelách zákonů najednou:

- základních registrech;
- kyberbezpečnosti;
- evidenci obyvatel;
- eIDAS;
- elektronických občanských průkazech.

Bohužel jednotlivé systémy spolu úzce souvisejí a každá novela zákona vyvolává změny uvnitř systémů, které se mezi sebou přelévají, proto jde o velice náročný proces.

CO JE NOVÉ?

Rozhodně se, podle Michala Peška, jedná o nový pohled na podporu občanů. Zároveň ale upozornil, že bude-li Správa základních registrů realizovat na základě zákona podporu v oblasti elektronické identifikace, rozhodně nepůjde o jednoduchou záležitost. SZR totiž nemá pracovat s daty občanů, přitom ale bude mít patrně zákonem uloženo, aby s některými daty pracovala. To jsou záležitosti, které se budou muset ještě, alespoň podle názoru ředitele SZR, legislativně upravit.

ZÁKLAD PROPOJENÉHO DATOVÉHO FONDU

Základní registry jsou základem propojeného datového fondu a dokládá to mimo jiné statistika z úvodu prezentace. Věnoval se tedy podrobněji jednotlivým projektům:

eGon Service Bus – informační systém základních registrů je určen pro to, aby stále komunikoval se čtyřmi základními registry. eGon Service Bus „sedí" vedle informačního systému základních registrů a přejímá to, co je nastaveno v registru práv a povinností. Přebírá tedy pouze informace o tom, kam se kdo může dostat. Zároveň umožňuje agendovým informačním systémům (AIS), aby nabídly data tomu, kdo může být jejich odběratelem. Jak Michal Pešek podtrhl, jsou tedy takto rozšiřovány jednotlivé služby tak, jak bylo naplánováno.

eGon Service Bus a propojování AIS jako samoobsluha – jedná se o projekt, který byl již ukončen. MV ČR s NAKITem toto řešení vyvinulo a cílem SZR je dále jej rozvíjet. Vedle základních registrů je nutno rovněž propojovat OVM mezi sebou, aby mohly sdílet navzájem data, která nabízejí tak, aby se nebudovaly paralelní datové fondy.

Michal Pešek dále uvedl, že projekty, které realizuje SZR, primárně navazují na projekty, které jsou rozběhnuté již řadu let. V souvislosti s CMS 2 se jedná o projekty, které mají souvislost s dohledy (DCGeOV), jež je nutné dobudovat především v rámci zákona o kybernetické bezpečnosti.

SZR skutečně upíná svoji pozornost na MORIS. Jak Michal Pešek uvedl, bylo zahájeno budování infrastruktury, tedy projekt, který sestává spíše z několika dílčích částí.
Tou první částí je otázka, jak budeme pracovat s eID? Je to podle Michala Peška fáze, která se už blíží do určitého finále. Především v rámci Národní identitní autority využijeme to, co legislativa umožňuje. Má na mysli především datové schránky, které fungují jako ID provider. Není pro ně nutné měnit žádnou legislativu, stačí pouze začít využívat možností, které takto nabízejí. V oblasti elektronické identity je dle slov Michala Peška hodně daleko Česká správa sociálního zabezpečení se svým portálem. Již více než rok zde funguje možnost přihlásit se na portál pomoci ID datové schránky. Stejný princip chce využít SZR. Budoucnost je bezpochyby v elektronickém občanském průkazu, ale nyní ještě legislativa v tomto smyslu schválena není, a je tedy nutné využít pouze toho, co je stávající legislativou umožněno.

eIDENTITA.CZ

Správě základních registrů se podařilo zaregistrovat doménu **eIdentita.cz**. Jak Michal Pešek uvedl, bude patřit k portálu, který bude rozcestníkem pro využívání služeb jak service providerů, tak ID providerů. Na této identifikační bráně by skutečně měla samotná identifikace probíhat, tzn., že dojde k ověření identity uživatele (občana), který hodlá poskytnout nějaké své údaje konkrétnímu poskytovateli určité služby. Pokud je identita ověřena, dojde k jejímu propojení se záznamem v registru obyvatel a vybranému poskytovateli služby jsou odeslány požadované údaje. V současnosti se tak může stát pouze na základě požadavku, kdy občan chce poskytnout nějaká data směrem ke státní správě. Do budoucna pak bude možné takto postupovat i směrem k soukromoprávním subjektům.

Michal Pešek dále ukázal, jak bude vypadat NIA portál. Ten přímo souvisí s portálem občana. Podle Michala Peška je zbytečné vyvíjet věci, které jsou již k dispozici, a tak portál občana bude front end, který čerpá ze základních registrů, a mezi tím je nějaká aplikační úroveň Národní identity. Zároveň musíme podle Michala Peška uvažovat o agendovém informačním systému pro identifikaci a autorizaci, protože i NIA bude muset splnit zákon č. 365/2000 Sb., o informačních systémech veřejné správy. To znamená, že bude muset být zaregistrována jako platný agendový informační systém. Funkčně bude NIA zajišťovat propojování, a tedy podstatu pro identifikaci fyzických i právnických subjektů. Musí tedy akceptovat existující ID providery a poskytovat identity tak, aby byly oddělitelné od poskytovatelů služeb. Identita bude tedy vždy spojena s konkrétním AIFem.
Michal Pešek v této souvislosti připomenul, že je rozdíl v termínech využívání dat a poskytování dat. Zatímco využívání dat znamená, že konkrétní instituce mohou, případně musí na základě zákona využívat pro výkon určité agendy data vedená v ZR a činí tak bez našeho vědomí (vyjma informačního výpisu), poskytování je úkon, kdy občan dává souhlas konkrétní instituci k použití jeho dat nad rámec daný legislativou.

CO NÁS ČEKÁ?

Jak Michal Pešek v závěru svého vystoupení uvedl, realizace Národní identitní autority je realizací státní certifikační autority. Navazujeme tedy na to, co zde bylo vyvinuto již s datovými schránkami, nastavujeme procesy mezi ID providery a státní certifikační autoritou a například mezi OP (do budoucna) a musíme dokončit legislativní opatření tak, aby systémy pracovaly v souladu s příslušnými standardy. Rovněž je nutné zajistit vše potřebné, aby fungovaly certifikáty, a otestovat vhodné čtečky pro úředníky.
V souvislosti s NIA je nutné vytvořit uživatelskou dokumentaci (měla být k dispozici od 1. 11. 2016). Ve stejném termínu bude NIA spuštěna k testovacímu provozu a k ověřovacímu provozu bude uvolněna 2. 1. 2017.

3C – Cloud computing, Centrální nákupy a dohledové centrum e-governmentu

Ředitel odboru kybernetické bezpečnosti a koordinace ICT MV ČR Ing. Miroslav Tůma, Ph.D., ve svém vystoupení prezentoval stručný vývoj strategického rámce Národního Cloud computingu, tedy eGovernment cloudu ČR. Dále rekapituloval, jak se vyvíjí centrální zadávání státu, a to především v oblasti softwarových produktů, a na závěr krátce informoval o dohledovém centru eGovernmentu, především o části SOCCR, tedy o zajištění kybernetické bezpečnosti, protože jak zdůraznil, všechny uvedené informační systémy a služby, o nichž již hovořili jeho předřečníci, musí být skutečně důsledně zabezpečeny.

CLOUD COMPUTING

Jak Miroslav Tůma upozornil, strategický rámec Národního Cloud computingu – eGovernment cloud (sGC) vychází z akčního plánu k Národní strategii kyberbezpečnosti 2015–2020.

Po půlročním vyjednávání a odlaďování bylo, po třech kolech připomínkového řízení v rámci jednotlivých rezortů a odborné veřejnosti, dosaženo aktuální verze strategického rámce. Náročnost tohoto procesu dokladoval skutečností, že se jedná o 45. verzi. Právě v týdnu, kdy se konala konference v Mikulově, byl dokument „vypuštěn" do mezirezortního připomínkového řízení a na konci září by měl být předložen vládě.

Podstatná, podle Miroslava Tůmy, je skutečnost, že dokument stanovuje, že se ČR vydá cestou budování cloudu pro veřejnou správu, v němž by měly být dvě části – státní a komerční.

Zatímco do „státní" části budou umisťovány informační systémy pouze na základě jasné právní úpravy, do komerční budou vpuštěny ostatní informační systémy na základě obvyklých výběrových řízení.

Princip budování a využívání cloudu spočívá v zefektivnění základního využití především HW prostředků veřejnou a státní správou tak, aby nedocházelo ke zbytečnému budování několika nových separátních datových center. Mělo by naopak dojít k jejich konzolidaci a především díky cloudu ke zvýšení bezpečnosti a snížení nákladů na provoz. Tím by, mimo jiné, mělo být zajištěno, že se státní správa zaměří na správu klíčových procesů, nikoli na správu ICT.

Jak Miroslav Tůma uvedl, jsme nyní ve fázi, kdy je strategický rámec předkládán vládě. Následovat bude první fáze, tedy příprava vybudování eGovernment Cloudu. Ta zahrnuje přípravu projektu, včetně všech analýz a dopadů. Další pak bude fáze realizační (budování cloudu) a fáze standardizační. Podle slov Miroslava Tůmy by měl být detailní projekt (první fáze) připraven do konce roku 2017.

MV ČR, podle jeho slov, předpokládá, že vláda vypracování tohoto projektu schválí. V reakci na to by měla být vytvořena pracovní skupina pod Radou vlády pro informační společnost, která bude složena ze zástupců MV ČR, MF ČR, NBÚ, dalších rezortů, zpravodajských služeb a odborné veřejnosti. Tato pracovní skupina, mimo jiné, vytvoří analytickou zprávu zaměřenou na:

- požadavky na státní a komerční část – provozní, bezpečnostní, SLA;
- analýzu IS státu – stanovení strategických IS státu;
- stanovení standardů eGC – platforem, služeb;
- stanovení jasných a přesně specifikovaných výjimek;
- zajištění právní podpory (zákon č. 365, zákon č. 137 atd.);
- kalkulace potřebných kapacit státní části;
- analýzu datových center státu – současné kapacity;
- pravidla financování státní části eGC;
- proces umístění IS do eGC – metodika migrace;
- metodiku hodnocení efektivity umístění IS do eGC – TCO.

Na konci příštího roku (2017) bude možné na základě těchto kroků předložit vládě jednoznačný projekt budování eGC ke schválení. Z něj bude zřejmé, co znamená Cloud, jaké má pro veřejnou správu výhody a jaké sebou nese nároky. Na vládě pak bude, aby učinila další rozhodnutí.

CENTRÁLNÍ NÁKUPY

V oblasti centrálních nákupů, jak Miroslav Tůma informoval, existují dvě skupiny:

- centrální nákupy sw produktů velkých výrobců;
- centrální nákupy ICT komodity (zastřešuje úkol, vycházející z usnesení vlády z května loňského roku, kdy stát má zajišťovat nákupy vybraných komodit, přičemž ICT komodita je jednou z nich).

V rámci sw produktů podle slov Miroslava Tůmy už nákup probíhá. V rámci ICT komodity se připravují standardy pro centrální zadávání a centrální nákupy, proto dále věnoval pozornost jednotlivým centrálním sw nákupům:

Microsoft

- Smlouva uzavřena v 12/2014 na 4,6 mld. Kč bez DPH s pěti dodavateli,
- expiruje 11/2018;
- Dosud bylo čerpáno 2,042 mld. Kč bez DPH, zbývá dočerpat 2,558 mld. Kč s DPH;
- Do dnešního dne využilo rámcovou smlouvu 115 subjektů OVM;
- Celková dosažená sleva je zatím 697 mil, což činí 24,94 % z ceníkových cen.

VMware

- Dne 15. 8. 2016 vydalo MV na základě doporučení hodnotící komise rozhodnutí o výběru pěti dodavatelů;
- K dnešnímu dni došly proti tomuto rozhodnutí dvě námitky, které se v současné době posuzují.

Cisco Systems

- Výběr 5 dodavatelů RS – následně budou prováděny minitendry a uzavírány prováděcí smlouvy;
- Termín zahájení výběrového řízení – říjen 2016;
- Vzhledem k účinnosti nového ZZVZ budou osloveni všichni pověřující zadavatelé s dodatkem ke smlouvě o centralizovaném zadávání z důvodu úprav proti stávajícímu ZVZ.

IBM

- Rámcová smlouva je koncipována na možnost nákupů:
  i. dle ceníku s vysoutěženou slevou,
  ii. formou AYCE (All you can eat) z předem definovaných balíčků pro jednotlivé subjekty nebo s možností uzavírat AYCE v době trvání rámcové smlouvy,
  iii. formou AYCE, které budou požadovány i v průběhu trvání RS;
- Termín zahájení výběrového řízení – listopad/prosinec 2016.

Oracle

- Soutěž vybere pět dodavatelů RS – následně budou prováděny minitendry a uzavírány prováděcí smlouvy;
- Nákup bude možný dle ceníku s vysoutěženou slevou nebo formou ULA (Unlimited Licence Agreement);
- RS umožní pořizování:
  - technické podpory pro stávající licence 22% z ceny licence plus garantované maximálně 3 % meziročního navýšení.
  - pořízení nových licencí, včetně podpory (garance max. 2% meziročního navýšení);
- Možnost uzavření smlouvy k centralizovanému zadávání;
- Předpokládaný termín zahájení soutěže – říjen/listopad 2016;
- I v případě této soutěže osloví MV pověřující zadavatele s dodatkem ke smlouvě z důvodu úprav dle nového ZVZ.

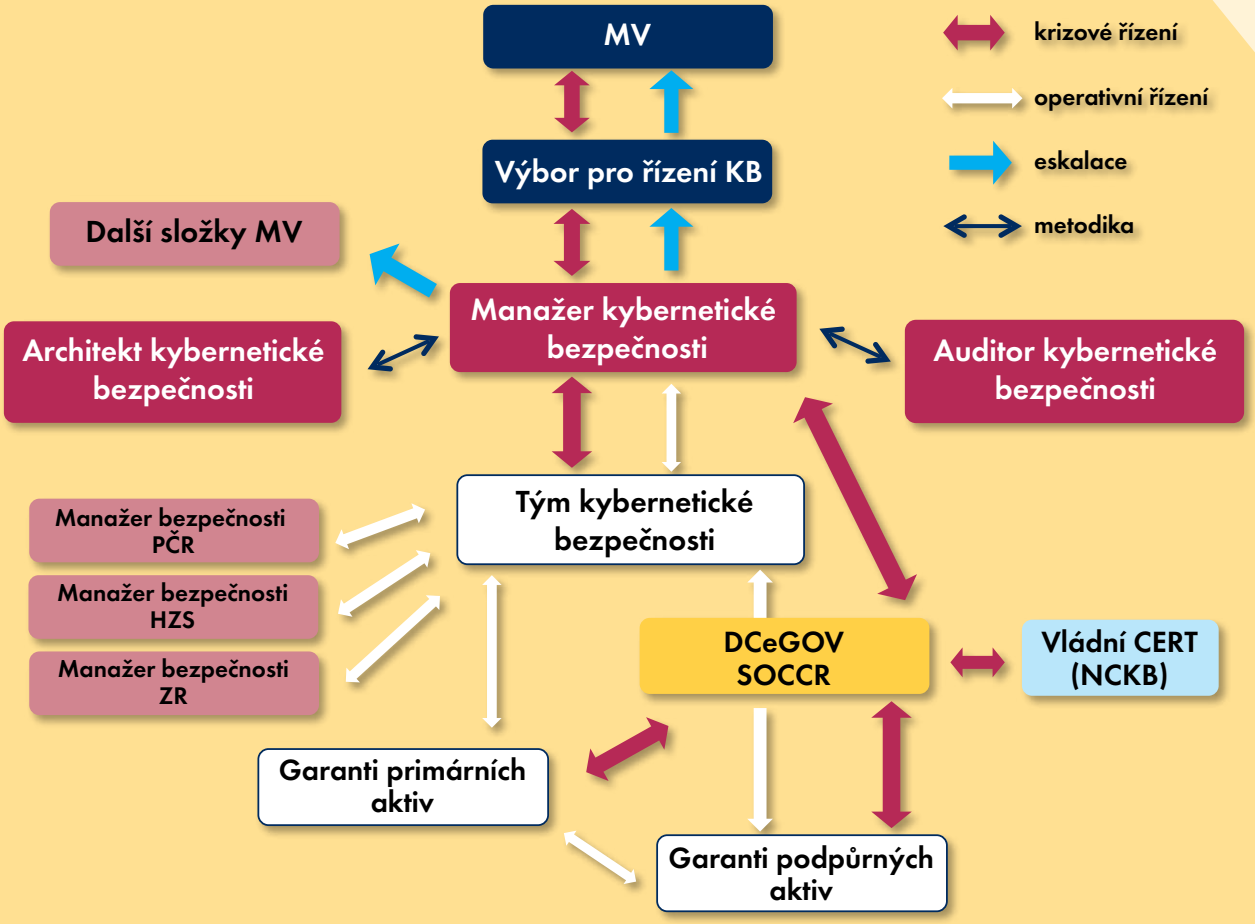
Dotazy k tématu centrálních nákupů
je možné směrovat na Ing. Ivo Rosypala
ivo.rosypal@mvcr.cz.

