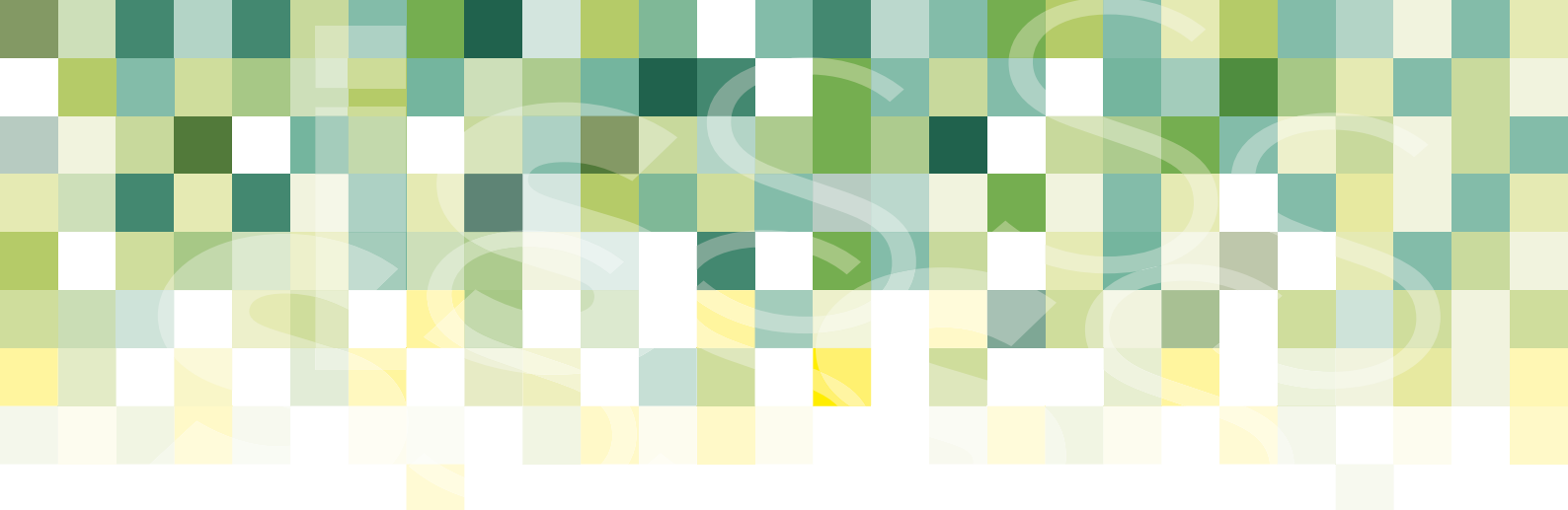




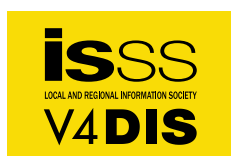
18. ROČNÍK KONFERENCE

ISSS 2015

DOPROVODNÁ MEZINÁRODNÍ KONFERENCE V4DIS

13.–14. dubna 2015 Hradec Králové
Kongresové centrum ALDIS

SBORNÍK KONFERENCE



Obsah

Úvodní slovo	3
<i>Pavel Kysilka, generální ředitel a předseda představenstva České spořitelny, a. s.</i>	
Úvodní slovo	4
<i>RNDr. Tomáš Renčín, výkonný ředitel konference</i>	

Informace

Seznam vystavovatelů a partnerů konference	6
Orientační plán kongresového centra ALDIS	7
Programový výbor a realizační tým konference ISSS/V4DIS 2015	10
Informace pro účastníky konference	11

Dokumenty

V4DIS 2015 – dvanáctý ročník	13
Český zavináč 2015	14
17. ročník soutěže Zlatý erb	16
Rok průmyslu a technického vzdělávání 2015	17
<i>David Vondrák, koordinátor kampaně „Rok průmyslu a technického vzdělávání 2015“</i>	

Přednášky

Nariadení eIDAS – co se aktuálně připravuje	20
<i>Filip Bílek, odbor eGovernmentu, Ministerstvo vnitra ČR</i>	
Administrativní audit je příspěvkem k vyšší efektivitě i bezpečnosti	24
<i>Ing. Miroslav Čejka, vedoucí týmu Spisové služby GORDIC spol. s r. o.</i>	
Fujitsu, místo plastu lidská dlaň	26
<i>Martin Černý, Senior project manager, Fujitsu Technology Solutions s.r.o.</i>	
Implementace .NET portálu na cloudové platformě Microsoft Azure	28
<i>David Hláček, YOUR SYSTEM, spol. s r. o.</i>	
Software pro podporu krajského krizového řízení a plánování, risk managementu, využití bezpečnostních dronů ve spojení s technologiemi Microsoft	33
<i>Ing. Rostislav Hlosta, vedoucí odboru Business Development, VÍTKOVICE IT SOLUTIONS a.s.</i>	
Rychlý mobilní internet a televizní signál mohou nerušeně existovat vedle sebe	39
<i>Ing. Miroslav Charbuský, Český telekomunikační úřad</i>	
Interaktivní úřad	40
<i>Ing. Jiří Ilčák, programátor, analytik GORDIC spol. s r. o.</i>	
GeoInfoStrategie	41
<i>RNDr. Eva Kubátová, odbor eGovernmentu, Ministerstvo vnitra ČR</i>	
Portal for ArcGIS	42
<i>Ing. Radek Kuttelwascher, vedoucí oddělení technické podpory prodeje, ARCDATA PRAHA, s.r.o.</i>	
Dohledový systém GINIS upozorňuje s předstihem na hrozící průřvihy	44
<i>Bc. Jan Kuttich, programátor GORDIC spol. s r. o.</i>	
Srovnání elektronické značky a elektronické pečeti	45
<i>Mgr. Tomáš Lechner, Ph.D., Vysoká škola ekonomická v Praze, Národohospodářská fakulta, Katedra práva</i>	
Moderní zdravotnictví pro moderní obce	51
<i>Peter Linhardt, eHealth senior consultant, NESS Czech s.r.o.</i>	
Mobilní aplikace pro turistu 3. tisíciletí	53
<i>Ing. Daniela Mikšová Mandáková, Bc. Robert Průcha, Turistické informační centrum Hradec Králové</i>	

SIEM a jak vyhovět podmínkám zákona o kybernetické bezpečnosti	58
<i>Ing. Maroš Mihalič, Country Manager, Novell-Praha, s.r.o.</i>	
Fungování základních registrů	63
<i>Ing. Michal Pešek, ředitel; Mgr. Marek Hejduk, pracovník pro vztah s veřejností, Správa základních registrů</i>	
Transparentní úřad	68
<i>Tomáš Pitrocha, obec Domašov; Mgr. Tomáš Lechner, Ph.D., Triada, spol. s r. o.</i>	
V elektronizaci, a tedy i bezpečnosti, medikačního procesu za Evropou zaostáváme	74
<i>Ing. Simona Plischke, výkonná ředitelka, HC Logic, s. r. o.</i>	
Fujitsu – když vaše smysly nestačí	77
<i>Milan Podivín, Head of Direct Business - Commercial and Public Sector for CZ & SK, Fujitsu Technology Solutions s.r.o.</i>	
Stoupá význam softwarové podpory finanční kontroly	80
<i>Ing. Vladimír Přeck, marketingový specialista, GORDIC spol. s r. o.</i>	
Spisová služba nikoliv jako nutné zlo, ale jako užitečný pomocník	81
<i>Bc. Irina Rálišová, MěÚ Sezemice; Mgr. Tomáš Lechner, Ph.D., Triada, spol. s r. o.</i>	
Výhody integrovaného informačního systému města	85
<i>Vladislava Šarkadyová, MěÚ Ústě; Mgr. Tomáš Lechner, Ph.D., Triada, spol. s r. o.</i>	
MPSV podpoří rozvoj využití asistivních technologií.	90
<i>RNDr. Jiří Schlanger, Ministerstvo práce a sociálních věcí ČR</i>	
Digitální model veřejné správy	92
<i>PhDr. et Mgr. Zdeněk Šimek, IT vývojář MV ČR, Mgr. Eva Šimková Heřková, analytik MV ČR</i>	
ZoKB – nutnost či zbytečný luxus? Bezpečnost?	98
<i>Jitka Sládková, Jiří Sedláček, Network Security Monitoring Cluster</i>	
Boj s korupcí zahrnuje i vzdělávání	102
<i>Ondřej Štrba, Technology Unit Manager, Servodata a.s.</i>	
Eskorty budou minulostí. Vyslýchání posadí před kameru	106
<i>Květoslav Štrunc, Cisco Systems (Czech Republic) s.r.o.</i>	
Kybernetická bezpečnost.....	110
<i>Ing. Igor Štverka, MBA, Sales Manager GORDIC spol. s r. o.</i>	
Základní registry jedou naplno!	111
<i>Zpracoval: Správa základních registrů a Ministerstvo vnitra ČR</i>	
Regulátor telekomunikačních a poštovních služeb	115
<i>Český telekomunikační úřad</i>	