DOHLEDOVÉ CENTRUM eGOVERNMENTU

Dohledové centrum je podle slov Miroslava Tůmy velice důležité, neboť všechny systémy, o nichž se zde v předchozích vystoupeních hovořilo, je potřeba zabezpečit a zajišťovat dohled. Tyto systémy totiž byly určeny buď jako součást kritické infrastruktury státu, nebo jako významné informační systémy. Miroslav Tůma v této souvislosti zdůraznil, že jen samotné MV ČR má 18 systémů v rámci kritické informační infrastruktury a 9 významných informačních systémů. Zabezpečení je nutné nejen z pohledu zákona o kybernetické bezpečnosti, ale i proto, aby systémy byly skutečně dostupné, věrohodné a sloužily danému účelu. I proto bylo vybudováno dohledové centrum, které pracuje v režimu 24x7 a 365 dní v roce monitoruje infrastrukturu a hlídá, vyhodnocuje a předchází bezpečnostním událostem a incidentům tak, aby systémy byly stále k dispozici.

Dohledové centrum je zařazeno do organizace MV ČR v rámci řízení kybernetické bezpečnosti.
Sestává ze dvou částí – z řídící a dohledové části. Jak referoval Miroslav Tůma, k 31. 3. 2016 se podařilo spustit plně funkční dohledové centrum v oblasti bezpečnostních dohledů - SOCCR a byly zahájeny práce na NOKu – provozním dohledu a napojování ostatních systémů do vyšší úrovně dohledu a zabezpečení.

Organizační zapojení DCeGOV



VIZE 2020

Základní pilíře DCeGOV

- CALL CENTRUM / příjem událostí;
- SOCCR / bezpečnostní proaktivní dohled;
- NOC / provozní proaktivní dohled.

Základní vlastnosti DCeGOV

- Soulad se ZoKB (zákon č.181/2014 Sb.) a ISO standardy;
- Geograficky redundantní řešení – vysoká dostupnost;
- Řízení bezpečnosti systémů v aktivním a pasivním módu;
- Zajištění proaktivního dohledu;
- 14 konektorů na úrovni krajů pro napojení krajských prvků a rozšíření monitoringu do všech přípojných uzlů síti MV;
- Vytváření efektivních procesů pomocí portálu Service Desk;
- Koordinace týmů (SOCCR, TKB, ...);
- Provoz 24x7x365;
- Modulární architektura, vlastní aktivní ochrana, znalostní databáze.

SOCCR zajišťuje dohled a hlavně online komunikaci s NCKB a ostatními složkami, které mohou přenášet informace a hlavně základní modely řešení jednotlivých krizových situací. Service Desk je podle mínění Miroslava Tůmy zpracován v poměrně robustní architektuře, která není určena pouze pro systémy MV ČR. Je rozprostřena do 14 krajů a dochází zde ke korelaci jednotlivých událostí a logů. Jak Miroslav Tůma uvedl, jsme tedy připraveni připojovat celou řadu systémů podle potřeby. Celá struktura je postavena na procesní organizaci tak, aby byly definovány produkty z jednotlivých procesů i to, které procesy a jak na sebe navazují.

V závěru svého vystoupení Miroslav Tůma nastínil, jak bude vypadat další rozvoj dohledového centra:

- analytické nástavby pro vyhodnocování NetFlow;
- nástroje pro identifikaci botnetů;
- technologie pro monitoring, filtraci a antimalware ochranu protokolů http, ftp, a to i šifrovaných;
- nástroje na simulace řízení kritických situací;
- billing;
- nástroje forenzní a BI analýzy pro rezort;
- rešerše a sledování aktuálních hrozeb;
- rešerše a sledování aktuálního technologického rozvoje;
- spolupráce s významnými pracovišti typu SOC.

Digitální agenda a Iniciativa 202020

Ing. Tomáš Prouza, MBA

- Narozen v roce 1973 v ocelovém srdci republiky, od 18 let žil v Praze na Vinohradech. Vystudoval ekonomii, diplomacii a žurnalistiku a každý z těchto oborů jej někdy živil. Jako novinář založil největší finanční server Peníze.CZ, ekonomii a diplomacii se věnoval jako náměstek ministra financí zodpovědný za fiskální politiku, finanční služby, evropské a zahraniční vztahy. Spoluzakládal finančně-poradenskou firmu a v roce 2012 se přestěhoval do svého dalšího oblíbeného města, Washingtonu, a pracoval pro Světovou banku.
- V lednu 2014 se vrátil do Prahy a od té doby se věnuje české evropské politice. Vedle zlepšení naší pozice v Bruselu i u partnerů a boje o srozumitelnost našeho přístupu k Evropě ho baví i otázka zavedení eura – ostatně byl od roku 2005 prvním „panem Euro" v České republice.
- V květnu 2016 ho česká vláda jmenovala koordinátorem digitální agendy ČR. Jeho úkolem je koordinovat a moderovat diskusi rezortů, hospodářských a sociálních partnerů a byznysu v oblasti digitální ekonomiky, která byla dříve roztříštěná. Jeho pěti prioritami jsou: e-skills, e-commerce, e-government, e-bezpečnost a e-výzvy.
- Rád čte (jen nemá kdy), rád poslouchá klasickou hudbu a chodí na operu, a pokud chce opravdu relaxovat, stará se o růže na zahradě, což je rodinná tradice už ve třetí generaci.

Státní tajemník pro evropské záležitosti Ing. Tomáš Prouza, MBA, byl v květnu tohoto roku jmenován koordinátorem digitální agendy ČR. Navštívili jsme je, abychom zjistili, co přesně je úkolem takového koordinátora, co může a musí řešit a jaké jsou jeho priority a plány.

V květnu tohoto roku jste byl jmenován koordinátorem digitální agendy ČR. Co přesně tato funkce obnáší? Koho a jak můžete koordinovat, kam v tomto smyslu sahají Vaše pravomoci – jedná se skutečně o koordinaci ve smyslu řízení například ostatních rezortů, nebo spíše o jakési expertní poradenství například pro členy vlády?

Vzhledem k tomu, jak byla digitální agenda v minulosti roztříštěná, rozhodla vláda o vytvoření funkce koordinátora, který by toto odvětví sjednotil a působil jako moderátor mezi rezorty, hospodářskými a sociálními partnery a IT byznysem. Cílem bylo vytvořit místo, kam by se mohli partneři obracet se svými problémy, místo, které by fungovalo jako most mezi jednotlivými rezorty a nejen mezi nimi, ale také mezi veřejnou a soukromou sférou, pokud jde o oblast digitální ekonomiky.

Navíc bavíme-li se o hlavní náplni koordinátora, kterou je, jak již z názvu vyplývá, koordinace digitálních aktivit veřejné a soukromé sféry, Úřad vlády jakožto zastřešující a nadrezortní instituce je k tomuto ideálním místem.

Vedle moderace a slaďování postojů je mým úkolem rovněž propagace a komunikování digitální agendy veřejnosti. To bylo zatím bohužel podceňované.

Jedním ze zásadních problémů českého e-governmentu je rezortní roztříštěnost. Je v tomto směru funkce digitálního koordinátora cestou nápravy? Případně bude následována nějakými dalšími systémovými kroky?

E-government patří mezi jednu z mých priorit, a to právě i z důvodu jeho dosavadní roztříštěnosti. Ustavení koordinátora není nápravou v pravém slova smyslu, ale má zjednodušit a zrychlit dnes mnohdy složitou diskusi mezi rezorty. Digitalizace státní správy je dnes samozřejmostí v řadě evropských zemí, není důvod, aby Česká republika byla výjimkou.

Jedna z Vašich priorit je e-government, a to ve smyslu zlepšení přístupu občanů ke službám státní správy. Jaký je tedy v současné době stav z pohledu uživatelského? Co je možné a vhodné v nejbližší době vylepšit? Jaký je cíl a je nějaký „jízdní řád" s jasným cílovým stavem?

V mezinárodních srovnáváních na tom bohužel nejsme dobře. V rámci hodnocení Evropské unie se nyní ČR ocitá na posledních místech (25. místo za rok 2015) a v rámci hodnocení OSN až na 53. místě. Úroveň e-governmentu v ČR je ale někdy zbytečně podceňovaná. Naše špatná umístění v žebříčcích není způsobeno tím, že bychom služby e-governmentu neměli vůbec. Problémem je, že tyto služby málo propagujeme a občané nevědí, že vůbec existují, případně, jak je využít.

Jednou z prvních věcí, na které teď v e-governmentu pracujeme, je mapování již fungujících služeb napříč republikou. Následovat bude ověření funkčnosti a toho, jak jsou „user -friendly", tedy jak intuitivní jsou pro občany, kteří je budou využívat. Mapování probíhá také u dalších služeb, u kterých se plánuje spuštění v tomto a příštím roce, jako je například nahlížení do zdravotní dokumentace.

Jízdním řádem nejen pro e-government je pro nás Akční plán pro rozvoj digitálního trhu. S mým týmem jsme tento Akční plán aktualizovali a po diskuzi s hospodářskými a sociálními partnery by jej měla na podzim schválit vláda.

Právě v oblasti digitální agendy veřejných služeb spadáme do skupiny zaostávajících států. Máme tedy už jasnou strategii nápravy, nebo se k ní teprve dostáváme?

Před pár dny jsme spustili Iniciativu 202020, která si klade za cíl podpořit a urychlit vývoj ČR v oblasti e-governmentu. Název Iniciativy je odvozen od ambice, aby se ČR do roku 2020 posunula ve světových žebříčcích hodnotících úroveň a využívání služeb e-governmentu dopředu a ocitla se tak mezi prvními dvaceti hodnocenými zeměmi.

Jedním z hlavních poslání této aktivity je posílit propagaci digitálních služeb a veřejné správy, a zvýšit tak povědomí veřejnosti o již funkčních elektronických službách, ať už se jedná o aktualizace adresy Vašeho trvalého pobytu mezi všemi úřady či potvrzení o bezdlužnosti. Dalším cílem Iniciativy je také podpora rozvoje nových služeb poskytovaných elektronickou cestou.

Vašich pět prioritních oblastí je uváděno v pořadí e-skills, e-commerce, e-government, e-bezpečnost a e-výzvy. Proč právě v tomto pořadí? Za vhodnější bych považoval například e-bezpečnost, e-skills a e-government...

Z mého pohledu není rozhodující, jak jsou priority řazeny na papíře, důležité přece je jejich samotný význam v rozvoji české digitální ekonomiky. Digitální svět je natolik dynamický, že pořadí priorit bychom museli měnit každým dnem. Bez digitálních dovedností e-skills se dnes neobejdete v práci ani soukromém životě, díky fungujícímu e-governmentu můžeme občanům ušetřit čas, který by strávili ve frontě, zatímco by si z pohodlí domova mohli objednat nákup. Samozřejmě, že e-bezpečnost je základem veškerého našeho digitálního počínání. Nicméně o bezpečnosti na internetu bychom se dnes nebavili bez předchozích priorit, které jsem tu zmínil. Mé priority jsou provázané a důležité pro mě je, aby se v těchto pěti oblastech mohli občané pohybovat pohodlně, rychle a digitálně.

Jaké nejbližší efekty spojené se vznikem Vaší funkce budeme jako občané a klienti e-governmentu moci registrovat?

Mou osobní ambicí je dostat výhody digitálního světa tam, kde dnes chybí a kde se o nich neví. Chci, aby si patnáctiletý kluk z malého města mohl zařídit občanský průkaz, aniž by musel vynechat fotbalový trénink kvůli cestě do krajského města. Chci, aby babičce z odřízнuté vesnice mohl její doktor poslat recept online. Měli bychom lidi naučit používat služby, které jim usnadní život a ušetří čas.

202020

Projekt Iniciativa 202020 chce:

- aktivně přispívat k nalezení shody v rámci celé politické reprezentace a celé veřejné správy na odstranění legislativních, organizačních, popř. dalších bariér bránících většímu rozšíření on-line služeb veřejné správy, které mohou usnadnit život a podnikání v České republice.
- aktivně zapojovat do propagace aktivit a zvyšování povědomí veřejnosti o funkčních digitálních službách státu, jejich nabídce a využitelnosti pro život a podnikání.
- usilovat o maximální možnou míru synergie s komerčním sektorem (banky, pojišťovny, e-shopy, apod.) v nabídce a ve způsobu poskytování on-line služeb a dalšího rozvoje e-governmentu.
- vytvářet podmínky pro zapojení škol a vědeckých pracovišť do rozvoje on-line služeb a služeb e-governmentu tak, aby se především v mladé generaci vzbudil větší zájem o fungování státu a poskytování jeho služeb.
- vytvořit podmínky pro zapojení vývojářů mobilních aplikací, kteří jsou úspěšní ve vývoji komerčních aplikací, aby rozšířili svůj potenciál i do oblasti veřejné správy.
- rozšířit sdílení „Best Practices" (nejlepší praxe) s lídry v poskytování on-line služeb v Evropě i ve světě.

Zprovozňování on-line služeb

On-line služba veřejné správy umožňuje občanovi nebo firmě vyřídit si svou životní situaci přes internet bez fyzické návštěvy úřadu (princip Digital by Default) a zároveň po něm nevyžaduje informace a dokumenty, kterými již úřad (veřejná správa) disponuje (princip Only Once).

Plnohodnotná on-line služba využívá:

- základní registry pro sdílení dat veřejné správy;
- prostředky k ověření elektronické identity občana nebo firmy;
- další existující prvky infrastruktury e-governmentu (EGonServiceBus, komunikační infrastruktura VS, centrální místo služeb, ...).

Prostředky k ověření elektronické identity

V současnosti se připravuje legislativní úprava, která umožní:

- vedle eOP využití dalších důvěryhodných prostředků k ověření elektronické identity – např. datové schránky, internetové bankovnictví, mojeID, mobilní ID (vytvoření Národní federace identit podle vzoru Estonska);
- stanovit podmínky pro využití prostředků elektronické identity při jednotlivých právních úkonech a stanovení právních účinků jednání učiněného on-line s využitím těchto prostředků;
- ponechat rozhodnutí o využití konkrétních prostředků k ověření elektronické identity na správci příslušné agendy (on-line služby).

ict unie

NAKIT

Národní agentura pro komunikační a informační technologie a její role v eGov

NAŠE POSLÁNÍ:

- Výrazně přispět ke kvalitativnímu a kvantitativnímu posunu elektronizace veřejné správy a poskytovaných služeb
- Provoz infrastruktury a postupný přechod k poskytování služeb (ministerstvu vnitra a celé veřejné správě) s garancí plnění dohodnutých SLA parametrů a požadavků na bezpečnost, na otevřeném a sdíleném principu
- Být bezpečným, spolehlivým a důvěryhodným partnerem pro realizaci a následný provoz telekomunikačních a IT projektů v oblastech eGovernmentu a národní a kybernetické bezpečností formou přímých dodávek či formou sdílených služeb
- Spolupráce se Státní pokladnou Centrem sdílených služeb, s. p.

JAKÉ PROJEKTY REALIZUJEME:

- **ITS NGN** (integrovaná telekomunikační síť resortu MV a složek IZS)
- **CMS 2.0** (centrální místo služeb veřejné správy)
- **NIS** (zvýšení úrovně operačního řízení, sjednocení platformy informací OS IZS)
- **KSP** (jednotná úroveň IS, modernizace technologií operačního řízení IZS)
- **DCeGov** (centrální, provozní a bezpečnostní dohledové centrum MV)
- **MORIS** (modulární registr pro informační systémy) a další

JAKÉ PROJEKTY PROVOZUJEME:

- **Komunikační technologie pro MV** (PEGAS, ITS NGN)
- **CMS 2.0** (centrální místo služeb veřejné správy)
- **EKIS** (nástroj MV při výkonu funkce správce rozpočtových pravidel a účetnictví)
- **ISoSS** (informační systém o státní službě) a další

Národní agentura pro komunikační a informační technologie, s. p. vznikla dne 21. ledna 2016 a 1. července 2016 se sloučila s bývalým Odštěpným závodem ICT služby České pošty s. p. V současné době má na 400 zaměstnanců.

A: Kodaňská 1441/46, 101 00 Praha 10 - Vršovice **M:** +420 234 066 500 **E:** info@nakit.cz **W:** www.nakit.cz

Premiér Sobotka představil projekt Iniciativa 202020 s cílem rozvoje e-Governmentu

Předseda vlády Bohuslav Sobotka představil ve čtvrtek 15. září 2016 projekt Iniciativa 202020. Ten má za cíl do konce roku 2020 posunout Českou republiku v rozvoji e-Governmentu v Evropě mezi prvních 20 států. Představení Iniciativy se zúčastnil také ministr vnitra Milan Chovanec, koordinátor digitální agendy ČR Tomáš Prouza a zakladatelé Iniciativy 202020 hejtman Kraje Vysočina Jiří Běhounek a prezident ICT Unie Zdeněk Zajíček.

„Rozvoj e-Governmentu, tedy elektronizace státní správy je prioritou vlády. Jsem rád, že v této oblasti dochází ke shodě jak na půdě parlamentu, tak i mezi odbornou veřejností. V elektronizaci státní správy jsme už udělali řadu důležitých kroků. Nyní musíme tyto projekty intenzivněji a srozumitelněji představovat občanům a firmám. Jsem velmi rád, že díky Iniciativě 202020 jsme našli společnou vůli připravit potřebné novely zákonů, které rozšíří nabídku elektronických služeb státu. Důležité je soustředit se také na oblasti, které jsou s digitalizací úzce spojeny. Především je to průmysl, vzdělávání, rekvalifikace pro získání digitálních dovedností na pracovním trhu, či investice do výzkumu a vývoje nových technologií," uvedl předseda vlády Bohuslav Sobotka.

Cílem projektu Iniciativa 202020 je k tématu elektronizace veřejné správy přivést nejen politiky a úředníky z centrální úrovně, ale také politickou a úřednickou reprezentaci krajů a obcí, zástupce českého průmyslu, podnikatelů, vysokých a středních škol, občanských sdružení a dalších profesních organizací. Iniciativa 202020 je zahrnuta do aktualizace Akčního plánu rozvoje digitálního trhu.

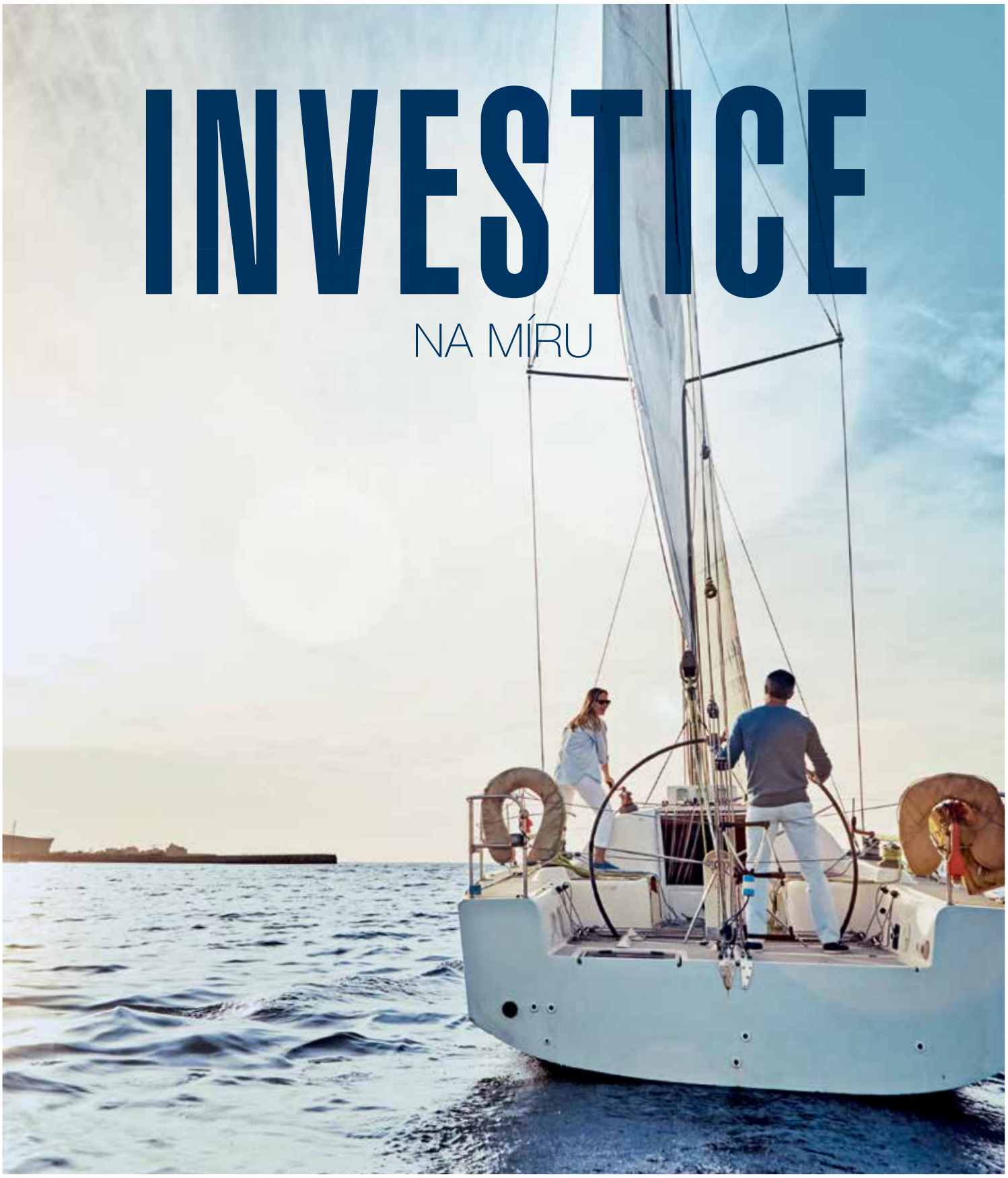
„Jsem přesvědčen, že tato Iniciativa přichází právě včas, protože i na úrovni EU se oblast rozvoje digitálních služeb státu dostává mezi klíčové priority pro rozvoj naší, ale i evropské konkurenceschopnosti. Nemůžeme si dovolit zůstat pozadu, a proto přes mnohé již zrealizované projekty musíme dát našemu snažení novou energii. Cítím se součástí Iniciativy 202020 a budu jí ze své funkce maximálně podporovat," uvedl Tomáš Prouza.

Česká republika se aktuálně pohybuje na 50. místě celosvětového žebříčku e-Government Development Index. Příčinou je zejména nedostatečná propagace služeb e-Governmentu, které Česká republika již poskytuje. Zároveň česká státní správa stále nenabízí dostatek online služeb, prostřednictvím kterých by bylo možné s úřady komunikovat výhradně přes internet bez nutnosti osobní návštěvy úřadů.

„Poté, kdy se v posledních deseti letech investovalo do velkých infrastrukturních projektů, které nejsou na první pohled vidět, je potřeba občanům a firmám konečně zprovoznit pestrou nabídku služeb, které budou stejně využívané a užitečné, jako je dnes nakupování přes internet nebo internetové bankovnictví," řekl Zdeněk Zajíček, prezident ICT Unie, která je jedním ze zakládajících členů Iniciativy.

O Iniciativě 202020 naleznete podrobnější informaci na nově spuštěných webových stránkách www.202020.cz nebo na facebookovém profilu Iniciativy 202020.cz.

202020



ČSOB Premium

Investice

Rozšíříme vaše investiční možnosti,
aby vaše peníze dále rostly a vy jste
mohli nerušeně dělat to, co vás právě baví.

ČSOB je generálním partnerem Golfu Hostivař.

800 370 370 | www.csobpremium.cz

VIZE 2020

OTO bude modernizován

Letos mě v Mikulově zaujalo hned několik věcí. Byly to informace o dalších plánech rozvoje českého e-Governmentu, věci kolem eIDAS, zákona o službách vytvářejících důvěru, zpráva o připravenosti nových kompozitních služeb a v neposlední řadě iniciativa 202020. Protože na dopady některých prezentovaných novinek si ještě chvíli počkáme, zaměřím se na ty, které mají účinek téměř okamžitý.

202020

Vezmu to od iniciativy. Svět nás řadí v e-Governmentu někam dozadu, přitom zde máme skvěle fungující elektronické služby. Dokonce masivně využívané občany této země – statistiky nelžou. Nejde pouze o okrajové využití e-služeb, jako je tomu v mnoha jiných zemích, ale o rutinní používání při řešení životních situací. Potíž je v tom, že se nedovedeme pochlubit.

Uvedu příklad ze života. Byl jsem na svatbě, kde nevěsta je jednatelkou společnosti. V sobotu se vdala a v úterý zjistila, že v obchodním rejstříku je už uvedena pod novým příjmením. Patří k Y generaci, která je zvyklá pracovat s novými technologiemi, ale tohle opravdu nečekala. Bez toho, aby sama musela o něco žádat, se o změnu příjmení v obchodním rejstříku „postaral" český e-Government. Stačilo, že se podepsala na konci obřadu do matričního archu, samozřejmě včetně ženicha, svědků a oddávajícího. Matrikářka poté nové skutečnosti (změna příjmení) zapsala prostřednictvím matričního formuláře v CzechPOINT@office do Informačního systému evidence obyvatel (ISEO). Odtud se nová informace dostala do Registru obyvatel. K tomu došlo automaticky při pravidelném updatu dat mezi ISEO a ROB. Z ROBu si změnu příjmení stáhl obchodní rejstřík a u příslušné společnosti aktualizoval příjmení jednatelky.

Ano, tohle funguje! Občan nemusí nikam chodit, informaci o změně stavu poskytl pouze jednou, ostatní ISVS a AIS tuto informaci získali ze základních registrů. Jenom je třeba se tím trochu „pochlubit", resp. umět dobře propagovat vlastní dobře fungující služby. Tohle nám opravdu chybí.

Kompozitní služby a fotografie

Patrně nejvíc mě ale zaujala zpráva o dokončení nových kompozitních služeb Správou základních registrů, zejména služba vydávající fotografie. Mimochodem služba, na kterou netrpělivě čeká Ministerstvo zahraničních věcí. To je totiž odpovědné za agendu cestovních dokladů, jejíž nedílnou součástí je ověření totožnosti osoby při ztrátě cestovních dokladů na zastupitelských úřadech České republiky. Služba ověřování totožnosti osoby byla dlouhou dobu zajišťována s využitím listinných formulářů, faxů a práce úředníků v České republice („analogově"). Jak jistě víte, od února 2014 byla tato agenda elektronizována a je součástí široké nabídky agend a funkcionalit v prostředí CzechPOINT@office. Pracovník zastupitelského úřadu má po přihlášení se do aplikace k dispozici elektronický formulář, do kterého zapisuje data ověřované osoby. Na pozadí tohoto formuláře dochází ke ztotožnění ověřované osoby vůči registru obyvatel. Prostě nádherná ukázka využití sdílených služeb eGovernmentu.

Podle statistik uveřejněných na webu Czech POINT, tuto službu využívá v cizině měsíčně zhruba 180 nešťastníků bez dokladů. V letošním červenci jich bylo dokonce více než 350. To není rozhodně málo...

Dá se tato služba ještě nějak vylepšit? Rozhodně ano! Právě kompozitní služba výdeje fotografií posune agendu ověřování totožnosti osoby ještě na vyšší úroveň spolehlivosti. Pracovník zastupitelského úřadu bude mít k dispozici kromě dat, sdělených nešťastným cestovatelem, ještě další kontrolní mechanismus – fotografii daného občana. A to vše v on-line režimu, tedy v průběhu ověřování totožnosti občana.

Kromě faktu, že agenda bude využívat další ze sdílených služeb e-Gov, je zde ještě jeden mimořádně důležitý aspekt – bezpečnostní. V minulosti při „analogovém" ověřování totožnosti osoby docházelo k pokusům různých kriminálních živlů, získat touto cestou cestovní doklad občana ČR. Elektronizace prostřednictvím agendy na CzechPOINT@office s využitím dat z registru obyvatel tyto pokusy určitě znesnadnila. Takže využití služby výdeje fotografií bude mít rozhodně velmi důležitý bezpečnostní dopad.

A která z hodnocených zemí se může pochlubit takovou agendou v rámci svého e-Governmentu? Agendou dostupnou občanům prakticky po celém světě? Jsme zase u té propagace...

Autentizační služby eGov

Mezi novinkami mě pak zaujalo právní ukotvení JIP/KAAS pro orgány veřejné moci (OVM). Tedy Jednotného identitního prostoru Czech POINT a jeho rozhraní Katalogu autentizačních a autorizačních služeb. K dnešnímu dni i bez tohoto právního ukotvení používá autentizační a autorizační služby pro přístup ke svým AIS několik desítek úřadů. Dokonce i Registr smluv využívá JIP/KAAS pro správu rolí přístupu. Potřeboval k tomu právní ukotvení? Jak je vidět, nepotřeboval. Každopádně právní ukotvení přináší OVM jistotu na legislativním základě, že se službami JIP/KAAS může počítat při návrhu svých nových IT systémů. Může počítat s praxí vyzkoušenou sdílenou službou eGovernmentu.

JIP/KAAS si již našel cestu ke svým „zákazníkům". Tak proč je opomíjena další sdílená služba e-Gov, tzv. Autentizační služba ISDS? Stejně jak JIP/KAAS umožňuje autentizaci uživatelů z řad zaměstnanců OVM a jimi zřízených organizací, nabízí ISDS službu autentizace pomocí přístupových údajů k datové schránce i pro další uživatele – občany, podnikající fyzické osoby nebo právnické osoby. Výhodu této služby zatím využila ČSSZ na svém ePortálu. Proč například tuto nabídku nevyužila taková VZP při nasazení elektronické komunikace prostřednictvím Moje VZP?

Ing. Martin Řehořek

- vystudoval FSI ČVUT a postgraduální studium v oboru aplikace mikropočítačů v průmyslu
- ve společnosti pracuje od roku 2007; v roce 2009 byl jmenován na pozici výkonného ředitele Novell Professional Services (později NEWPS.CZ)
- jednatelem společnosti NEWPS.CZ s.r.o. se stal v dubnu 2015
- je odpovědný za řízení společnosti, obchodní aktivity společnosti, rozvoj prodeje produktů a služeb

Ta má sloužit nejenom občanům, ale také právnickým osobám. Pokud chci tuto komunikaci používat, musím se registrovat, neboli vytvořit si u VZP nový uživatelský účet. Proč bych to dělal? Vždyť na VZP je z pohledu zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů nahlíženo jako na orgán veřejné moci. VZP je oprávněna autentizační službu ISDS využívat. Proč mi teda nenabídla možnost přihlášení se k Moje VZP prostřednictvím mým přihlašovacích údajů z ISDS?

Podobných příkladů, kde by si občan nemusel pokaždé vytvářet další uživatelský účet, je více. Jistě se s tím setkáváte taky. Co brání využití autentizační služby ISDS v širším měřítku? Legislativně nic. Procesně taky nic. Takže, proč se do toho nepustit a usnadnit občanovi prahnoucímu po elektronické komunikace trochu život?