Katalog

Generální partner konference	117
Hlavní partneři konference.....	118
Hlavní odborný partner konference.....	120
Partneři konference	121
Partneři odborných bloků	124
Spolupracující instituce a sdružení.....	125
Kraje a města.....	127
Ministerstva.....	128
Prezentace firem.....	129
Pořadatelé.....	139

Úvodní slovo Pavla Kysilky, generálního ředitele a předsedy představenstva České spořitelny, a. s., generálního partnera konference ISSS 2015

Vážené dámy, vážení pánové,

rád bych Vás i letos přivítal na konferenci ISSS, tentokrát už na osmnáctém ročníku. Jsem potěšen, že Česká spořitelna je i letos partnerem konference, která vždy přináší nový vhled do oblasti informačních a komunikačních technologií. Ty považuji právě v bankovníctví za klíčové i ve styku se zákazníky. Těším se, že během letošního ročníku budeme pokračovat v diskusi z loňského roku, která se zaměřila mimo jiné na důvody, proč v této oblasti Česká republika stále ještě zaostává za mnoha zeměmi ve světě. Máme za sebou v e-governmentu v ČR ovšem i několik úspěchů – mohu zmínit úspěšný projekt CzechPoint a platformu datových schránek. Tato řešení přispěla k optimalizaci a zrychlení zásadních procesů veřejné správy.

I vzhledem k tomu, že Česká spořitelna je největší bankou v České republice, dlouhodobě se zabýváme otázkou ochrany dat a osobních údajů našich klientů. Jsem přesvědčen, že je to jedna z nejdůležitějších oblastí, která by měla fungovat opravdu bezchybně. Dále je pro nás klíčový e-banking. Chceme pro zákazníky bezchybný proces založení si nového bankovní účtu online s využitím státem garantované elektronické identity, autentizace a kvalifikovaného elektronického podpisu.

Během dvou dnů konference tedy společně probereme tak zásadní témata jako veřejné zakázky, získávání prostředků na IT projekty, záležitost mobilních a cloudových technologií, které se nás v bankovníctví velmi dotýkají, stejně jako oblast kybernetické bezpečnosti.

Těším se na společné diskuse na všechna tato témata spolu se špičkami domácí politické scény, zástupci veřejné správy z České republiky i zahraničí a dalšími významnými osobnostmi.

*Pavel Kysilka,
generální ředitel a předseda představenstva
České spořitelny, a. s.*

Úvodní slovo RNDr. Tomáše Renčina, výkonného ředitele konference

Dámy a pánové, milí hosté a vážení kolegové,

dovolte, abych vás přivítal na již 18. ročníku konference ISSS, která je již podvanácté doprovázena visegrádskou konferencí V4DIS, a v současné době zastává pozici jedné z největších akcí svého druhu v celém regionu střední a východní Evropy.

V kongresovém centru Aldis se opět po roce scházejí vrcholní politici, zástupci ministerstev, státních orgánů i samospráv, informatici úřadů obcí, měst i krajů, stejně jako desítky odborníků, kteří se zabývají informatizací veřejné správy, i zástupci dodavatelů technologií a služeb do celého segmentu veřejné správy, aby zde jednali o aktuální situaci v oblasti e-governmentu a probíhající reformě veřejné správy.

Společně se ohlédneme za vším podstatným, co se v průběhu uplynulého roku událo, probereme klíčové projekty a jejich další rozvoj a samozřejmě se budeme zabývat budoucností. Nebudou chybět témata jako e-identita, kybernetická bezpečnost, veřejné zakázky, financování projektů z fondů EU, elektronizace zdravotnictví, mobilní řešení pro veřejnou správu, digitalizace a archivace dokumentů a mnohá další. Vedle maratónu přednášek a diskusí se uskuteční také významné doprovodné akce, jako například zasedání Rady vlády pro informační společnost, jednání komisí Rady Asociace krajů či setkání Sdružení tajemníků obecních a městských úřadů.

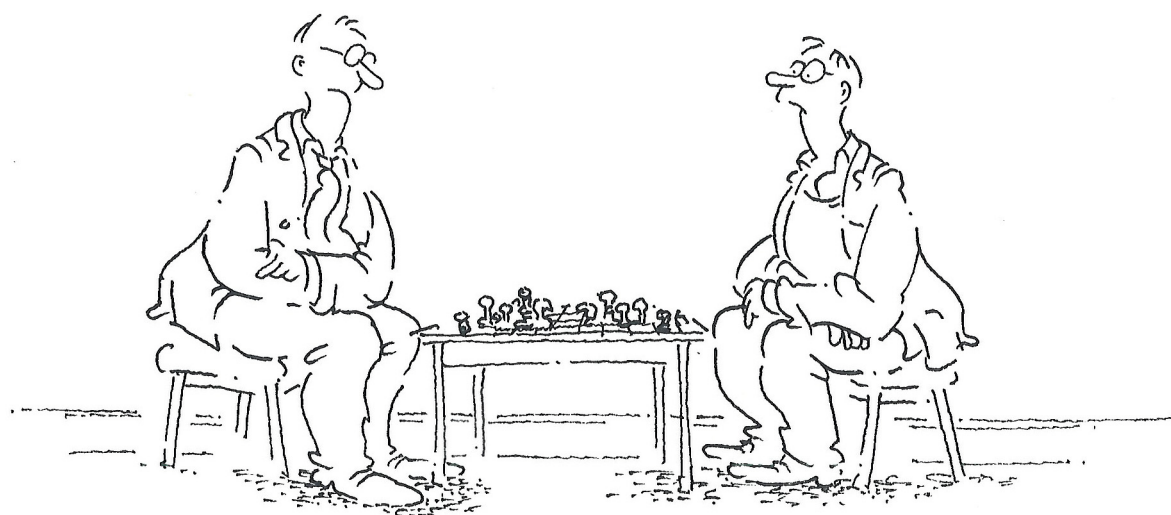
Naše díky patří Kraji Vysočina za spolupořadatelství, Ministerstvu vnitra ČR za spolupráci na programu, České spořitelně jako generálnímu partnerovi akce, městu Hradec Králové coby hostiteli i všem ostatním spolupracovníkům a partnerům, kteří se zasloužili o úspěšnou realizaci. Nesmím zapomenout na ty, kdo této akci poskytli osobní záštitu – premiéra a členy vlády, Asociaci krajů ČR i hejtmana Královéhradeckého kraje, stejně jako na místopředsedu Senátu Parlamentu ČR, který tradičně zaštiťuje visegrádskou konferenci. Zmínit musím také paní komisařku Věru Jourovou, která zde zastupuje Evropskou komisi, navazuje na loňskou osobní účast místopředsedkyně EK a místopředsedy Evropského parlamentu a stvrzuje unikátní pozici této akce v celoevropském měřítku.

Celý organizační tým samozřejmě velmi těší, že v celém spektru státní správy i samospráv, stejně jako mezi odborníky a dodavateli produktů a služeb, je o účast na hradecké konferenci stále velký zájem. Velice si vážíme také toho, že si sem každoročně najdou cestu i vrcholní představitelé států, mohou sdělit své vize a plány více než dvěma tisícovkám přítomných účastníků a v mnoha případech se i seznámit s jejich pohledem na konkrétní záležitost.

Věřím, že i osmnáctý ročník konference ISSS/V4DIS bude úspěšný a že zde najdete mnoho zajímavostí, potřebných informací i inspirace pro vaši další práci. Děkujeme vám za účast, těší nás vaše důvěra a doufáme, že ji ani letos nezklameme.

*RNDr. Tomáš Renčín,
výkonný ředitel konferenc*

INFORMACE



PROMIŇTE DOTAZ - HRAJEME ŠACHY NEBO ČLOVĚČE, NEZLOB SE ?

SEZNAM VYSTAVOVATELŮ

PARTNEŘI KONFERENCE

GENERÁLNÍ PARTNER	UMÍSTĚNÍ	STÁNEK
Česká spořitelna, a. s.	1. patro	26

HLAVNÍ PARTNEŘI	UMÍSTĚNÍ	STÁNEK
Atos IT Solutions and Services, s. r. o.		
Cisco Systems (Czech Republic) s.r.o.		
Česká pošta, s. p.	1. patro	17
ICZ a.s.	1. patro	25
VITA software, s.r.o.	1. patro	22

HLAVNÍ ODBORNÝ PARTNER	UMÍSTĚNÍ	STÁNEK
Microsoft s.r.o.	1. patro	12

PARTNEŘI	UMÍSTĚNÍ	STÁNEK
Asseco Central Europe, a. s.	1. patro	10
AV MEDIA, a. s.	1. patro	11
Citrix Systems Czech Republic s.r.o.	1. patro	31
DATASYS s.r.o.		
Fujitsu Technology Solutions s.r.o.		
GORDIC spol. s r. o.	1. patro	29
NEWPS.CZ s.r.o.		
O2 Czech Republic a.s.	přízemí	51

ABECEDNÍ SEZNAM EXPOZIC

EXPOZICE	UMÍSTĚNÍ	STÁNEK
ARCDATA PRAHA, s.r.o.	1. patro	20
Asseco Central Europe, a. s.	1. patro	10
ATLAS consulting spol. s r.o. – CODEXIS	přízemí	47
AV MEDIA, a. s.	1. patro	11
AVERIA LTD - org. složka	přízemí	57
BiZZdesign Česká republika, s.r.o.	1. patro	23
Citrix Systems Czech Republic s.r.o.	1. patro	31
Corpus Solutions a.s.	1. patro	30
CZ.NIC, z. s. p. o.	přízemí	41
ČD - Telematika a.s.	přízemí	53
Česká pošta, s. p.	1. patro	17
Česká spořitelna, a. s.	1. patro	26
Český telekomunikační úřad	přízemí	45
Český úřad zeměměřický a katastrální	1. patro	2
DIGIS, spol. s r. o.	1. patro	16
GEOVAP, spol. s r.o.	1. patro	9
GEPRO spol. s r.o.	1. patro	3
GORDIC spol. s r. o.	1. patro	29
ICZ a.s.	1. patro	25
IterSoft s.r.o. Choceň	1. patro	13
Kraj Vysočina	1. patro	33
MARBES CONSULTING s.r.o.	1. patro	14
Microsoft s.r.o.	1. patro	12
Ministerstvo pro místní rozvoj ČR	1. patro	1
Ministerstvo vnitra ČR	2. patro	80

EXPOZICE	UMÍSTĚNÍ	STÁNEK
Ministerstvo zemědělství ČR	přízemí	49
Network Security Monitoring Cluster	přízemí	46
NEWTON Media, a.s.	1. patro	34
O2 Czech Republic a.s.	přízemí	51
OKI Systems (Czech and Slovak) s.r.o.	přízemí	56
OKsystem a.s.	1. patro	27
QCM, s.r.o.	1. patro	28
Software602 a.s.	1. patro	7
Státní pokladna Centrum sdílených služeb, s. p.	1. patro	32
STÁTNÍ TISKÁRNA CENIN, státní podnik	1. patro	5
STYRAX, a.s.	1. patro	6
Tender systems s.r.o.	přízemí	54
TRIADA, spol. s r. o.	1. patro	39
Turistické informační centrum Hradec Králové	přízemí	52
Tyflo Centrum Brno, o. p. s.	2. patro	81
T-MAPY spol. s r.o.	1. patro	15
T-Mobile Czech Republic a.s.	1. patro	4
VEEAM SOFTWARE	přízemí	55
Vema, a. s.	1. patro	19
VERA, spol. s r.o.	přízemí	43
VITA software, s.r.o.	1. patro	22
Vysoká škola CEVRO Institut, o.p.s.	1. patro	21
WEBHOUSE, s. r. o.	přízemí	42
Wolters Kluwer, a.s.	1. patro	8
Zeměměřický úřad	1. patro	2

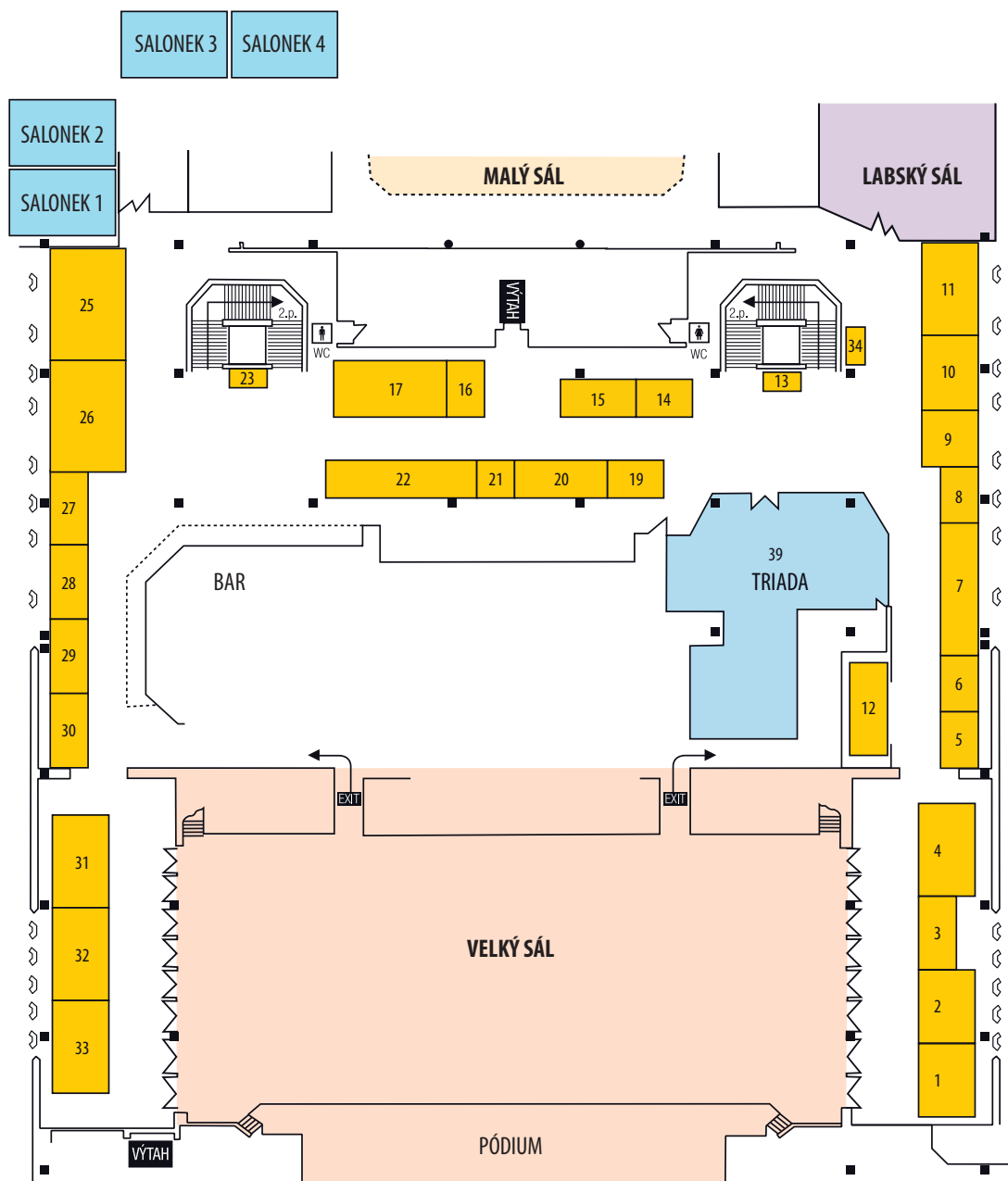
PŘÍZEMÍ



EXPOZICE	STÁNEK
ATLAS consulting spol. s r.o. – CODEXIS	47
AVERIA LTD - org. složka	57
CZ.NIC, z. s. p. o.	41
ČD - Telematika a.s.	53
Český telekomunikační úřad	45
Ministerstvo zemědělství ČR	49
Network Security Monitoring Cluster	46

EXPOZICE	STÁNEK
O2 Czech Republic a.s.	51
OKI Systems (Czech and Slovak) s.r.o.	56
Tender systems s.r.o.	54
Turistické informační centrum Hradec Králové	52
VEEAM SOFTWARE	55
VERA, spol. s r.o.	43
WEBHOUSE, s. r. o.	42