Myslím, že s posunutím České republiky v hodnocení e-Governmentu se dá skutečně něco udělat. A nemusí to být ani složité, ani nákladné.

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

NEWPS.CZ

VIZE 2020

Pohled společnosti Cisco na transformaci vládních IT

Na základě naléhavé potřeby snížit provozní náklady a zvýšit efektivitu veřejného sektoru zahajují vlády po celém světě iniciativy napříč mnoha funkcemi s cílem přehodnotit způsob poskytování veřejných služeb jak směrem k občanům, tak mezi jednotlivými ministerstvy. Snaží se pozitivně využít sílu inovací a nových obchodních paradigmat (IT jako služba), jež formují stávající podobu oblasti technologií. Zejména zkoumají nejlepší model pro zprovoznění vládního cloudu a příležitosti k restrukturalizaci, které přinášejí moderní modely sdílených IT služeb.

Transformace vlády prostřednictvím IT

Výdaje na IT tvoří průměrně 3 % vládních rozpočtů. To je značná částka, ale pouze marginální: skutečná příležitost spočívá mimo oblast snižování nákladů na IT – jde o využití IT ke zvyšování provozní efektivity a kvality služeb. Lze dosáhnout značných úspor v provozním rozpočtu vlády a současně poskytovat skutečnou a trvalou hodnotu občanům, podnikům i subjektům veřejného sektoru.

K výhodám patří:

- možnost poskytovat inovativní služby občanům;
- posílení pravomocí zaměstnanců prostřednictvím samoobslužných portálů;
- zvýšení spolehlivosti a zabezpečení aplikací;
- zlepšení přehledu a kontroly pro vyšší vedoucí pracovníky;
- zavedení inteligentnějšího řízení, správy rizik a dodržování předpisů.

Spojení sil pro vytvoření nové koncepce hodnoty

Vládní úřady a ministerstva v České republice přistupovaly v minulosti k nákupu, údržbě a řízení IT nekonzistentně. Jinými slovy, nakupují nezávisle služby od celé řady poskytovatelů IT a přicházejí tak o možnost využívat úspor z rozsahu.

I kdyby několik úřadů najalo jako poskytovatele služeb stejnou třetí stranu, každý musí navázat vztah a uzavřít smlouvu samostatně. Strategie nákupu a úrovně služeb jsou přizpůsobeny individuálním potřebám každé organizace, což dále zvyšuje celkové náklady pro veřejný sektor.

V posledním desetiletí si tyto organizace uvědomily, že spojením sil by získaly obrovské příležitosti. To vedlo ke zkoumání nových modelů vzájemné spolupráce při zajišťování, nákupu a poskytování IT.

Neexistuje žádná jediná správná cesta ani řešení, které by se hodilo pro všechny. Různé země zavádějí různé modely řízení na základě místních historických a kulturních podmínek a situace v oblasti stávajících IT systémů. Cíl je ovšem

TYPICKÝMI PŘEKÁŽKAMI ÚSPĚCHU JSOU:

- nedostatky v komunikaci mezi organizací sdílených IT služeb a jednotlivými vládními úřady a ministerstvy;
- nedostatek osob, které by prosazovaly změny nutné k implementaci nové vize;
- vertikálně orientovaný přístup k nákupu služeb a vybavení soustředěný na produkty, které je nutno integrovat, ale nikoli na služby a úrovně služeb (SLA);
- neschopnost změnit staré IT postupy prostřednictvím nových dovedností a inovací;
- nedostatek kultury orientované na zákazníka;
- potíže při konsolidaci IT, od Service Desk po datové centrum;
- nedostatečná kontrola a přehled o IT procesech a službách v reálném čase;
- nejistota ohledně předpisů v oblasti dat – umístění/suverenita dat a zabezpečení informací;
- šíření dat a aplikací na nekonzistentních platformách.
- Spoléhání se na manuální, časově náročné IT
- Rozpočtové modely, které již nejsou vhodné pro služby na bázi cloudu

vždy stejný: odstranit organizační překážky a promyslet, jak mohou IT poskytovat hmatatelnou hodnotu.

Pět modelů řízení

Přístup sdílených IT služeb nabízí vládě skutečnou příležitost k transformaci.

Prvním krokem je možnost výběru a kombinace aspektů z různých modelů k vytvoření vhodného řešení. Používá se pět běžných modelů a každý z nich má jiné silné a slabé stránky.

1. Interní sdílené služby

Tento model je prvním krokem ke cloudu. Jeden interní poskytovatel dodává IT služby několika úřadům nebo ministerstvům.

Silné stránky: Poskytuje uživatelům rychlou, pohotovou IT podporu, uklidňující fyzickou blízkost a přístup k týmu Help Desku.

Slabé stránky: Toto řešení lze jen obtížně škálovat a neposkytuje výrazné nové finanční úspory ani neposouvá organizaci vpřed na cestě k dosažení skutečné výhody v podobě IT jako služby.

2. Centralizovaný nákup

V tomto modelu je za strategii nákupu zodpovědný centrální úřad, který nakupuje pro všechna ostatní ministerstva. Dojde k nastolení důvěry a klientské úřady si uvědomí, že nemá smysl, aby individuálně udržovaly složité mechanismy řízení, když jsou rozdíly mezi úrovněmi služeb minimální.

Silné stránky: Zaměření na snižování nákladů prostřednictvím úspor z rozsahu a racionalizace IT; díky centralizovanému nákupu se uplatňuje standardní přístup k architektuře.

Slabé stránky: Nezaměřuje se na zvyšování produktivity uživatelů a nese s sebou riziko fragmentovaného, špatně integrovaného přístupu bez širší vize IT pro významné nové trendy, jako je BYOD.

3. Vládní poskytovatel služeb

Tento model vyčleňuje IT oddělení velkého ministerstva jako samostatnou, neziskovou organizaci. Je 100% vlastněna státem, funguje a vstupuje do konkurence jako komerční organizace, ale dodržuje pravidla pro zadávání veřejných zakázek.

Silné stránky: Plně se věnuje uspokojování potřeb vlády. Rozhoduje, co řešit interně, co outsourcovat a komu.

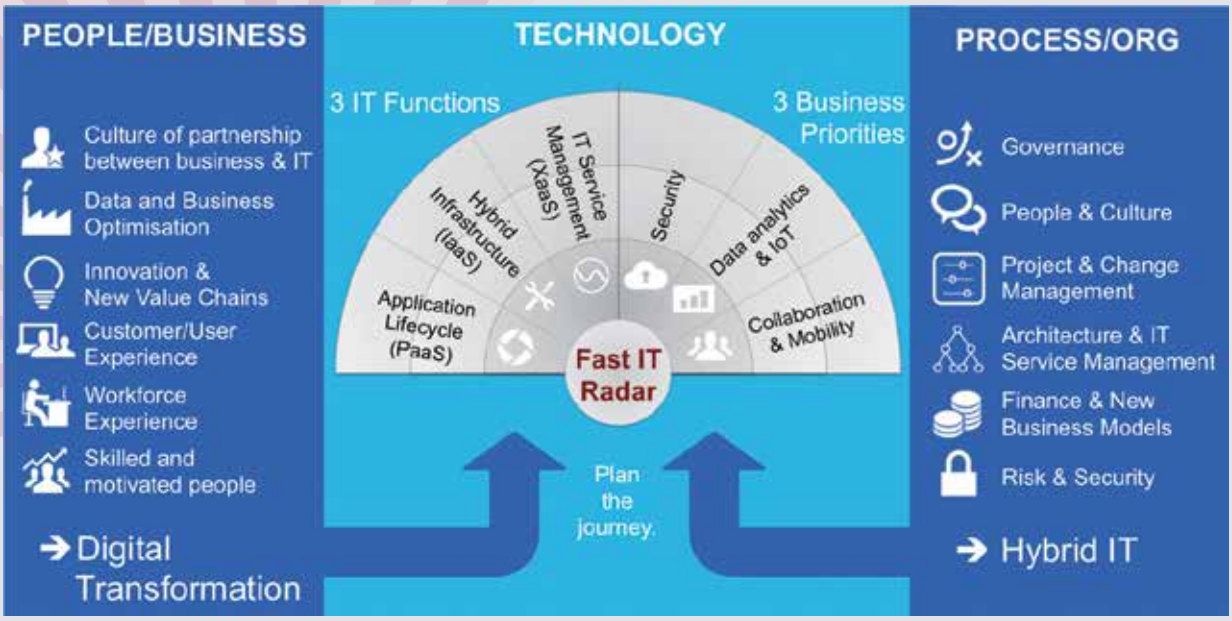
Slabé stránky: Vyžaduje poměrně velké počáteční investice.

4. Spravované služby / PPP

Tento model je založen na těsném partnerství mezi veřejným a soukromým sektorem.

Silné stránky: Bohaté zkušenosti třetích stran, značné úspory z rozsahu a neustálé inovace.

Slabé stránky: Vyžaduje čas k vybudování vzájemně prospěšného vztahu na bázi důvěry.



5. Otevřený trh

Tento model využívá „cloudový obchod" na bázi katalogu, ke kterému mohou uživatelé volně přistupovat a nakupovat IT služby na požádání.

Silné stránky: Pružná koncepce, která industrializuje přístup, staví uživatele do středu dění a nabízí nižší počáteční náklady. Rovněž přináší úspory nákladů z průběžného placení.

Slabé stránky: I tento model nákupu může být fragmentovaný, kdy uživatelé nakoupí BYOD na jednom místě, VPN jinde a systémy pro spolupráci ještě jinde.

Podpora transformace vládních IT

Většina metodik transformace IT bohužel není schopna přistupovat ke všem proměnlivým faktorům komplexním způsobem, takže je pro českou vládu obtížné učinit informované rozhodnutí, které by bylo zaměřeno na budoucnost a podpořilo digitální transformaci vlády v nadcházejícím desetiletí.

Aby bylo možno realizovat odpovídající kombinaci výše popsaných 5 modelů, je nezbytně nutné, aby česká vláda vytvořila přístup, který bude zahrnovat 3 pilíře transformace IT: technologie A ZÁROVEŇ lidé A ZÁROVEŇ procesy.

1. **Lidé/podnikání.** Identifikovat a zdokumentovat nejdůležitější prvky v organizaci, které posouvají podnikání vpřed a umožňují lidem podávat nejlepší výkony. Odpovědět na otázky: Co ve skutečnosti znamená „digitální transformace v ČR" a jak by ji vládní IT měly podporovat? Jaké jsou klíčové prvky, které posouvají podnikání vpřed a umožňují lidem podávat nejlepší výkony, a to jak v současnosti, tak v budoucnu?
2. **Procesy/organizace.** Zhodnotit, jak jsou (nebo by měly být) IT strukturovány, a definovat, jak se měří (nebo by se měl měřit) úspěch. To zahrnuje diskuzi o tom, co by se mělo dělat interně a co by se mělo outsourcovat. Navrhnout konkrétní řešení pro maximalizaci hodnoty IT pro podnikání, včetně řady kroků, které jsou potřeba k zajištění akceschopnosti, pružnosti, bezpečnosti a nákladové efektivity IT.
3. **Technologie.** Vytvořit individuálně přizpůsobený „radar Fast IT", který poskytne plán postupu pro 3 klíčové funkce IT (aplikace, infrastruktura, služby) a 3 klíčové podnikové priority (zabezpečení, data/IoT, mobilní spolupráce).

Jakákoli metodika, která komplexně neřeší tyto 3 pilíře společně, by nutně musela selhat a její závěry by byly částečné nebo ještě hůř, nesprávné.

Patrick Bikar,
Governmet Digital Transformation,
Practice Lead, Cisco EMEAR

Chcete-li získat více informací o řešeních společnosti Cisco pro digitální transformaci vlády, navštivte prosím stránky: **www.cisco.com/go/government** nebo se obraťte na **fast-it@cisco.com**.

press release

ATOS na konferenci e-government v Mikulově

Mikulov, 6. - 7. září 2016 – ATOS, největší evropská IT firma prezentovala na konferenci e-government v Mikulově svůj pohled na stav kybernetické bezpečnosti ve státní správě. Během dvou dnů zde bylo možné diskutovat s představiteli státní správy na téma elektronizace a kybernetická bezpečnost bezpečnost v prostředí veřejné správy.

ATOS prezentoval aktuální téma "Kybernetická bezpečnost ve státní správě" pohledem systémového integrátora. Vyzdvihl aktuální problémy jako nedostatečný počet odborníků na problematiku detekce a analýzu incident a kapacity veřejných organizací pokrýt neustále narůstající hrozby. Byl představen koncept ATOS SOC (Security Operations Center) center, která pomáhají incidenty řešit jak zákazníkům v komerční, tak veřejné sféře. Zástupce ATOSu p. Tomáš Hlavsa, pozval zástupce veřejné správy na referenční návštěvu globální SOC centra v polské Bydgoszczi, kde ATOS svým stávajícím I budoucím zákazníkům představuje své schopnosti a kapacity na poli boje s kybernetickými hrozbami.

About Atos

Atos SE (Societas Europaea) je lídrem v digitálních službách, který dosáhl za rok 2015 ročního výnosu ve výši 12 miliard EUR a který zaměstnává 100 tisíc pracovníků v 72 zemích.
Akvizicí společnosti Siemens IT Solutions and Services v říjnu 2010 začal Atos působit v České republice pod jménem Atos IT Solutions and Services, s.r.o. Atos v České republice dosáhl v roce 2015 čistého obratu firmy 39 697,- tis. EUR a zaměstnává 300 zaměstnanců v Praze, Brně, Ostravě a Vysokém Mýtě
Atos přináší poradenství a systémovou integraci, řízené služby a outsourcing business procesů, cloudové operace, Big Data a řešení pro kybernetickou bezpečnost, stejně tak jako i transakční služby prostřednictvím společnosti Worldline, evropského lídra v oblasti platebních a transakčních služeb.
Díky vysoké technologické odbornosti a znalostem průmyslových odvětví společnost Atos pracuje s klienty z různých obchodních sektorů jako jsou: finanční služby, zdravotnictví, výrobní průmysl, média, telekomunikace, energetika, veřejný sektor, doprava, obrana a retailové podniky.
Atos se zaměřuje na technologie, které přinášejí pokrok a pomáhají organizacím vytvářet firmu budoucnosti.
Společnost Atos je celosvětovým technologickým partnerem Olympijských a Paralympijských her a je kotovaná na pařížské burze NYSE Euronext Paris. Společnost Atos působí pod značkami Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify a Worldline.

Pro více informací: www.cz.atos.net
Kontakt:
Tomáš Hlavsa, Tel.: + 420 604 290 196, Email: tomas.hlavsa@atos.net

eIDAS včera, dnes a zítra

Poradce náměstka ministra vnitra pro ICT Ing. Robert Piffl zahájil své vystoupení tvrzením, že opakování je matka moudrosti, a proto připomenul, že již od roku 2014 existuje Nařízení Evropského parlamentu a Rady EU č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále jen Nařízení EU).

Podstatné je, že toto nařízení je od 1. 7. 2016 účinné a platné v oblasti služeb vytvářejících důvěru, a jak Robert Piffl upozornil, existuje k němu 8 prováděcích aktů:

1. prováděcí rozhodnutí Komise (EU) 2015/296 ze dne 24. února 2015, kterým se stanoví procesní opatření pro spolupráci mezi členskými státy v oblasti elektronické identifikace podle čl. 12 odst. 7 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu;
2. prováděcí nařízení Komise (EU) 2015/806 ze dne 22. května 2015, kterým se stanoví specifikace týkající se podoby značky důvěry EU pro kvalifikované služby vytvářející důvěru;
3. prováděcí rozhodnutí Komise (EU) 2015/1506 ze dne 8. září 2015, kterým se stanoví specifikace pro formáty zaručených elektronických podpisů a zaručených pečetí uznávaných subjekty veřejného sektoru podle čl. 27 odst. 5 a čl. 37 odst. 5 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu;
4. prováděcí rozhodnutí Komise (EU) 2015/1505 ze dne 8. září 2015, kterým se stanoví technické specifikace a formáty důvěryhodných seznamů podle čl. 22 odst. 5 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu;
5. prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu;
6. prováděcí nařízení Komise (EU) 2015/1501 ze dne 8. září 2015 o rámci interoperability podle čl. 12 odst. 8 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu;
7. prováděcí rozhodnutí Komise (EU) 2015/1984 ze dne 3. listopadu 2015, kterým se stanoví okolnosti, formáty a postupy pro oznamování podle čl. 9 odst. 5 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (oznámeno pod číslem C(2015) 7369);
8. prováděcí rozhodnutí Komise (EU) 2016/650 ze dne 25. dubna 2016, kterým se stanoví normy pro posuzování bezpečnosti kvalifikovaných prostředků pro vytváření elektronických podpisů a pečetí podle čl. 30 odst. 3 a čl. 39 odst. 2 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu.