1. PATRO

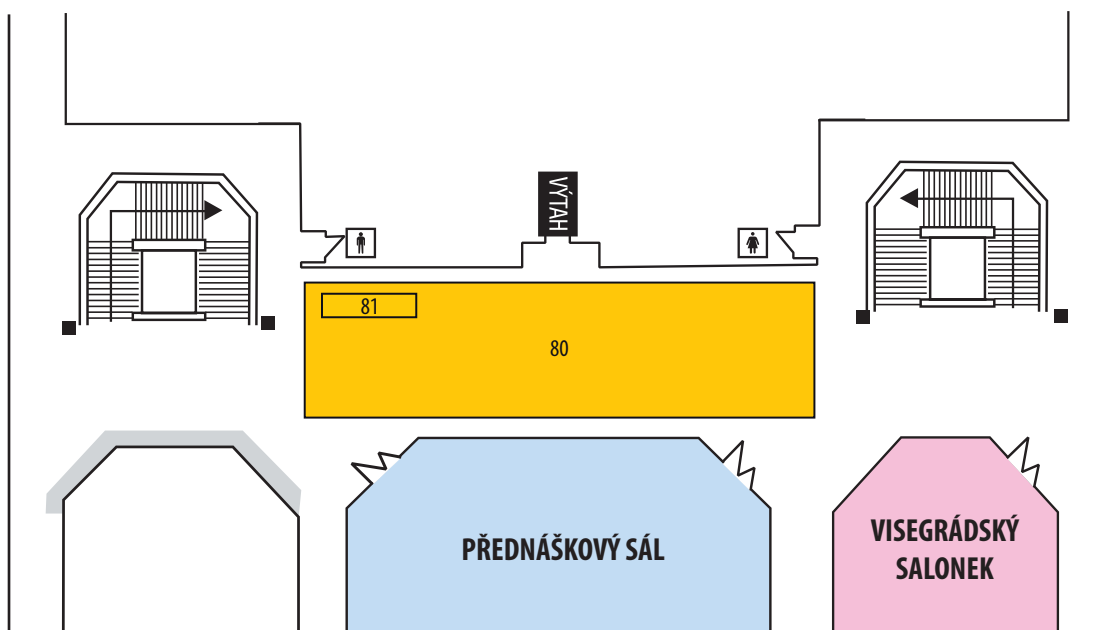


EXPOZICE	STÁNEK
ARCDATA PRAHA, s.r.o.	20
Asseco Central Europe, a. s.	10
AV MEDIA, a. s.	11
BiZZdesign Česká republika, s.r.o.	23
Citrix Systems Czech Republic s.r.o.	31
Corpus Solutions a.s.	30
Česká pošta, s. p.	17
Česká spořitelna, a. s.	26
Český úřad zeměměřický a katastrální	2
DIGIS, spol. s r. o.	16
GEOVAP, spol. s r.o.	9
GEPRO spol. s r.o.	3

EXPOZICE	STÁNEK
GORDIC spol. s r. o.	29
ICZ a.s.	25
IterSoft s.r.o. Choceň	13
Kraj Vysočina	33
MARBES CONSULTING s.r.o.	14
Microsoft s.r.o.	12
Ministerstvo pro místní rozvoj ČR	1
NEWTON Media, a.s.	34
OKsystem a.s.	27
QCM, s.r.o.	28
Software602 a.s.	7
Státní pokladna Centrum sdílených služeb, s. p.	32

EXPOZICE	STÁNEK
STÁTNÍ TISKÁRNA CENIN, státní podnik	5
STYRAX, a.s.	6
TRIADA, spol. s r. o.	39
T-MAPY spol. s r.o.	15
T-Mobile Czech Republic a.s.	4
Vema, a. s.	19
VITA software, s.r.o.	22
Vysoká škola CEVRO Institut, o.p.s.	21
Wolters Kluwer, a.s.	8
Zeměměřický úřad	2

2. PATRO



EXPOZICE	STÁNEK
Ministerstvo vnitra ČR	80
TyfloCentrum Brno, o. p. s.	81

Programový výbor a realizační tým konference ISSS/V4DIS 2015

Programový ředitel

Mgr. Vojtěch Dvořáček

Programový výbor

RNDr. Tomáš Renčín
Předseda programového výboru

Ing. Svatoslav Novák
ICT UNIE, o. s.

Ing. Petr Pavlinec
Krajský úřad kraje Vysočina

Ing. Ivo Bělonohý
*Sdružení tajemníků
městských a obecních úřadů*

Ing. Pavel Rous
Magistrát města Kladna

Ing. Cyril Čapka
Komise pro informatiku Svazu měst a obcí ČR

Realizační tým

RNDr. Tomáš Renčín
výkonný ředitel konference

Mgr. Vojtěch Dvořáček
programový ředitel konference

Marek Zubr
asistent

Blanka Brychtová
*manažer výstavních prostor,
organizační zajištění*

PhDr. Prokop Konopa
manažer komunikace

Kateřina Pánková
VIP prostory, redakce sborníku

Mgr. Jan Brychta
technické zabezpečení

Simona Češková
registrace účastníků, doprava

Ing. Arnošt Hanzl
organizační zajištění

Roman Falhar, DiS.
soutěže, PPT prezentace, ubytování

Ing. Petr Palisa
webmaster

JUDr. Ing. Antonín Eliáš
časopis Obec a finance

Sekretariát konference

U Svobodárny 1110/12, 190 00 Praha 9
tel.: +420 284 001 284, fax: +420 284 818 027
e-mail: sekretariat@issc.cz, www.issc.cz

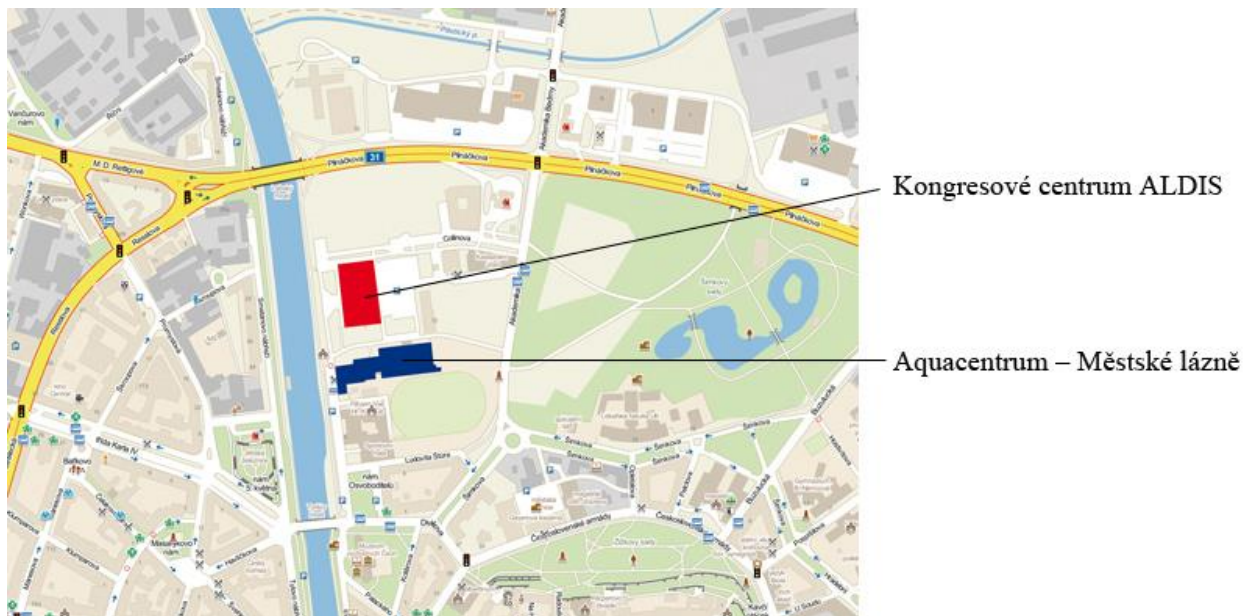
Informace pro účastníky konference

Místo konání konference

Kongresové centrum ALDIS

Eliščino nábřeží 375, 500 02 Hradec Králové

GPS souřadnice: 15,83272°, 50,21572



Městská hromadná doprava

- Pro účastníky konference je ve spolupráci s Dopravním podnikem města Hradec Králové zajištěna ZDARMA
- Účastníci se prokazují konferenční kartičkou, kterou obdrží při prezenci
- Nejblíže zastávka přímo před kongresovým centrem – Aldis
- Zastávky MHD do 500 m – Muzeum, Adalbertinum
- Pro více informací navštivte www.dpmhk.cz

Aquacentrum – Městské lázně

- Pro účastníky konference je jako možnost relaxace po náročném konferenčním programu zajištěno koupání v Městských lázních, které se nacházejí v těsném sousedství KC Aldis
- Účastníci se prokazují vstupenkou, kterou obdrží spolu se vstupenkou na konferenci
- Provozní doba:

neděle	12. 4. 2015	10.00–20.00 hod.
pondělí	13. 4. 2015	10.00–21.00 hod.
úterý	14. 4. 2015	10.00–21.00 hod.

Společenský večer – pondělí 13. dubna 2015

- Na závěr prvního konferenčního od 20 hodin tradičně připravujeme společenský večer v prostorách Velkého a Malého sálu KC ALDIS
- Vyhlášení soutěží Zlatý Erb, Biblioweb a Cena ministra vnitra
- Občerstvení formou rautu, hudba k poslechu i tanci

DOKUMENTY



TO JE NOVÝ MODEL OPTIMISTŮ. S VELKEJMA KAPSAMA NA PŘÍSPĚVKY, DÁVKY, PODPORY, DOTACE A JINOU FINANČNÍ POMOC OD STATU.

V4DIS 2015 – dvanáctý ročník

I v letošním roce se současně s ISSS uskuteční tradiční mezinárodní konference V4DIS (Visegrad Four for Developing Information Society). Setkání zástupců veřejné správy zemí Visegrádské čtyřky opět přivítá řadu významných hostů nejen z visegrádského regionu, ale i z dalších evropských zemí. Oficiální záštitu konferenci tradičně poskytuje místopředseda Senátu Parlamentu ČR Přemysl Sobotka. V současné době se jedná o účasti zástupce Evropské komise, jenž by navázal na vystoupení místopředsedkyně EK Neelie Kroes, která byla hostem posledního ročníku. Přítomni by měli být i oficiální koordinátoři e-governmentu (tzv. „digitální šampioni“) ze zemí V4 a řada tuzemských i zahraničních odborníků věnujících se problematice informatizace společnosti a reformě veřejné správy. Dvanáctý ročník V4DIS podpořil i Mezinárodní visegrádský fond a spoluorganizátorem setkání je opět Kraj Vysočina, který také v minulých letech vedl rozsáhlý projekt mapující stav informatizace veřejné správy v celém regionu – LDA V4.

Hlavními tématy konference bude hodnocení rozvoje e-governmentu v zemích Visegrádu, stejně jako informace o klíčových projektech, které se podařilo rozpracovat nebo dokončit. Jak se již stalo tradicí, značný prostor dostanou projekty z oblasti e-turismu, otázky týkající se dalšího rozvoje přeshraniční spolupráce, zkušenosti z implementace moderních technologií v širokém spektru oblastí souvisejících s veřejnou správou a ukázky příkladů dobré praxe.

Součástí programu konference V4DIS bude vedle tradičních doprovodných akcí konference ISSS i tradiční nedělní VIP večer v Klicperově divadle a slavnostní vyhlášení cen mezinárodní soutěže Eurocrest či ocenění účastníků soutěže mladých talentů JuniorErb, kteří jako obvykle obdrží i pamětní listy místopředsedy Senátu Parlamentu ČR.

Více informací: <http://www.v4dis.eu/>

Český zavináč 2015

V rámci programu slavnostního setkání v předvečer zahájení 18. ročníku konference ISSS v Hradci Králové budou jako obvykle v Klicperově divadle vyhlášeny výsledky soutěže Český zavináč.

„V rámci ocenění Český zavináč hodnotíme každoročně celou řadu různorodých osobností, projektů a aktivit,“ říká RNDr. Tomáš Renčín, ředitel konference ISSS a člen poroty sdružení Český zavináč. „S tím, jak informatizace veřejné správy a vlastně celé společnosti postupuje, je tento výběr stále složitější. Mezi nominovanými projekty a aktivitami se tentokrát objevily úplné novinky, ale také ohlédnutí k určitým milníkům rozvoje e-governmentu v minulosti.“

Soutěž se poprvé uskutečnila v roce **1999**. Prvním vítězem se stal tehdejší ministr spravedlnosti **Otakar Motejl**, a to za zpřístupnění Obchodního rejstříku (www.justice.cz) a za dlouhodobě otevřený přístup nositele tohoto ocenění k potřebám široké veřejnosti.

O rok později, v roce **2000**, zvítězila **Kancelář Poslanecké sněmovny Parlamentu ČR**. Porota ocenila společný projekt Parlamentní knihovny a odboru informatiky Kanceláře Poslanecké sněmovny Parlamentu ČR, nazvaný Digitální knihovna Český parlament (www.psp.cz/eknih). Digitální knihovnu tvoří archiv digitalizovaných tiskopisných zpráv z jednání našeho parlamentu od roku 1918 do současnosti.

Na třetím ročníku soutěže bylo Českým zavináčem **2001** oceněno **Ministerstvo vnitra České republiky** za projekty zaměřené na praktickou pomoc občanům. Projekty „Pátrání po vozidlech“, „Neplatné doklady“ a „Úřad není labyrint“ se setkaly s mimořádným ohlasem veřejnosti a mají dlouhodobě vysokou sledovanost.

V roce **2002** se laureátem stalo **Ministerstvo financí**. Porota tak podpořila nejen internetový „Registr plátců DPH“ a „Registr plátců spotřební daně“, ale také aktivitu a koncepčnost, s níž ministerstvo přistoupilo k řešení komplexního využití moderních technologií v oblasti daňové správy jako celku.

Držitelem Českého zavináče **2003** se stal bilaterální projekt „**Společná česko-slovenská digitální parlamentní knihovna**“. Jednalo se o zcela mimořádný počín v rozvoji informační společnosti v obou zemích, který znamenal průlom ve vzájemné informovanosti zákonodárných sborů a široké české a slovenské veřejnosti.

V roce **2004** si za nepřetržitou a bezplatnou službu „Nahlížení do katastru nemovitostí“ dostupnou všem uživatelům internetu, odnesl ocenění **Český úřad zeměměřický a katastrální**. Aplikace umožnila získávat některé vybrané údaje týkající se parcel a budov evidovaných v katastru nemovitostí, a dále pak informace o stavu jednotlivých řízení založených na příslušném katastrálním pracovišti, a to jak pro účely zápisu vlastnických a jiných práv, tak pro účely potvrzování geometrických plánů.

V roce **2005** se neudělovala hlavní cena, ale **dvě čestná uznání**, a to projektu **České spořitelny, a. s.**, – „Ověřování vlastnictví nemovitosti pomocí dálkového přístupu ke katastru nemovitostí pro potřeby posuzování hypotečních úvěrů“ a projektu **Úřadu MČ Praha 6** – „Ověřování vlastnictví nemovitosti pomocí dálkového přístupu ke katastru nemovitostí“.

V roce **2006** se držiteli ceny společně staly dva subjekty veřejné správy – „**Podvýbor pro informační systémy ve veřejné správě Výboru pro veřejnou správu, regionální rozvoj a životní prostředí Poslanecké sněmovny Parlamentu ČR**“ a „**Ministerstvo informatiky ČR**“, a to za úspěšné prosazení zásadního rozšíření okruhů míst, která jsou oprávněná k vydávání ověřených výpisů z úředních rejstříků a databází, do návrhu novely zákona o informačních systémech veřejné správy.

U příležitosti jubilejního desátého ročníku konference ISSS v roce **2007** získal prestižní ocenění prezident Nejvyššího kontrolního úřadu ČR **Ing. František Dohnal** za dlouholeté úsilí o rozvoj informační společnosti a významný podíl na elektronizaci veřejné správy na místní i regionální úrovni.

V roce **2008** vybrala porota jako vítěze novou službu **Dopravního podniku hl. m. Prahy** – možnost nákupu jízdenky prostřednictvím zaslání krátké textové zprávy z jakékoli stávající sítě GSM, která byla spuštěna v listopadu 2007.

V roce **2009** získaly toto prestižní ocenění dvě osobnosti, které se v posledních letech výrazným způsobem podílely na rozvoji informační společnosti v České republice – **Zdeněk Zajíček** (náměstek ministra vnitra ČR) a **Jaroslav Winter** (zakladatel sdružení BMI – Březen – měsíc internetu).

V roce **2010** bylo oceněno dlouhodobé úsilí **Kraje Vysočina** při rozvoji informatiky na úrovni kraje. Ocenění bylo předáno do rukou současného hejtmána MUDr. Jiřího Běhounka a jeho předchůdců na tomto postu Ing. Františka Dohnala a RNDr. Miloše Vystrčila.

V roce **2011** porota udělila cenu oblíbené celostátní soutěži o nejlepší webové stránky měst a obcí „**Zlatý erb**“, která byla podle slov odborné poroty v minulých letech nesmírně důležitá pro zprůhlednění procesů probíhajících na úřadech měst a obcí. Přispěla zásadním způsobem k prosazení webových stránek jako důležitého informačního kanálu a rovněž k posunu vnímání webů obcí a měst od pouhé prezentace k efektivní komunikaci s občany.