Robert Piffl zopakoval, že uvedené nařízení vstoupilo v platnost 23. 7. 2014 a postupně vstupuje v účinnost (1. 7. 2016 vstoupila v účinnost ta část, která se týká služeb vytvářejících důvěru pro elektronické transakce) a zároveň s tím novým nařízením se cosi zrušilo nebo postupně ruší. Jedná se například o směrnici č. 93 z roku 1999 a všechny náležitosti a konstrukce postavené na této směrnici, které byly nahrazeny Nařízením EU.

NAŘÍZENÍ eIDAS A STAV V ČR

Podle Roberta je velice důležité si uvědomit, že se jedná se o **nařízení**, je tedy **přímo účinné**. Nařízení řeší jak problematiku **elektronické identifikace**, tak **služby vytvářející důvěru pro elektronické transakce**. Protože se jedná o nařízení, nikoli směrnici, není potřeba jeho implementace v českém právním řádu, přesto byly na MV ČR v této souvislosti připraveny dva zastřešující zákony. Jedná se o **zákon o službách vytvářejících důvěru pro elektronické transakce** (již podepsán prezidentem) a druhý zákon o elektronické identifikaci. Tento druhý zákon již existuje v paragrafovém znění, je dopracovávána RIA a je připraven pro připomínková řízení. Výsledný stav je tedy takový, že zde budeme mít nařízení, které je přímo účinné, a zároveň na území ČR budeme mít dva základní právní předpisy, které nesmí být s tímto nařízením v rozporu.

Protože Nařízení EU je opravdu přímo účinné a má přednost před národními legislativami, je nutno si uvědomit, že zde existuje řada právních předpisů, řada tzv. agendových zákonů, řada různých nařízení českých úřadů, které by mohly s tímto Nařízením kolidovat. Celá veřejná správa byla v roce 2014 vyzvána, aby porovnala své vyhlášky a nařízení ve vztahu s Nařízením eIDAS tak, aby zde nebyl rozpor. Podle Roberta Piffla je toto vyladění skutečně důležité, neboť pokud například Nařízení eIDAS říká, že kvalifikovaný elektronický podpis má stejný právní účinek jako vlastnoruční podpis na listině, tak to tak je. Znamená to, že žádný úředník nemůže tvrdit a požadovat opak.

Robert Piffl zdůraznil, že jako členský stát jsme s naší harmonizací celkem v pořádku. Podle jeho slov máme určité malé zpoždění, neboť bylo potřeba důsledně analyzovat všech 8 aktů, nicméně, jak bylo řečeno, zákon o službách vytvářejících důvěru je podepsán a vychází ve Sbírce zákonů. Zároveň s tímto návrhem zákona byl přijat návrh zákona, který mění řadu právních předpisů (návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce, zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a zákon č. 121/2000 Sb., o právu autorském, o právech o službách vytvářejících důvěru pro elektronické transakce souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů. Podstatné je, že tento zákon přináší dvouleté přechodné období, kdy na území ČR bude povýšen uznávaný podpis na úroveň kvalifikovaného podpisu, a zavádí možnost existence elektronické značky, která by, na základě zrušení zákona o elektronickém podpisu, měla být rovněž zrušena. V uvedeném zákoně je tedy obsaženo vše, co by mělo pomoci při výkonu působnosti OVM při přijímání dokumentů, jejich vystavování, podepisování, přidělování časových razítek atd.

ELEKTRONICKÁ IDENTIFIKACE

Druhou velice podstatnou částí Nařízení eIDAS je elektronická identifikace. Nejedná se o problematiku, která by byla vyloženě pod časovým tlakem, protože samo Nařízení eIDAS říká a upravuje pouze tzv. oznámené systémy elektronické identifikace, které se týkají přeshraničních transakcí. Nic jiného toto nařízení neupravuje. Říká tedy, jak si budou jednotlivé členské státy navzájem uznávat systémy elektronické identifikace pomocí mezinárodních uzlů, a pro tuto oblast je zde definováno paragrafové znění. Aby vše navazovalo, MV ČR připravilo zákon o elektronické identifikaci (zvládnuto za 45 dní). Nyní je dopracována RIA, důvodová zpráva a v nejbližších dnech by měl být návrh předložen do vnitřního a vnějšího připomínkového řízení (řízení jsou spojená, aby se splnil termín předložení do konce roku). Důležité je, že tento zákon zřizuje **národní bod pro identifikaci a autentizaci (NIA)** a doplňuje to, co ani nařízení eIDAS řešit nemůže – postavení iden-

titních systémů, identity providerů, server providerů a „pravidla hry" na území ČR. Je to tedy jakési zastřešení trojúhelníku: eIDAS – zákon o službách – zákon o elektronické identifikaci.

OBČANSKÉ PRŮKAZY

Pokud jde o prostředek pro elektronickou identifikaci, je podle Roberta Piffla podstatný návrh **novely zákona o občanských průkazech,** který:

- zavede jednotné občanské průkazy s čipem v průběhu roku 2018;
- na občanském průkazu s čipem bude identifikační certifikát občanského průkazu a kvalifikovaný podpis na kvalifikovaném certifikátu držitele občanského průkazu;
- občanský průkaz s čipem bude QSCD pro vytváření elektronických podpisů;
- občanský průkaz s čipem bude vydáván bezplatně;
- pro skupinu cca 30–35 tisíc vydaných OP s čipem před účinností novely zákona bude provedena bezplatná výměna za nový OP s čipem;
- v současné době je novela zákona projednávána v legislativních komisích vlády ČR.

Robert Piffl přítomné upozornil na skutečnost, že obecně je v ČR řada právních předpisů, které upravují klíčové oblasti působnosti. Mezi nejdůležitější patří **zákon o archivnictví a spisové službě** – všechny úřady by měly mít v pořádku systém spisové služby, včetně směrnic a všeho, co se týká oběhu a tvorby dokumentů, práce s elektronickými fakturami, předávání elektronických smluv atp., všechny úřady musí být schopny rozpoznat, zda se jedná o kvalifikovaný podpis, zda je z důvěryhodného seznamu atp. Protože těch povinností je skutečně mnoho, je podle Roberta Piffla velmi dobře, že se zavádějí až od roku 2018, aby bylo možné vše v klidu doladit. Upozornil proto především na paragrafy 5, 6, 7 zákona o službách vytvářejících důvěru, které upřesňují některé z uvedených povinností.
I proto vláda ve svém usnesení č. 265 z 30.3. 2016 uložila všem odpovědným orgánům, které provozují systémy veřejné správy, úkol, aby MV ČR do 30. 6. 2016 odevzdaly analýzy svých informačních systémů v návaznosti s Nařízením eIDAS v souvislosti s povinností od 28. 9. 2018 rozpoznávat identitní prostor oznámených systémů elektronické identifikace v rámci EU a zároveň, aby do 30. 9. předložily harmonogram úprav svých informačních systémů tak, aby umožnily úplné elektronické podání. To jsou kroky, které pokud budou řádně realizované, mohou v mezinárodním srovnání posunout ČR z 55. místa v rámci poskytování služeb e-governmentu, protože, jak zdůraznil Robert Piffl, zatímco backend (základní registry) máme velmi dobrý, stále nám chybí na front endu.

OČEKÁVANÝ HARMONOGRAM

V závěru vystoupení Robert Piffl prezentoval harmonogram nejbližších kroků v souvislosti s nařízením eIDAS:

- v letech 2016/2017 očekáváme přijetí novel právních předpisů a návrhů nových zákonů,
- které MV ČR připravilo a připravuje;
- v roce 2016 proběhne vyhodnocení analýz a harmonogramů dle usnesení vlády ČR, návrh dalších opatření počátkem roku 2017;
- v roce 2017 očekáváme zákon o elektronické identifikaci (od roku 2017 bude též možnost připojení „ve zkušebním provozu");
- v roce 2018 očekáváme zavedení jednotných eOP s čipem (identifikační a podpisový certifikát na eOP);
- v roce 2018 spuštění NIA, následně nahlášení jako identitní systém České republiky;
- od 28. 9. 2018 plná funkcionalita, následné budoucí připojení soukromoprávních subjektů.

Jak zdůraznil, i když se to nezdá, je harmonogram velice napnutý, aby se vše stihlo do uvedeného data. Protože nyní nastává možnost vyjadřovat se k návrhu zákona o elektronické identifikaci, upozornil, že je to v ČR poprvé, kdy by měla být zavedena fikce prokazování identity prostřednictvím systému elektronické identifikace, která bude mít stejný účinek, jako kdybych stál fyzicky na konkrétním úřadě. S ohledem na význam tohoto kroku apeloval Robert Piffl na přítomné, aby spíše než torpédování návrhu množstvím připomínek jej podpořili tak, aby se zmiňované principy podařilo protlačit a realizovat.

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 16 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

Vztah nařízení eIDAS k ochraně osobních údajů

aneb co bude znamenat nové nařízení GDPR pro elektronické transakce nejen ve veřejné správě

JUDr. Josef Donát, LL.M., partner advokátní kanceláře ROWAN LEGAL, zvolil tento název svého příspěvku na konferenci z toho důvodu, aby upozornil na to, že nové evropské nařízení o ochraně osobních údajů (General Data Protection Regulation, zkráceně GDPR), jehož účinnost je stanovena na jaro roku 2018, bude mít dopad také na oblast elektronických transakcí. Podle slov Josefa Donáta se v příštím roce stane z GDPR velmi aktuální téma a bude se řešit podobně, jako se dnes řeší nařízení eIDAS.

Význam ochrany osobních údajů v oblasti elektronických transakcí je patrný zejména z povinnosti uplatňovat nařízení eIDAS v souladu se zásadami ochrany osobních údajů, která vyjádřena již v preambuli eIDAS a dále se vyskytuje celkem v 12 článcích. Dle Josefa Donáta je důležité si uvědomit, že GDPR přináší řadu novinek a zcela zásadně mění mnohé doposud zaběhnuté postupy a procesy při zpracování osobních údajů. Pokud například dojde k narušení bezpečnosti na straně poskytovatele služeb vytvářejících důvěru, nastane pro poskytovatele zpravidla nejen povinnost informovat MV ČR, ale také Úřad pro ochranu osobních údajů a v některých případech dokonce i jednotlivé fyzické osoby.

NEDÁVNÝ VÝVOJ

Před tím, než se Josef Donát pustil do výkladu jednotlivých aspektů samotného GDPR, uvedl některé zásadní milníky v oblasti ochrany osobních údajů z nedávné historie. Doposud platilo, že co o nás internet jednou napsal, to v kyberprostoru zůstalo a bylo k dohledání. Nastaly ovšem určité změny.

- Poměrně nedávno se podařilo soudní cestou prosadit tzv. „právo být zapomenut“, tedy právo být za určitých okolností, a pokud pominou některé skutečnosti, odstraněn z výsledků vyhledávání webových vyhledávačů.
- Student práv z Vídně a aktivista v oblasti ochrany osobních údajů, Max Schrems, dosáhl průlomového rozhodnutí Evropského soudního dvora v oblasti předávání osobních údajů do USA. Schrems byl dlouhodobě znepokojen tím, že Facebook předává data různým službám a orgánům Spojených států a nedbá při tom ochrany osobních údajů, jakou by měl dodržovat podle evropských právních předpisů. Se svými výhradami uspěl, dosáhl zrušení dosavadního právního rámce Safe Harbour pro předávání, a rozpoutal tak diskuzi o přiměřenosti ochrany dat evropských občanů ve Spojených státech. Zrušení programu Safe Harbour v praxi velmi komplikovalo jakékoliv předávání osobních údajů do USA, a proto byla velice rychle zahájena konstruktivní vyjednávání mezi oběma stranami o vytvoření nového rámce pro předávání. Na základě této debaty byl vytvořen systém ochrany osobních údajů s názvem Privacy Shield. Tento právní rámec je založen na dohodě, na jejíž podobě a následné implementaci se podílela shodou okolností eurokomisařka Věra Jourová. Výsledný program oproti Safe Harbour zajišťuje mnohem vyšší ochranu osobních údajů v USA, a to tím, že pro předávání stanoví přísnější pravidla, omezuje přístup vládních orgánů k těmto osobním údajům a zakotvuje také paletu možností, které může evropský občan využít, pokud má pocit, že jeho osobní údaje jsou zpracovány v rozporu se stanovenými pravidly.
- Vedle těchto událostí probíhala, už od roku 2012, příprava nového Nařízení GDPR. Přesto, že se jedná o zásadní nařízení, existuje řada záležitostí, které musí, nebo mohou členské státy upravit národní úpravou. Zcela kompletní přehled práv a povinností, které nová úprava přináší, bude tedy znám až s přijetím této národní legislativy.

ZÁKLADNÍ POJMY

Samotný výklad o GDPR začal Josef Donát vysvětlením některých pojmů, které jsou novým nařízením upravovány či zaváděny.

Subjektem údajů je dle GDPR identifikovaná fyzická osoba nebo fyzická osoba, kterou lze přímo či nepřímo identifikovat prostředky, o nichž lze důvodně předpokládat, že je správce nebo jakákoli jiná fyzická nebo právnická osoba použijí pro identifikaci dané osoby, zejména s odkazem na identifikační číslo, lokalizační údaje, elektronický identifikátor nebo s odkazem na jeden či více zvláštních prvků její fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo sociální identity.

Osobními údaji jsou veškeré informace o subjektu údajů.

Zpracováním GDPR rozumí jakýkoliv úkon nebo soubor úkonů s osobními údaji, které jsou prováděny pomocí, či bez pomoci automatizovaných postupů, jako je shromažďování, zaznamenávání, uspořádávání, strukturování, uchovávání, přizpůsobování nebo pozměňování osobních údajů, ale také jejich vyhledávání, konzultace, použití, sdělení prostřednictvím přenosu, šíření nebo jakékoli jiné zpřístupnění, srovnání či kombinování, jakož i blokování, výmaz nebo likvidace.

Správce je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, který sám, nebo společně s jinými určuje účel, podmínky a prostředky zpracování osobních údajů; jsou-li účel, podmínky a prostředky zpracování určeny právem Unie či členského státu, je možné určit správce nebo zvláštní kritéria pro jeho jmenování na základě práva Unie nebo členského státu.

Zpracovatelem je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, který zpracovává osobní údaje jménem správce.

Josef Donát upozornil na skutečnost, že je velice důležité si uvědomit, kdo je správce a kdo zpracovatel. Aby orgány veřejné moci (OVM) skutečně dostály všem svým novým povinnostem, doporučuje Josef Donát, aby si vždy uvědomovaly, že zpracování osobních údajů je vlastně téměř jakýkoliv úkon, který se s těmito údaji provádí. Tedy vždy je dobré si myslet, že údaje, s nimiž pracujeme, jsou osobními údaji, a vždy předpokládat, že je zpracováváme. Vědomí toho, kdo je správce a kdo zpracovatel, je důležité i s ohledem na to, kdo bude sankcionován. Správce, jak Josef Donát upozornil, určuje účel, podmínky a způsoby zpracování údajů, zatímco zpracovatel, tak činí jménem správce. Podle Josefa Donáta je tedy veřejná správa téměř vždy v úloze správce, zatímco případní dodavatelé IT řešení a služeb budou ve většině případů zpracovatelé.