V roce **2012** byl Českým zavináčem oceněn **Ondřej Felix**, a to za zásadní přínos pro elektronizaci veřejné správy v ČR, který sehrál v roli hlavního architekta e-governmentu, a za dotažení řady klíčových projektů do fáze konečné realizace.

V roce **2013** získala tradiční cenu **ICT Unie**. Porota ocenila především celkový přínos k dalšímu rozvoji informatizace veřejné správy a trvalé úsilí o smysluplný dialog mezi světem ICT a veřejnou sférou přinášející benefity celé společnosti.

V roce **2014** porota ocenila velice potřebnou osvětovou činnost v oblasti internetu a elektronických služeb a rozhodla se udělit cenu sdružení **CZ.NIC**. Při rozhodování přihlédla i k dalším aktivitám sdružení, které přispívají k rozvoji informační společnosti, jako jsou podpora open-source projektů, provoz národního bezpečnostního týmu CSIRT.CZ či implementace nových technologií (IPv6, DNSSEC).

Více informací včetně kompletního archivu minulých ročníků lze najít na www.issc.cz.

17. ročník soutěže Zlatý erb

Města a obce České republiky mají i v roce 2015 možnost zúčastnit se klání o nejlepší oficiální internetové stránky a elektronickou službu.

Stejně jako v předchozích letech probíhá soutěž i letos dvoustupňově, tj. nejprve se uskuteční krajská kola pod patronací jednotlivých krajských úřadů, ze kterých poté vzejdou soutěžící kola celostátního. To vyvrcholí slavnostním předáním cen na konferenci ISSS v pondělí 13. dubna v rámci programu společenského gala-večera v Hradci Králové.

Některé kraje přichystaly v rámci svého kola specifické kategorie – například Kraj Vysočina a Jihomoravský kraj oceňuje nejlepší webové stránky dobrovolných hasičů, Kraj Vysočina navíc také nejlepší weby školských zařízení.

Zlatý erb již tradičně poutá pozornost měst, obcí a veřejnosti. Soutěž byla založena v roce 1999 jako nástroj pro podporu modernizace místních samospráv. V roce 2002 byla oceněna jako finalista světové prestižní ceny Stockholm Challenge Award a v roce 2011 zvítězila v soutěži Český zavináč.

Přihlášení pro města a obce probíhá prostřednictvím stránek <http://www.zlatyerb.cz>. Krajská kola byla zahájena 2. února a jejich vítězové byly vyhlášeni na slavnostních ceremoniálech v březnu letošního roku.

Více informací: <http://zlatyerb.obce.cz/>

Rok průmyslu a technického vzdělávání 2015

David Vondrák, koordinátor kampaně „Rok průmyslu a technického vzdělávání 2015“

Rok 2015 byl Svazem průmyslu a dopravy ČR a dalšími partnerskými organizacemi vyhlášen Rokem průmyslu a technického vzdělávání. Jde o celonárodní kampaň propagující novou, moderní podobu průmyslu 21. století a rozmanitost, inovativnost a společenskou odpovědnost současných průmyslových oborů. Současně si klade za úkol vyzdvihnout důležitost a nepostradatelnost kvalitního technického vzdělávání jak pro budoucnost průmyslu v ČR, tak i pro osobní perspektivu jednotlivců. Nedílnou součástí kampaně jsou návrhy systémových změn v oblasti vzdělávání, tak aby působily ve prospěch zvyšování zaměstnanosti v průmyslových odvětvích.



ROK PRŮMYSLU
A TECHNICKÉHO
VZDĚLÁVÁNÍ

Absolutní většina naší veřejnosti si uvědomuje význam tuzemského průmyslu, který zaměstnává téměř 30 procent lidí, a hodnotí ho pozitivně. Přesto u běžné populace přetrvává jeho tradiční a zastaralé vnímání, což je jedním z faktorů nižšího zájmu žáků a studentů a jejich rodičů o technické obory. Změnit postupně pohled na průmysl jako na moderní součást ekonomiky, zvýšit zájem o technické obory a upravit systém vzdělávání právě k podpoře technických oborů je společným zájmem Svazu průmyslu a dopravy ČR (SP ČR) a dalších zaměstnavatelských a podnikatelských svazů a asociací a tuzemských firem a také vlády a ministerstev jako jsou MŠMT, MPO a MPSV, škol i dalších institucí. Pomoci naplnit tyto záměry by měl probíhající Rok průmyslu a technického vzdělávání, který Svaz průmyslu a dopravy ČR se svými partnery pro letošní rok vyhlásil. Generálním partnerem kampaně je Česká spořitelna, a.s.

Hlavním záměrem Roku průmyslu a technického vzdělávání 2015 je vedle zvýšení zájmu veřejnosti o průmysl a o technické obory a prosazení koncepčních a systémových změn v oblasti vzdělávání také zvýšení zájmu škol i firem o spolupráci a přiblížení dobrých příkladů z praxe. Rok průmyslu a technického vzdělávání 2015 je celoroční kampaň složená z řady aktivit a různých akcí, které jsou reakcí na požadavek podnikatelské sféry důrazněji poukázat na jeden z klíčových problémů konkurenceschopnosti ČR. Tím je disproporce mezi vysokou mírou nezaměstnanosti a dlouhodobě neuspokojenou poptávkou firem po mnoha desítkách tisíc technicky vzdělaných pracovníků, které český vzdělávací systém zaměstnavatelům nenabízí.

Svaz průmyslu a dopravy ČR chce prostřednictvím aktivit Roku průmyslu a technického vzdělávání postupně začít měnit pohled veřejnosti a ukázat, že průmysl je moderní současnost a budoucnost nabízející dobré pracovní perspektivy. Přitom kvalita a vysoká technologická úroveň průmyslových firem patří mezi hlavní přednosti ČR v rámci globální konkurenceschopnosti. Současně chce SP ČR společně se svými členskými svazy a asociacemi i individuálními členskými firmami více poukazovat na klíčové problémy v oblasti technického vzdělávání a potřebu optimalizovat soustavu oborů a škol ve vazbě na predikce trhu práce. V České republice dochází od roku 1994 k demografickému poklesu a tento fakt regresivní vlny se přelévá do středních škol. Kvůli zavedení víceletých gymnázií došlo k poklesu zájmu o vzdělávání na průmyslových školách. Navíc kvalita obecného vzdělávání opadá. Tento stav je zapotřebí řešit. Je třeba preferovat technické a polytechnické vzdělávání na všech stupních. Řešením nesouladu mezi oborovou nabídkou škol a potřebami zaměstnavatelů je zavedení predikčního systému krátkodobých potřeb regionálního trhu práce, garantovaného MŠMT a MPSV.

SP ČR dlouhodobě prosazuje posilování prvků polytechnické výchovy v mateřských a základních školách a obnovení povinných dílen na 2. stupni základních škol a praktické výuky v reálném pracovním prostředí. Vedle toho SP ČR prosadil zavedení povinné matematiky při státních maturitách a je připraven spolupracovat na zavedení mistrovské zkoušky pro absolventy učebních oborů.

Rovněž systém duálního vzdělávání by byl logickým návratem k systému, který zde fungoval po řadu let, ale bohužel byl za posledních dvacet let opuštěn. Je potřeba tento návrh modifikovat tak, aby odpovídal realitě 21. století v kontextu globalizovaného světa. Odborná příprava žáků by v maximální možné míře měla probíhat na reálných pracovištích. Zaměstnavatele je k tomu třeba motivovat, a to i jinými způsoby, než jen daňovými odpočty. Tato a další témata chce SP ČR v průběhu roku komunikovat na konferencích, při diskusních setkáních, kulatých stolech apod. a medializovat je.

Kampaň se opírá o několik pátečních aktivit zaměřených především na rodiče a mladé lidi. V průběhu celého roku bude SP ČR zviditelňovat spolupráci firem a podniků se školami na nejrozličnějších úrovních. Pod hlavičkou kampaně budou realizovány rozmanité akce a činnosti: například dny otevřených dveří ve školách, exkurze ve firmách, vědomostní soutěže pro žáky a studenty, projekty vzdělávání učitelů odborných vyučovacích předmětů a praktického vyučování ve firmách a na pracovištích reálné praxe. Vedle online kampaně probíhající i na sociálních sítích, vyhlášení studentských soutěží, vydávání publikací jako Almanach technického vzdělávání či statistický přehled Panorama průmyslu se počítá například i s většími akcemi pro veřejnost jako je Den průmyslu v Ostravě. Připraveny jsou rovněž tematicky související konference, semináře a workshopy, diskusní kulaté stoly, motivační akce pro rodiče s dětmi či popularizační pořady o průmyslu a technických oborech v Českém rozhlase a v České televizi. Webová stránka **www.rokprumyslu.eu**, jejíž ambicí je, stát se interaktivním centrálním místem shrnujícím již existující a fungující aktivity podpory technického vzdělávání a spolupráce mezi průmyslem a školami umožňuje registraci pro účast v kampani pro další zájemce.