VÍC NEŽ SOUHLAS

Zpracování osobních údajů je podle současné i budoucí legislativy na ochranu osobních údajů možné pouze na základě uzavřeného okruhu právních důvodů. Tyto právní důvody, jako je např. souhlas se zpracováním, oprávněný zájem či zpracování na základě zákonné povinnosti, zůstávají zachovány, nicméně, zejména pro OVM, se pravidla pro jejich uplatnění liší. Podle nového nařízení budou mít OVM zejména velice ztíženou možnost spoléhat se na souhlas se zpracováním. V preambuli k nařízení je výslovně řečeno, že vzhledem k nerovnému postavení subjektů údajů a OVM lze jen obtížně předpokládat, že souhlas lze považovat za svobodný. Zároveň zakotvuje nařízení ohledně svobody souhlasu důležité pravidlo, které říká, že poskytování určité služby nesmí být podmíněno poskytnutím souhlasu se zpracováním v rozsahu, který převyšuje rozsah nutný pro poskytování této služby. Pokud je tedy nabízená služba oddělitelná od části zpracování osobních údajů, subjekt údajů musí mít právo si vybrat. Ve výsledku lze tedy konstatovat, že OVM by podle GDPR neměly zpracovávat údaje na základě souhlasu subjektů údajů a pokud tak nyní činí, měly by do účinnosti GDPR začít spoléhat na jiný souhlas. Další důležité omezení pro OVM spočívá v ustanovení, které zakazuje OVM používat jako právní důvod oprávněný zájem.

Nově budou tedy OVM nejčastěji muset spoléhat na právní důvod zpracování na základě plnění právní povinnosti, které jim ukládá zákon a dále také na právní důvod zpracování na základě plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci. GDPR zmocňuje členské země k tomu, aby zachovaly či zavedly konkrétnější ustanovení, která budou použití těchto dvou právních důvodů dále upravovat. Konkrétní pravidla budou tedy známá až po přijetí implementačního předpisu.

NOVÁ PRÁVA FYZICKÝCH OSOB

GDPR mimo jiné upravuje některá stávající a zavádí zcela nová práva subjektů údajů vůči správcům, tedy i OVM. Jedná se především o:

- právo na výmaz (právo „být zapomenut"), tedy právo na odstranění osobních údajů, které se dotčeného subjektu údajů týkají (Josef Donát ale upozornil, že toto právo lze uplatnit pouze za naplnění některé z vymezených podmínek, jako je např. odvolání souhlasu, protiprávní zpracování, apod. Netýká se to ovšem situací, kdy se jedná o zpracování osobních údajů uložené zákonem);
- právo vznést námitku, tedy právo namítat proti zpracování ve veřejném zájmu nebo při výkonu veřejné moci (nebo proti zpracování na základě oprávněného zájmu, které však není pro OVM při plnění jejich úkolů relevantní), kdy je následně posuzováno, jestli převažuje individuální zájem subjektu údajů, nebo OVM;
- právo na přenositelnost údajů („portabilita"), tedy právo požadovat, aby správce údajů předal subjektu údajů jím poskytnuté údaje ve strojově čitelném formátu a právo žádat, aby je předal přímo jinému správci (zde je nutné upozornit, že toto právo se uplatní pouze při zpracování na základě souhlasu či plnění smlouvy).

S uplatňováním těchto nových zpráv úzce souvisí povinnost správce subjektu údajů v takovém uplatňování napomáhat. Správce tedy bude muset být vstřícný vůči subjektům dat a mít např. zavedená řešení typu hot-line, Help Desk, online formuláře, telefonní linky, apod.

Z hlediska nových práv subjektů údajů ve vztahu k OVM je důležité také ustanovení v čl. 23, který stanoví, že členské země mohou legislativními opatřeními omezit práva subjektů údajů a odpovídající povinnosti správců nebo zpracovatelů, a to v případech, kdy je toto omezení nutné za účelem zajištění důležitých veřejných zájmů, jako je např. národní bezpečnost, obrana, ochrana nezávislosti soudnictví či vymáhání občanskoprávních nároků.

JE TOHO HODNĚ A ZBÝVÁ PÁR MĚSÍCŮ

Závěrem svého vystoupení Josef Donát upozornil přítomné, že povinností, které na úřady (ale i komerční subjekty) dolehnou, je velké množství. Časově i zdrojově náročné může být s ohledem na velikost povinného subjektu např. zavedení potřebných opatření v oblasti bezpečnosti osobních údajů. Zároveň se situace poněkud ztěžuje zaváděním nových termínů, jako je například záměrná a standardní ochrana osobních údajů, čímž je stanovena povinnost vždy ze všeho nejdřív posuzovat, zda je potřeba zpracovávat osobní údaje, případně v jakém rozsahu a jakými prostředky a dále zvažovat, zda se jedná o zpracovatelské **minimum**, a jestli náhodou nezpracováváme údaje ve větším rozsahu, než je nutno. Mezi další povinnosti patří např. povinnost správce prověřovat zpracovatele, zda je kvalitní a bezpečný, protože jinak odpovědnost padne na správce. V případě, že dojde k bezpečnostnímu narušení, je při významném incidentu nutné jeho nahlášení dozorovému úřadu, ale i samotným subjektům osobních údajů, což může být komplikované. Správci musí rovněž brát v úvahu stávající smluvní závazky (s provozovateli a dodavateli IT služeb) a prověřovat je s ohledem na nové požadavky, nastavit součinnost při zabezpečení, hlášení incidentů atp.

V nařízení je upuštěno od povinnosti oznamovat záměr zpracovávat osobní údaje ÚOOÚ, nicméně toto je vyváženo zavedením povinnosti systematické evidence zpracování osobních údajů v nařízením stanoveném rozsahu a také povinností provádět interně tzv. posouzení dopadu ochrany osobních údajů v některých případech, kdy existuje riziko pro práva a svobody jednotlivců.

NOVÁ ROLE

Nařízení nově stanovuje pro některé správce povinnost jmenovat tzv. pověřence pro ochranu údajů. Jedná se o osobu, která bude nezávisle monitorovat dodržování souladu s nařízením a plnit další nařízením stanovené úkoly, jako je např. kontakt s ÚOOÚ. Tato osoba bude podřízená přímo vrcholnému managementu a musí jí být umožněn přístup ke všem procesům, které v rámci výkonu své funkce potřebuje. Pro OVM je jmenování pověřence povinné, nicméně s ohledem na organizační strukturu bude možné v některých případech jmenovat pro několik úřadů jednoho pověřence.

Kvalifikace a postavení pověřence pro osobní údaje:

- Pověřenec musí mít expertní znalost práva a praxe ochrany osobních údajů;
- pokud je zamezeno možnosti střetu zájmů, může tuto funkci vykonávat zaměstnanec subjektu, nebo může

pověřenec vykonávat činnost na základě smlouvy o poskytování služby;
- povinná organizace musí zajistit, že pověřenec bude o všech záležitostech týkajících se zpracování informován a musí zajistit také jeho faktickou nezávislost;
- pověřenec je vázán ohledně výkonu své funkce mlčenlivostí.

Úkoly pověřence:
- Pověřenec především poučuje povinnou organizaci o závazcích z právních předpisů o ochraně osobních údajů;
- dohlíží na soulad zpracování s legislativou na ochranu osobních údajů;
- spolupracuje s dozorovým úřadem; a je kontaktní osobou pro subjekty osobních údajů.

POKUTY A JINÉ SANKCE

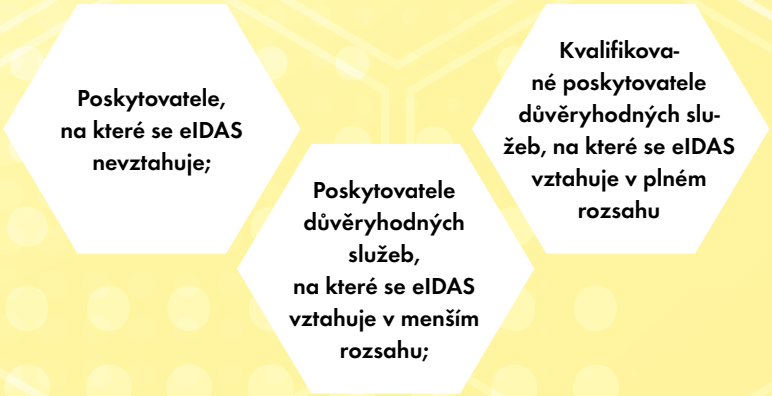
Že se nejedná o nic, co by měli brát správci a zpracovatelé na lehkou váhu, doložil na úplný závěr Josef Donát skutečností, že zatímco současná horní hranice sankce za porušení pravidel při zpracování osobních údajů činí v ČR 10 mil. Kč (nejvyšší byla uložena pokuta ve výši 3,6 mil. Kč), nyní to bude až 20 mil. EUR nebo 4 % z ročního celosvětového obratu organizace.

Pro OVM nicméně platí čl. 83 odst. 7, který říká, že „Členské státy mohou stanovit pravidla týkající se toho, zda a do jaké míry je možno ukládat správní pokuty orgánům veřejné moci a veřejným subjektům usazeným v daném členském státě." Pokud se však členské státy rozhodnou OVM pokuty neudělovat, musí dle čl. 84 stanovit pro tyto případy jiné sankce, které budou účinné, přiměřené a odrazující. Výsledná podoba těchto norem je však předmětem debaty a jistá bude, stejně jako v mnohých jiných případech, kdy jsou členské země zmocněny k národní úpravě, až s definitivním přijetím implementačního předpisu.

Odpovědnost poskytovatelů služeb vytvářejících důvěru podle eIDAS

Od 1. července 2016 je v celé Evropské unii účinné nařízení Evropského parlamentu a Rady (EU) č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu, známé pod zkratkou eIDAS. Převážná část nařízení se týká služeb vytvářejících důvěru, tj. služeb umožňujících používání elektronických podpisů, pečetí a časových razítek. Tedy služeb, které byly dosud označovány jako certifikační služby, a jejich poskytovatelé byli poskytovateli certifikačních služeb. Takto byly definovány v zákonu o elektronickém podpisu, dnes již zrušeném.

Podle nařízení eIDAS je možné poskytovatele důvěryhodných služeb rozdělit do tří skupin:



Nařízení eIDAS se nevztahuje zejména na ty poskytovatele, jejichž služby jsou využívány výhradně uvnitř uzavřených systémů a mezi určeným okruhem účastníků, přičemž nemají žádný vliv na třetí osoby. Jedná se například o systémy zavedené v podnicích nebo institucích za účelem řízení vnitřních procesů využívajících služby vytvářející důvěru.

Je tedy zřejmé, že režimu eIDAS by měly podléhat takové služby vytvářející důvěru, které jsou poskytovány veřejnosti a které tedy mají vliv na třetí osoby. Jejich poskytovatelé se mohou rozhodnout, zda postoupí náročné hodnocení, které eIDAS definuje, a získají statut kvalifikovaného poskytovatele. Podmínky pro získání a udržení tohoto statutu jsou sice náročné, ovšem umožňují poskytovat tzv. kvalifikované služby, které jsou akceptovatelné v rámci EU a které jsou v určitých agendách vyžadovány. Tak je tomu například podle nového zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, v případě komunikace, jejímž účastníkem je veřejnoprávní podepisující nebo jiná osoba v souvislosti s výkonem její působnosti.

Poskytovatelé důvěryhodných služeb, na které se eIDAS vztahuje, odpovídají za škodu, kterou úmyslně nebo z nedbalosti způsobí fyzické nebo právnické osobě nesplněním povinností dle nařízení eIDAS. Odlišná je však úprava důkazního břemene. „Nekvalifikovaní" poskytovatelé nejsou nositelé důkazního břemene, to naopak spočívá na fyzické nebo právnické osobě, která uplatňuje nárok na náhradu škody, tedy zpravidla na zákazníkovi. Kvalifikovaný poskytovatel naopak musí prokázat, že škoda nastala bez jeho úmyslu nebo nedbalosti. Musí tedy prokázat, že učinil vše potřebné, aby vzniku škody zabránil.

Nařízení eIDAS zcela konkrétně definuje povinnosti, které kvalifikovaný poskytovatel musí splňovat, a to jak při získání tohoto statutu, tak při vlastním provozu. S tím souvisí i stanovení sankcí, které takovému poskytovateli hrozí a které mohou činit při nesplnění celé řady povinností až

2 miliony Kč. Stejné výše může sice dosáhnout sankce i u „nekvalifikovaného" poskytovatele, ale pouze v případě nesplnění jediné a spíše obecně definované povinnosti týkající se přijetí vhodných technických a organizačních opatření k řízení rizik. Celkově je tedy odpovědnost kvalifikovaných poskytovatelů na výrazně vyšší úrovni.

Povinnosti poskytovatelů jsou definovány pro služby, které jsou již řadu let standardně poskytovány – vydávání certifikátů veřejného klíče a časových razítek. Zásady pro poskytování těchto služeb jsou všeobecně známé a příslušné technické normy jsou běžně používány. Nařízení eIDAS však stanoví i požadavky na nové služby. Jednou z nich je ověřování platnosti elektronických podpisů a elektronických pečetí, ale definována je celá řada dalších. V případě těchto nových služeb se může stát důkazní břemeno, je-li na straně klienta, skutečným břemenem a prokazování mu může způsobit značné problémy.

Lze očekávat, že elektronizace a s tím nezbytně i počet elektronických dokumentů poroste. Proto o novou službu ověřování platnosti elektronického podpisu zákazníci projevují značný zájem. K ní se v recitálu eIDAS uvádí, že:

„V zájmu zajištění právní jistoty ohledně platnosti podpisu je nezbytné upřesnit prvky kvalifikovaného elektronického podpisu, které by měla posoudit spoléhající se strana, jež provádí ověření platnosti. Upřesnění požadavků na kvalifikované poskytovatele služeb vytvářejících důvěru, kteří mohou poskytovat kvalifikovanou službu ověřování platnosti spoléhajícím se stranám, jež nejsou ochotny nebo schopny provádět ověřování platnosti kvalifikovaných elektronických podpisů samy, by navíc mělo soukromý a veřejný sektor podnítit k investicím do těchto služeb."

Příjemci elektronicky podepsaných dokumentů vědí, že správné ověření platnosti elektronického podpisu není triviální záležitostí. Je otázkou, zda je v praxi vždy prováděno řádně a v úplnosti. Tvůrci nařízení eIDAS si byli vědomi důležitosti této problematiky a stanovili konkrétní požadavky na ověřování platnosti kvalifikovaných elektronických podpisů. Příslušná služba je definována jako kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a využijí ji především ti, kdo nemají v úmyslu řešit problematiku ověřování vlastními silami a zároveň jsou příjemci větších objemů elektronicky podepsaných datových zpráv.

Zákon o službách vytvářejících důvěru pro elektronické transakce stanoví povinnost ověřování platnosti zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu, a to bez ohledu na to, zda byl elektronický podpis vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů nebo nikoliv. Není tedy rozhodující, zda byla data pro vytváření elektronického podpisu uložena na hodnocené čipové kartě nebo v úložišti operačního systému na pevném disku počítače.

Právní akty Evropské unie bývají terčem kritiky a někdy jsou považovány za příliš svazující. Jsme ale přesvědčeni, že nařízení eIDAS je krokem správným směrem. Směrnice o zásadách Společenství pro elektronické podpisy, kterou eIDAS zrušilo, byla přijata v roce 1999 a neodpovídala aktuálním požadavkům praxe. Tak například přes hranice členských států bylo možné bez dalšího uznávat pouze kvalifikované certifikáty. Požadavky na další služby stanovovaly jednotlivé členské státy podle své potřeby, a tak nebyly akceptovatelné za jejich hranicemi. To s ohledem na stále stoupající objem elektronické komunikace v rámci EU vytvářelo stále větší bariéry. Je nutné pamatovat i na skutečnost, že elektronicky podepsaný dokument, který byl prvotně určen pro komunikaci v rámci ČR, může být následně využit jako podklad pro komunikaci do jiného státu EU.