Svaz průmyslu a dopravy ČR je největším zaměstnavatelským svazem v zemi. Posláním této dobrovolné, nestátní organizace, nezávislé na vládě, politických stranách a odborech, je ovlivňovat hospodářskou a sociální politiku vlády a působit na vytváření optimálních podmínek pro podnikání. Hájí zájmy zaměstnavatelů v evropských a mezinárodních organizacích, zejména jako člen vlivného evropského svazu zaměstnavatelů BusinessEurope.

Chcete se pochlubit svými úspěchy při zavádění inovací? Vadí vám nedostatek technicky vzdělaných pracovníků? Omezuje to vaši výrobu a plány? Chcete navázat spolupráci se školami nebo naopak již máte kvalitní platformy či projekty spolupráce a chcete o nich dát vědět?

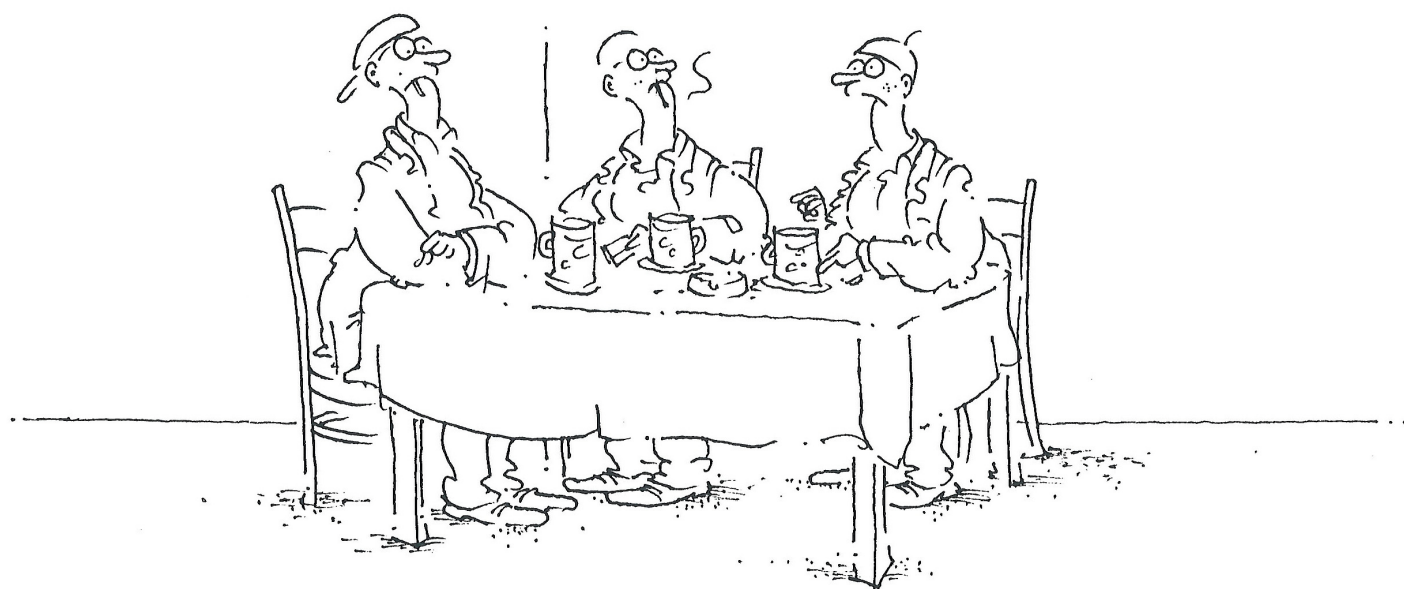
Zapojte se do „Roku průmyslu a technického vzdělávání 2015“ – společné snahy, která chce propojit vaše aktivity a zviditelnit je!

Vaše přihlášení do kampaně Rokem průmyslu a technického vzdělávání můžete realizovat prostřednictvím registračního formuláře na stránkách **www.rokprumyslu.eu**, prostřednictvím emailové adresy **rokprumyslu@sPCR.cz**, případně přímo na tel: 225 279 504 nebo adrese **dvondrak@sPCR.cz**.



Svaz průmyslu a dopravy ČR

PŘEDNÁŠKY



HELE NERAD, NEBYLS V BRUSELU!

Nařízení eIDAS – co se aktuálně připravuje

Filip Bílek, odbor eGovernmentu, Ministerstvo vnitra ČR

1. Úvodem

Pro zachování kontinuity považujeme za vhodné zrekapitulovat ve stručnosti dosavadní průběh týkající se nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále jen „nařízení eIDAS“). Návrh nařízení eIDAS vydala Evropská Komise dne 4. června 2012. Tento návrh patří, jakožto jedno z klíčových opatření Aktu o jednotném trhu (KOM(2011)206), mezi nejvýznamnější iniciativy v oblasti budování jednotného digitálního trhu a má za cíl zvýšit důvěryhodnost elektronických transakcí v rámci vnitřního trhu EU. Evropská Komise zde navazuje na úkoly vytyčené v Digitální agendě pro Evropu (KOM(2010)245). Pracovní skupina Rady (EU) pro telekomunikace a informační společnost tento návrh nařízení opakovaně projednávala v průběhu roků 2012 až 2014, přičemž předmětem diskuzí se postupně staly všechny části návrhu. Dne 28. srpna 2014 bylo nařízení eIDAS publikováno v Úředním věstníku EU a vstoupilo v platnost 17. září letošního roku.

Konečné znění oficiálního českého překladu nařízení eIDAS je k dispozici na stránkách Úředního věstníku EU (na stránce si lze zvolit konkrétní jazyk):

[http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG¹](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG<sup>1</sup)

Nařízení bude použitelné od 1. července 2016 s tím, že jednotlivá ustanovení budou, s ohledem na nutnost předložení souvisejících prováděcích aktů a na potřebu přizpůsobení členských států, nabývat účinnosti postupně v období let 2016 – 2018. Povinné uznávání prostředků pro elektronickou identifikaci by mělo nastat cca od září roku 2018 (na základě termínu přijetí určitých prováděcích aktů do 18. září 2015 plus 3 roky).

2. Co se připravuje na úrovni EU

V dubnu minulého roku byla Evropskou Komisí (dále jen „EK“) založena **expertní skupina eIDAS**, která má za úkol pomoci EK zejména při navrhování prováděcích aktů, jež mají zajistit splnění požadavků stanovených v nařízení eIDAS. Mezi další úkoly této skupiny patří výměna tzv. „best-practise“ mezi členskými státy a koordinace spolupráce členských států. Na této skupině se projednávají hlavní oblasti nařízení eIDAS, které vyžadují vytvoření prováděcích aktů (oblast elektronické identifikace plus oblast služeb vytvářejících důvěru). Nařízení eIDAS stanovuje pro přijetí některých prováděcích aktů i pevně dané termíny. To se týká zejména oblasti elektronické identifikace, kde vesměs všechny prováděcí akty mají pevně stanovené termíny přijetí EK. Příkladem lze uvést prováděcí akt dle čl. 8 odst. 3 nařízení eIDAS, který stanoví specifikace, normy a postupy pro úroveň záruk prostředků pro elektronickou identifikaci. Z oblasti služeb vytvářejících důvěru má například stanoven termín prováděcí akt, kterým se stanoví referenční formáty zaručených elektronických podpisů a pečeti – viz čl. 27 a 37 odst. 5.

Dle čl. 48 nařízení eIDAS byl založen výbor², ve kterém EK žádá členské státy o stanoviska k návrhům prováděcích aktů. Na základě získaného stanoviska je možné návrh implementačního aktu přijmout. Tato procedura již úspěšně proběhla u prvního prováděcího aktu, pro který je EK zmocněna na základě čl. 12 odst. 7 nařízení eIDAS (termín stanoven do 18. března 2015). Prováděcí akt byl zveřejněn v Úředním věstní-

¹ Ke zveřejněnému oficiálnímu překladu nařízení eIDAS bylo vydáno CORRIGENDUM vzhledem k chybně uvedenému datu ve článku 12 odstavci 8. Zmíněné CORRIGENDUM lze nalézt na stránce: <http://data.consilium.europa.eu/doc/document/ST-14750-2014-INIT/en/pdf>

² Tento výbor je výborem ve smyslu [nařízení Evropského parlamentu a Rady \(EU\) č. 182/2011 ze dne 16. února 2011](#), kterým se stanoví pravidla a obecné zásady způsobu, jakým členské státy kontrolují Komisi při výkonu prováděcích pravomocí.

ku EU na adrese: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=OJ:JOL_2015_053_R_0006 a jedná se o 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.