Ing. Petr Budiš, Ph.D.,MBA
předseda představenstva
a ředitel společnosti

Platforma KYBEZ na mikulovské konferenci aneb kam jsme pokročili po přijetí ZoKB

Díky přijetí zákona o kybernetické bezpečnosti se zvýšil zájem jak odborné, tak laické veřejnosti o tuto oblast informačních technologií. Nelze se proto divit, že i na mikulovské konferenci Egovernment 20:10 byla kybernetická bezpečnost skloňována ve všech pádech. Zástupci bezpečnostní platformy KYBEZ a společnosti GORDIC se pokusili shrnout, kam jsme se od výchozího bodu, tedy přijetí zákona o kybernetické bezpečnosti (ZoKB), posunuli.

Zákon o kybernetické bezpečnosti jako nový milník

Samotnou právní úpravu kybernetické bezpečnosti považuje Jaromír Řezáč, generální ředitel společnosti GORDIC, za zatím poslední z důležitých milníků, které nejvíce ovlivnily vývoj e-governmentu v naší zemi. Na letošním semináři ke kybernetické bezpečnosti, který se konal v Poslanecké sněmovně, mezi ně dále zařadil vznik spisové služby, projekt datových schránek, základní registry a Czech POINT jako systém, který vedl ke zrovnoprávnění elektronických procesů s analogovými. Zákon podle něho dává základ skutečně systémovému řešení této problematiky.

Jaromír Řezáč se letos ve Sněmovně rovněž pochvalně vyjádřil k tomu, jak Národní bezpečnostní úřad pojal zákon i jakým způsobem přistupuje k uvádění tohoto předpisu do praxe. Optimální řešení pro Českou republiku vidí v přiměřené, ohleduplné a ekonomicky přijatelné implementaci zákona, což zatím NBÚ v praxi naplňuje: *„Díky zákonu tak úřad pomohl už nyní splnit do značné míry požadavky normy NIS,"* připomněl evropskou směrnici o bezpečnosti sítí a informací (Network and Information Security, NIS), jež má vstoupit do našeho právního řádu do konce roku 2017. Norma mimo jiné stanoví, že „provozovatelé kritických infrastruktur" musí nasadit odpovídající opatření pro správu bezpečnostních rizik a hlášení závažných incidentů státním orgánům nebo pověřenému subjektu.

Platforma KYBEZ a vzdělávání

Nezbytnou součástí naplnění vize bezpečné infrastruktury (nejen) státu i samospráv je spolupráce na poli kybernetické bezpečnosti. I proto vznikla platforma KYBEZ, v současnosti největší sdružení firem z cyber security, angažující se v osvětové a vzdělávací činnosti a v přípravě komplexních bezpečnostních řešení. Ty jsou určeny jak pro provozovatele významných informačních systémů a kritické informační infrastruktury, tak i pro stovky dalších organizací, kterých se zajištění kybernetické bezpečnosti týká bezesporu také.

KYBEZ Platforma kybernetické bezpečnosti

> *„Naším cílem je upozorňovat na nebezpečí z podceňování kybernetických rizik, poskytovat konzultace, řešení a podporu pro veřejný i soukromý sektor. To se týká nejen organizací a úřadů, jež jsou povinné řešit kybernetickou bezpečnost ve smyslu zákona o kybernetické bezpečnosti, tak i všech ostatních. Protože i pro ně platí, že kybernetická bezpečnost není jen zákonná povinnost, ale existenční nutnost,"* říká Jaromír Řezáč.

Důležitým aspektem fungování platformy je intenzivní spolupráce s akademickou sférou. I proto vznikla vědecká rada, reprezentovaná osobnostmi, které se této problematice intenzivně věnují na akademické půdě. Ve druhém zářijovém týdnu proběhlo první zasedání vědecké rady platformy KYBEZ. Ta odsouhlasila záměr „evangelizace" široké veřejnosti pro oblast kybernetické bezpečnosti. Členy rady pro platformu KYBEZ se stali zástupci Střední školy informatiky, poštovnictví a finančnictví Brno a Univerzity Tomáše Bati Zlín. O zapojení dalších škol a vzdělávacích institucí se dále jedná.

Platforma se aktuálně zapojila do organizace „Středoškolské soutěže v kybernetické bezpečnosti", na které se podílí řada institucí České republiky v čele s NBÚ. Kybernetická soutěž je organizována pro všechny studenty středních škol. V rámci soutěže budou vytvořeny podklady, které mohou středoškolským pedagogům posloužit jako metodická pomůcka při vzdělávání studentů v oblasti kybernetické bezpečnosti, informačních a komunikačních technologií a programování.

Mikulov: Kam jsme tedy pokročili?

Ale zpět do Mikulova. Jan Dienstbier, viceprezident Českého institutu manažerů informační bezpečnosti, poznamenal, že jednotliví správci KII a VIS přistupují s odpovědností k plnění povinností vyplývajících ze zákona o kybernetické bezpečnosti. Existují však rozdíly mezi úrovní zabezpečení informačních a komunikačních systémů u jednotlivých správců.

> *„Nejvýraznější odlišnosti byly evidovány mezi správci v soukromé a veřejné sféře, kdy ve veřejné sféře bývá kybernetická bezpečnost a informační bezpečnost podceňována nebo strádá, kromě nedostatku expertů, také nedostatkem financí či administrativními a regulatorními bariérami, byť toto hodnocení samozřejmě nelze na veřejnou sféru uplatnit paušálně,"* citoval J. Dienstbier ze závěrů NKÚ.

Pro úspěšné zvládnutí bezpečnostních hrozeb budoucnosti bude záležet na spolupráci státu, firem a školství. Připomněl, že z celostátního pohledu nejsou přínosy cyber security pouze bezpečnostní, ale i ekonomické a vzdělanostní. Z oboru může těžit celá země. Jako příklad nám může posloužit Izrael. Ten se z pozice státu s průměrnou úrovní kybernetické bezpečnosti vypracoval v celosvětového lídra v této oblasti a informační technologie a kybernetická bezpečnost dnes tvoří významné procento na celkovém objemu průmyslu země.

> *„Kybernetická a informační bezpečnost bývá podceňována ve veřejné sféře,"* říká Jan Dienstbier.

Ing. Jan Dienstbier

- viceprezident ČIMIB
- vystudoval ČVUT obor automatizované systémy řízení. Celou svoji profesní karieru působí v oblasti ICT ve státní správě a v řadě předních dodavatelských firem.
- v současné době působní jako nezávislý konzultant.

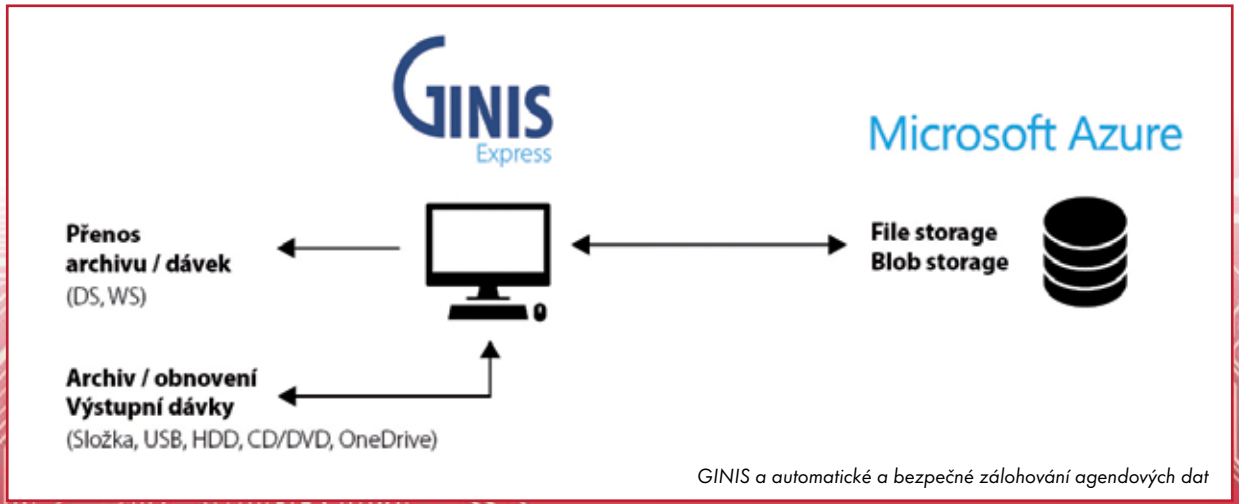
Tři role systému GINIS

Jan Dienstbier rovněž zmínil roli samotných agendových informačních systémů a představil možnost zálohování dat z informačního systému GINIS Express v cloudové platformě MS Azure. Jedná se o škálovatelné řešení s nulovou kapitálovou investicí a nízkými provozními náklady.

Samotný systém GINIS byl jako první v České republice certifikován na shodu s požadavky zákona. Pro jeho správnou implementaci je samozřejmě nutná analýza konkrétního provozního prostředí a zejména zasazení konfigurace do již existujícího technologického prostředí.

A jak v Mikulově také zaznělo, GINIS může hrát z hlediska kybernetické bezpečnosti ještě jednu roli. Jeho DRMS subsystém, tedy elektronická spisová služba, doplněná o specifické šablony, formuláře a parametry, představuje komplexní nástroj pro administrativní podporu procesů zákona o kybernetické bezpečnosti a normy pro řízení bezpečnosti ISO 27000.

Ing. Jan Dienstbier



GINIS a automatické a bezpečné zálohování agendových dat

Centrum projektů statutárního města Brna

Díky integraci aktuálních účetně-ekonomických a projektových dat v datové kostce získá vedení města nástroj pro přímý dohled nad velkými investičními akcemi.

Výchozí stav

Vedení statutárního města Brna (SMM) v minulosti postrádalo komplexní nástroj pro řízení klíčových investic města, který by umožňoval:

- dynamicky poskytovat pohled na stav projektů realizovaných městem;
- sledovat, zda realizace projektu je v souladu s rozpočtovanými prostředky a plánem;
- identifikovat a poskytnout jednoduchý náhled na odchylky v realizaci projektu.

Cílem tedy bylo sloučit pohledy na velké investiční akce z hlediska účetně-ekonomického a hlediska projektového řízení. Radnice by díky tomu získala větší přehled o investičních projektech s možností operativních zásahů vedení, pokud by se projekt nevyvíjel podle plánu.

Řešení

Na pracovních schůzkách v minulém roce zadalo vedení města tento úkol svým odborným útvarům. Dodavatel ekonomického systému, společnost GORDIC, měl v rámci

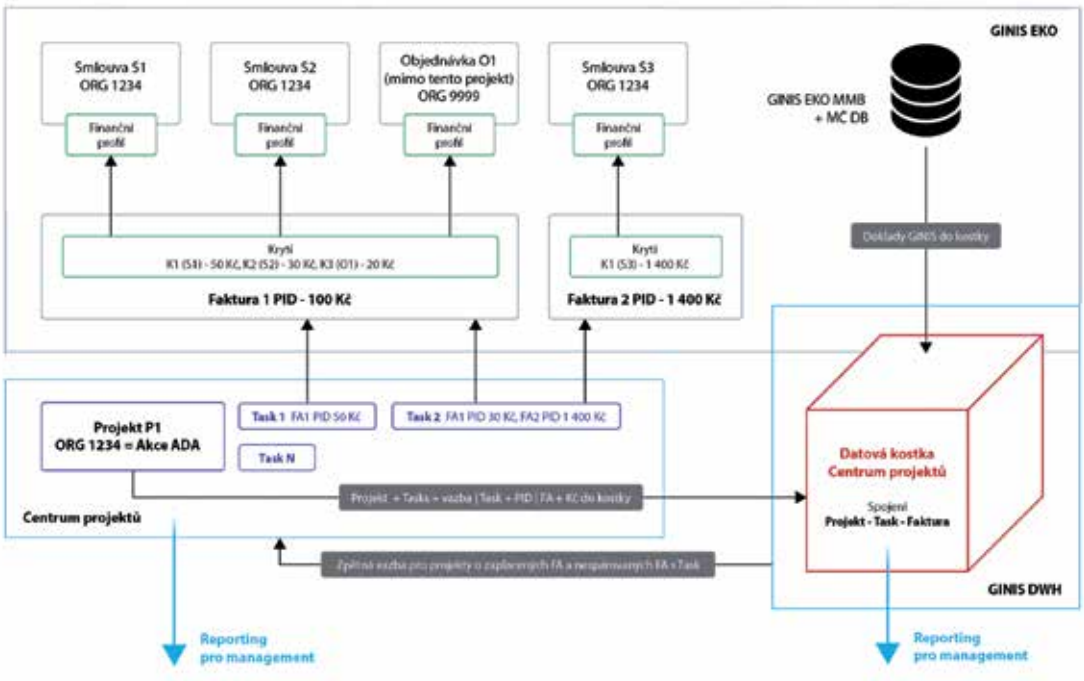


Schéma komplexního systému poskytujícího reporty pro management – centrum projektů, resp. GINIS DWH

řešení za úkol navrhnout pro tento účel datovou integraci v rámci komplexního řešení. Tím se stala datová kostka pro centrum projektů, čerpající on-line data z ekonomického systému GINIS EKO, integrovaná s projektovými daty, v té době aktuálně vedenými v aplikaci Microsoft Project.
Níže uvedená celková architektura byla navržena jako komplexní řešení splňující klíčové požadavky objednatele. Důležitou součástí řešení je fakt, že provozní data z GINIS EKO proudí do centra projektů až po provedení párování příslušných dokladů a vybraných částek z dokladů na jednotlivé tasky (etapy projektu). Informace o párování dokladů a další vybraná data pro centrum projektů se zpracovávají zcela automatizovaně. Jedná se o informace poskytované k projektům, např. ze smluv, dokladů o jejich úhradách, a informace o další řadě finančních položek z celého ekonomického systému města.
Centrum projektů je komplexní systém poskytující ucelené výstupy zejména pro vedení města, odbor investic i pro ekonomický odbor, který se do prací na projektu velmi aktivně zapojil. Po právě dokončované migraci projektových dat z Microsoft Project bude systém finálně provozován na platformě Share Point, resp. v prostředí Azure.

Výstupy

Při zobrazení dat z centra projektů, resp. datové kostky budou uživatelům umožněny pohledy poskytující informaci ve formě tzv. karty projektu. Ta kromě identifikace a postupu realizace projektu obsahuje například informace o jeho plánovaných výdajích v aktuálním i v dalších rozpočtových obdobích, ale i o rezervaci prostředků na projekt. K dispozici jsou také příslušné smlouvy, případně doklady s požadavkem na čerpání prostředků (faktury).
Nechybí samozřejmě ani aktuální stav čerpání prostředků na projektu, tj. skutečné výdaje (proplacené doklady) v členění podle jednotlivých tasků. Vedení je kromě toho informováno o změnách projektu z hlediska termínů. „Semaforová" vizualizace signalizuje, zda je projekt či jeho etapy v pořádku, zda je doporučen dozor, či se jedná o nestandardní vývoj.

Přínosy

Vybudovaný systém představuje komplexní, ale zároveň uživatelsky jednoduchý nástroj ke sledování průběhu klíčových investičních akcí, zejména z hlediska hlídání kritických odchylek, např. dodržení jejich harmonogramu, rozpočtu, avizování rizik. V případě avizovaných problémů mohou projektoví manažeři úřadu, příp. vedení města zasáhnout a řešit včas nápravu. Díky nalezení společné shody nad komplexním návrhem projektu mezi zapojenými odbory, resp. uživateli a pružnému přístupu dodavatelů při rozumně provedené datové i technologické integraci nedojde při plnění dat do centra projektů k výraznějšímu navýšení administrativní zátěže úřadu. Realizovaný systém je vhodný obecně k řízení investic v libovolném resortu či velké firmě.

Jaká data budou využita z GINIS EKO?

- identifikace projektu, zdrojem modul ADA (administrace akcí);
- rozpočtový profil projektu (v rozpočtu schválené prostředky na projekt, včetně jeho úprav), zdrojem je schválený a upravený rozpočet města;
- finanční profil smlouvy obsahující plán výdajů na smlouvu, zdrojem modul SML (smlouvy);
- rezervace, blokace a čerpání výdajů na smlouvu (projekt), zdrojem modul KDF (kniha došlých faktur), resp. obecně jakýkoliv (typicky výdajový) doklad vázaný ke smlouvě a projektu (poukaz, pokladní doklad, opravný doklad...).

Jaká data budou využita z MS Project?

- evidence projektu s jednoznačnou identifikací;
- harmonogram projektu, včetně milníků;
- etapizace projektu do tzv. tasků, včetně informací o činnosti v rámci tasku, jeho délce a finanční náročnosti;
- informace o čerpání prostředků na jednotlivé aktivity v rámci tasku s využitím podkladů z GINIS EKO.

Základní technologie

ERP: GORDIC GINIS v. 3.76
DWH: datový sklad GINIS
PM: Microsoft Project
DB server: ORACLE
Cloudová platforma: MS Azure

Ing. Jaroslav Hanák,
projektový manager společnosti
GORDIC spol. s r. o.

Den s Microsoftem

V rámci konferece ROK INFORMATIKY, která se letos konala v červnu v Náchodě, probíhala soutěž společnosti Microsoft, jejíž vítězové měli možnost navštívit tuto společnost v rámci tzv. Dne s Microsoftem. Stalo se tak 4. října 2016. Zástupci města Dobříš, statutárního města Prostějov a města Svitavy měli tak možnost poprvé nahlédnou „pod pokličku" společnosti Microsoft.

Den s Microsoftem proběhl ve velmi příjemné atmosféře. Během celého dne jsme výherce seznamovali s tím, jak naši zaměstnanci pracují s novými technologiemi, jak je využívají a jaké možnosti jim tyto prostředky nabízejí. Nejprve jsme našim hostům ukázali nové prostory v nichž Microsoft sídlí. Výherci soutěže tak měli možnost vidět, jak vypadá nový svět práce, digitální kancelář, spolupráce ve virtuálním prostředí a jak vypadají prostory pro zákazníky i pro zaměstnance.

V rámci oběda jsme s hosty diskutovali možnosti reálného nasazení jednotlivých řešení a technologií na městských úřadech. Ihned poté jsme se pustili do ukázek jednotlivých řešení postavených na platformě Office 365. Kromě toho, že to je řešení které Microsoft prodává a nabízí, jedná se i o prostředí, se kterým ve společnosti Microsoft jednotlivě týmy, skupiny lidí a jednotlivci pracují. Debata k využití těchto prostředků se protáhla do pozdního odpoledne a týkala se především toho, jak by bylo možné tato řešení nasadit v jednotlivých městech s ohledem na aktuální situaci, používaná řešení a možnosti, které jednotlivé městské úřady mají.

Byla to živá diskuse plná dalších nápadů a už teď se výherci dohodli na dalším setkání, kde by své poznatky z návštěvy společnosti Microsoft chtěli dále rozvíjet směrem k jejich nasazení v jednotlivých městech. Den s Microsoftem skončil s jednoznačným závěrem, že taková setkání mají smysl a v podobných akcích by jsme měli pokračovat i v následujícím období. Už teď se těšíme na pokračování.

Ľubomír Bandžuch
Manažer veřejné správy
Microsoft Czech Republic

Microsoft

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 platťe 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

- Platťe 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 · CANONICAL · mongolab · php

Misska z Mikulova odjela SEATEM s iPadem pod paží

V rámci konference e-government 20:10, aneb žijem si jak na zámku, ať to trvá věčně probíhá tradiční společenský večer, jehož součástí je vyvrcholení soutěže MISS EGOVERNMENT 2016.

Dámy, které se dostaly do finálového večera, si musely připravit vlastní vystoupení – taneční či pěvecké číslo, hereckou scénku atp. Krom této volné disciplíny podstoupily rovněž rozhovor s moderátorem, v němž přítomným divákům a porotě představily sebe sama, své zájmy a hlavně se takto snažily zaujmout. Porota totiž jednotlivé výkony sledovala a bodovala. Kromě poroty však bylo důležité i mínění publika, a to při volbě Miss Sympatie.

Porota, které předsedala náměstkyně ministra vnitra pro řízení sekce veřejné správy **Mgr. Jana Vildumetzová**, spolu s Miss Egovernment 2015 **Hanou Pospíšilovou**, za vydatné podpory náměstka ministra vnitra pro státní službu **RNDr. Josefa Postráneckého** a zástupců hlavních partnerů konference, společností CISCO a GORDIC, určila nakonec, že **Miss Egovernment 2016** se stala **Karolína Doskočilová** z České pošty, s.p., Letovice. **Na druhém místě** byla vyhlášena **Jana Lengálová** z České pošty, s.p., Brno a **druhou vicemiss** se stala **Michaela Bouškova** z České pošty, s.p., Praha 2.

Úspěch **Jany Lengálové** ještě podrthla skutečnost, že byla vyhlášena rovněž **Miss Sympatie**, tedy že kromě poroty si získala také přízeň přítomných diváků. Tyto výsledky mimo jiné znamenají, že reprezentantky České pošty tentokrát drtivě porazily zástupkyně úřadů veřejné a státní správy. Měla by to tedy být pro příští roky určitá výzva jak pro ministerstva, kraje, města, tak obce, aby nominovaly své sympatické pracovnice do soutěže.
Vítězka soutěže si odvezla, kromě poháru ze skláren Rückl, iPad, který věnoval platinový partner konference, společnost CISCO. Dále voucher na zapůjčení nového modelu vozu SEAT či voucher na víkendový pobyt ve wellness centru hotelu Galant v Mikulově pro dvě osoby. Tyto pobyty získaly i dámy na druhém a třetím místě. Všechny dámy, nejen ty na prvních místech, obdržely rovněž dárky od MV ČR a České pošty, odborných partnerů konference.

ICZ

DÍKY SPRÁVNÝM INFORMACÍM SE DO TOHO MŮŽETE POŘÁDNĚ OPŘÍT.

STEJNĚ JAKO V OSOBNÍM, TAK I V PROFESNÍM ŽIVOTĚ SE PODMÍNKY ČASTO MĚNÍ. KDYŽ MÁ TÝM TY SPRÁVNÉ INFORMACE, DOKÁŽE SI VŽDY PORADIT.
PROTO JSOU ZDE INFORMAČNÍ SYSTÉMY ICZ.

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

www.i.cz

My jsme poté, co utichl potlesk a dozněly fanfáry, požádali vítězky o krátké rozhovory. Ptali jsme se jich:

1. Jak prožívaly finálový večer, jak na ně působila atmosféra a jaké byly jejich pocity v průběhu večera a při vyhlašování výsledků?
2. Zda by se do soutěže, po zkušenostech, které nyní mají, přihlásily znovu? Jakou „přípravu" by případně doporučily těm, které je budou v příštím ročníku následovat?
3. Jaká byla reakce okolí na jejich umístění? Jak to s nimi prožívali v rodině nebo na pracovišti?
4. Co by organizátorům doporučily do příštích let zlepšit, nebo vymyslet, co v Mikulově chybí?

Miss Egovernment 2016 Karolína Doskočilová

1. Myslím, že budu hovořit za všechny zúčastněné dámy, když řeknu, že panovala mírná nervozita na všech frontách. Mikulov je nádherné místo a jeho zámek je opravdu skvostem, tudíž atmosféra celého večera byla jedním slovem kouzelná. Co se týče mé osoby, byla jsem velice zvědavá na průběh celého večera. Organizace však byla skvělá, a tak se vše neslo ve velmi přátelském duchu. Vyhlašování výsledků bylo velice napínavé a titul Miss Egovernment jsem opravdu nečekala. Pro mě korunka znamenala úžasnou tečku za celým večerem.

2. Přihlásila bych se znovu. Jako pracovnice přepážky se službami Czech POINT jsem soutěž vnímala jako poděkování za odváděnou práci a velice příjemné zpestření pro ty z nás, které se zabývají touto prací. Příprava je samozřejmě individuální. Každá soutěžící byla něčím výjimečná a předvedla volnou disciplínu, kterou si sama zvolila. Nejlepší přípravou je však dobrá nálada a úsměv.

3. Do Mikulova jsem jela podpořena rodinou a známými, kteří mi opravdu fandili se vším všudy. Byli mi velkou oporou a já jim za to velice děkuji. Původní myšlenka vypravit celou poštu i dodejnu Letovice byla bohužel organizačně nemožná, avšak druhý den jsem byla na pracovišti uvítána jako pravá Miss. Dostala jsem květiny, blahopřání a samozřejmě proběhlo i zkoušení korunky. Byl to nepopsatelný pocit.

4. Organizace i místo, jak jsem již zmiňovala, vše bylo kouzelné. Nádvoří dodalo soutěži na vážnosti a kráse. Počasí bylo chladnější, ale to ovlivnit nelze. Vzkázala bych organizátorům, aby udrželi standard této soutěže a poděkovala jim za nezapomenutelný večer.

I. Vicemiss Egovernment 2016 a zároveň i Miss Sympatie Jana Lengálová

1. Finálový večer byl nad moje očekávání... když pominu chladnější počasí, tak atmosféra byla užasná.
2. Jestli bych se znovu přihlásila? To je otázkou!!! Přihlásily mě kolegyně, takže těžko říct, ale každopádně toho vůbec nelituju, zajímavá zkušenost. Rada zní, nepřipravovat se – stačí být přirozená.
3. Reakce mého okolí byla překvapující jak v rodině, tak na pracovišti. Nejvtipnější na tom je, že mi všichni říkají ‚MISSKO', ale málo kdo ví, co znamená Egovernment, takže po vysvětlení toho výrazu říkají: „Tak to seš dobrá".
4. Organizátorům bych nic nevytýkala, byl to skvělý večer, plný zábavy.

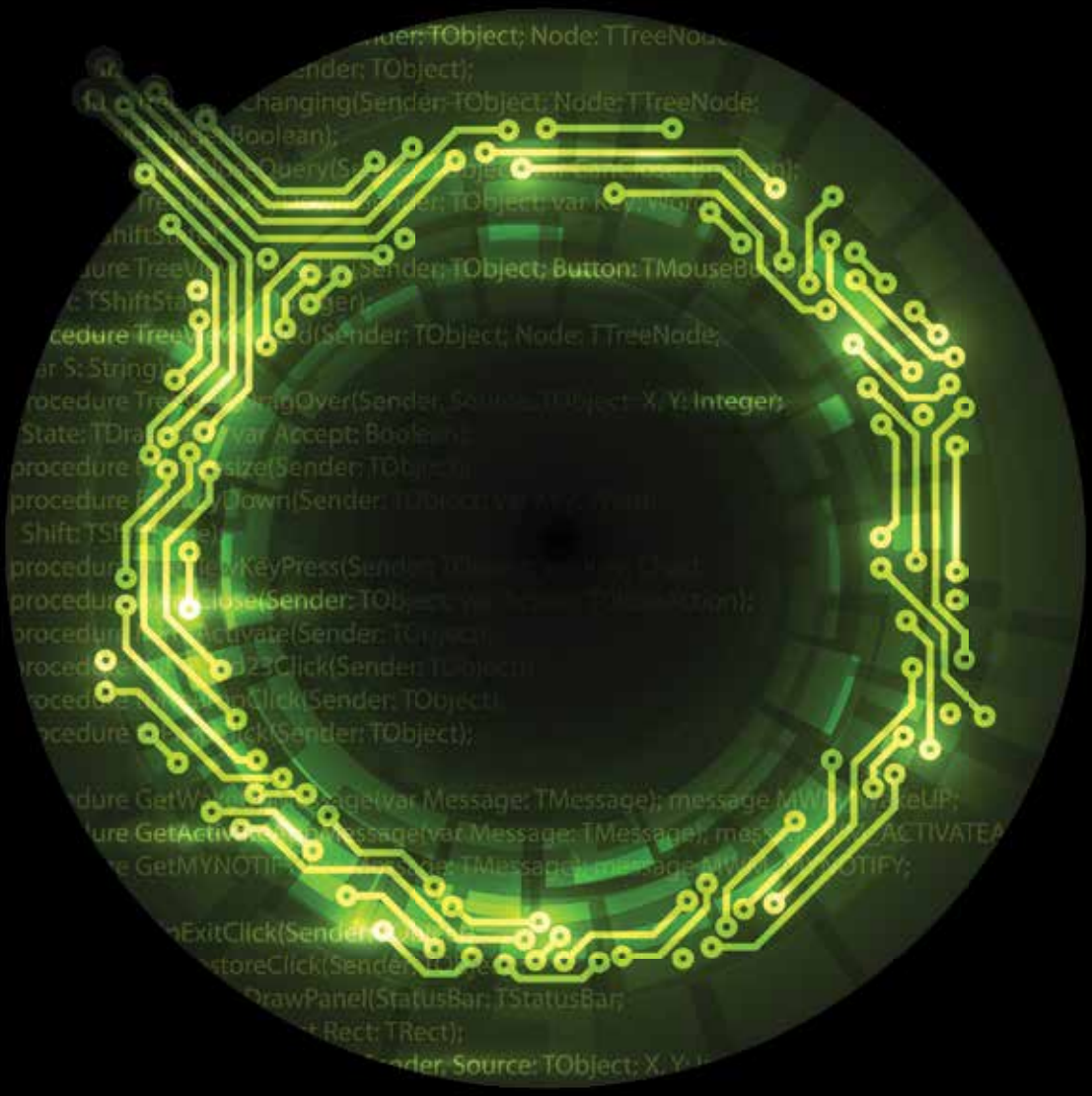
II. Vicemiss Egovernment 2016 Michaela Bouškova

1. Do Mikulova na finálový večer jsme přijely někdy v odpoledních hodinách, aby byl čas na přípravu finálového večera. Ze začátku jsem se obávala, jaké budou konkurentky, jestli budou dávat špendlíky do bot či podobné věci (smích), ale nebylo tomu tak, holky byly super, rozuměly jsme si a i mně to pomáhalo nebýt tolik nervózní z výstupu na pódiu, což se mi zrovna při rozhovoru moc nedařilo, protože nervóza je prostě ve mně a pokazila jsem ho. Z následující volné disciplíny jsem už měla lepší pocit.
2. Samozřejmě jsem měla vybrané své favoritky a při vyhlašování výsledků jsem byla celkem překvapená, že se jedna z mých favoritek neumístila. Celé to probíhalo tak rychle, sedět na trůnu je něco nezapomenutelného, nikdy jsem takhle nic nevyhrála, tak jsem si to užívala maximálně naplno. Ceny byly také skvělé, už se moc těšíme s přítelem na jednu z cen, a to víkendový pobyt v Mikulově.

3. Do soutěže mě přihlásila moje paní vedoucí, nejdříve jsem účast odmítala, ale pak jsem si říkala, proč ne, že to bude fajn zkušenost. Nikomu jsem o tom ale neříkala, věděly to jen kolegyně a ty mi samozřejmě gratulovaly, vedoucí byla z umístění nadšená. Věděl to přítel, který mi dělal na finálovém večeru doprovod, ten mi od té doby říká, že jsem jeho „Misska" (místo „Míša").
4. Určitě nebýt nervózní, jako jsem byla já, nikdo vás neukousne, ale je to opravdu těžké mluvit před tolika lidmi nebo alespoň pro mě, ale obecenstvo bylo skvělé, po vyhlašování, když jsem se vydala na cestu zpět do Prahy, mě lidé zastavovali a blahopřáli mi, to mi udělalo opravdu velkou radost, a pokud to teď čtou, ještě jednou děkuji.

Děkujeme a vítězkám blahopřejeme. Nyní zpracováváme poznatky z letošního ročníku a již brzy vyhlásíme ročník nový. Včas Vás budeme informovat, abyste mohli sebe, nebo své sympatické kolegyně přihlásit. Případně sledujte **www.egovernment.cz/miss**.

Deloitte.



Jsme Deloitte

A na výsledku nám záleží

Tečka

GORDIC®

Interaktivně. Inteligentně. Intuitivně.

informační systémy – kybernetická bezpečnost
internet věcí – cloudová řešení – mobilní aplikace
card management

www.gordic.cz