Pro účely spolupráce členských států má každý členský stát určit tzv. „jednotné kontaktní místo“. Seznam jednotných kontaktních míst bude zveřejněn EK. Spoluprací se myslí hlavně vyměňování zkušeností, osvědčených postupů v oblasti systémů elektronické identifikace a dále také v případě, kdy členský stát požaduje dodatečné informace o systému elektronické identifikace jiného členského státu. Dalším důležitým prvkem, který má přispět k budování důvěry v oblasti elektronické identifikace mezi členskými státy, je proces vzájemného hodnocení, jež je zmíněn ve čl. 12 odst. 6 písm. c) nařízení eIDAS a jehož účelem je přezkoumat interoperabilitu a bezpečnost systémů elektronické identifikace. Nejméně šest měsíců před plánovaným oznámením systému elektronické identifikace oznamující stát poskytne ostatním členským státům popis systému elektronické identifikace, který hodlá oznámit. Tento systém by měl být následně podroben procesu vzájemného hodnocení, který spočívá v tom, že ostatní členské státy tzv. hodnotitelé, kteří se dobrovolně přihlásí, přezkoumají, jakým způsobem dotýčný systém elektronické identifikace splňuje požadavky nařízení eIDAS, zejména co se týče interoperability systému elektronické identifikace, a také uváděnou úroveň záruky prostředků pro elektronickou identifikaci vydaných v rámci tohoto systému. Proces vzájemného hodnocení může zahrnovat například posouzení relevantní dokumentace vztahující se k systému elektronické identifikace, dále přezkum procesů, zohlednění posudku nezávislé strany, seminářů apod. Velký důraz bude zřejmě kladen na kontrolu, zda systém elektronické identifikace, jež je předmětem procesu vzájemného hodnocení, splňuje požadavky na danou úroveň záruky.

Skupina hodnotitelů pak následně do jednoho měsíce od skončení procesu vzájemného hodnocení předloží svoje závěry formou vyhotovené zprávy prostřednictvím sítě pro spolupráci („cooperation network“). Jedním z úkolů sítě pro spolupráci je přezkum výsledků vzájemného hodnocení, které by měla dodat síti skupina hodnotitelů³. Síť pro spolupráci bude založena prostřednictvím tohoto prováděcího rozhodnutí. V případě, že výsledek hodnocení systému elektronické identifikace bude negativní, oznamující členský stát by měl svoje rozhodnutí oznámit systém elektronické identifikace vzít zpět a provést úpravy tohoto systému tak, aby vyhovoval požadavkům na interoperabilitu a příslušnou úroveň záruky.

Dalšími prováděcími akty, které se aktuálně projednávají na expertní skupině, jsou všechny, které mají specifikován pevný termín přijetí:

- Prováděcí akt pro značku důvěry EU pro kvalifikované služby vytvářející důvěru (čl. 23 nařízení eIDAS) – byla vypsána soutěž na grafickou podobu značky, viz internetové stránky: <https://ec.europa.eu/digital-agenda/en/news/e-mark-u-trust-competition-first-results-public-online-voting>. Nejpozdější termín pro přijetí prováděcího aktu je **1. července 2015**.
- Prováděcí akt pro důvěryhodné seznamy (čl. 22 nařízení eIDAS). Prováděcí akt stanoví technické specifikace a formáty pro důvěryhodné seznamy, které mají povinně obsahovat informace o kvalifikovaných poskytovatelích služeb vytvářejících důvěru a o samotných kvalifikovaných službách vytvářejících důvěru, které poskytují. Nejpozdější termín pro přijetí prováděcího aktu je **18. září 2015**.
- Prováděcí akt stanovující referenční formáty zaručených elektronických podpisů a pečeti nebo referenční metody, jsou-li používány alternativní formáty (čl. 27 a 37 nařízení eIDAS). Tento prováděcí akt by měl být zejména založen na již existujícím prováděcím rozhodnutí Komise č. 2014/148/EU, kterým se mění rozhodnutí 2011/130/EU, kterým se stanoví minimální požadavky na přeshraniční zpracování dokumentů elektronicky podepsaných příslušnými orgány podle směrnice 2006/123/ES

³ Systém elektronické identifikace nemůže být předmětem dalšího vzájemného hodnocení po dobu dvou let od uzavření vzájemného hodnocení, pokud k tomu nedá souhlas síť pro spolupráci.

Evropského parlamentu a Rady o službách na vnitřním trhu. Nejpozdější termín pro přijetí prováděcího aktu je **18. září 2015**.

- Prováděcí akt pro rámec interoperability (čl. 12 nařízení eIDAS), který se sestává například z odkazu na minimální technické požadavky týkající se úrovně záruk, odkazu na minimální technické požadavky potřebné pro interoperabilitu, odkazu na minimální soubor osobních identifikačních údajů jednoznačně identifikující fyzickou či právnickou osobu a dalších. Tento prováděcí akt bude spolu s prováděcím aktem pro úroveň záruk stěžejní v oblasti elektronické identifikace. Nejpozdější termín pro přijetí prováděcího aktu je **18. září 2015**.
- Prováděcí akt, s jehož pomocí budou vymezeny tři úrovně záruk prostředků pro elektronickou identifikaci (čl. 8 nařízení eIDAS). Nařízení eIDAS rozeznává tři úrovně záruky: nízká, značná a vysoká. Prováděcí akt by měl stanovit pro všechny úrovně záruky pravidla, která je třeba aplikovat například při procesu kontroly totožnosti osoby před vydáním prostředku pro elektronickou identifikaci. Nejpozdější termín pro přijetí prováděcího aktu **18. září 2015**.

Prováděcí akt stanovující postup a okolnosti oznamování systému elektronické identifikace (čl. 9 nařízení eIDAS) nemá stanoven pevný termín přijetí, nicméně je nutné stanovit pravidla a postupy oznámení a také detailní určení informací, které je třeba předat EK, aby mohl být systém elektronické identifikace úspěšně oznámen. EK má za povinnost oznámené systémy elektronické identifikace zveřejnit v Úředním věstníku EU.

Při tvorbě prováděcích aktů z oblasti elektronické identifikace by měla EK také zohlednit zkušenosti a osvědčené postupy jednoho z pilotních projektů velkého rozsahu⁴ STORK 2.0 (Secure idenTity acrOss boRders linKed 2.0) <https://www.eid-stork2.eu/>. V rámci projektu STORK 2.0 zúčastněné státy na několika pilotních scénářích ověřují výhody použití přeshraniční elektronické identity v konkrétních individualizovaných přeshraničních elektronických službách. Více informací o jednotlivých pilotech lze nalézt na stránkách https://www.eid-stork2.eu/index.php?option=com_content&view=article&id=406&Itemid=112.

3. Srovnání několika aspektů ZoEP a nařízení eIDAS

Při srovnání našeho zákona č. 227/2000 Sb., o elektronickém podpisu (ZoEP) a nařízení eIDAS vyplývá, že největší změnou v oblasti elektronického podpisu, čistě z pohledu uživatele využívajícího elektronické podepisování, bude nutnost používání kvalifikovaného prostředku pro vytváření elektronického podpisu v případě, že uživatel chce zajistit, aby jím vytvořený elektronický podpis byl uznatelný i za hranicemi ČR. Pokud bude zaručený elektronický podpis založen na kvalifikovaném certifikátu (dnešní náš uznávaný elektronický podpis) a bude vytvořen pomocí kvalifikovaného prostředku pro vytváření elektronického podpisu (tj. soukromý klíč bude uložen na bezpečném prostředku, ze kterého nebude možné tajný klíč extrahovat, bude chráněn proti zneužití třetí osobou – např. pomocí PIN atd.), bude mít takový kvalifikovaný elektronický podpis stejné právní účinky, jako vlastnoruční podpis, a to v celé EU. Při kontrole platnosti elektronického podpisu tedy bude nutno zjišťovat i to, zda soukromý klíč, který odpovídá veřejnému klíči v certifikátu, je uložen v kvalifikovaném prostředku pro vytváření elektronického podpisu. Tato informace by měla být uvedena v samotném certifikátu (i teď lze v některých certifikátech nalézt informaci o tom, že soukromý klíč je uložen na bezpečném prostředku – SSCD – Secure Signature Creation Device). Již mnoho členských států EU má ve svých právních řádech stanovenou povinnost používat bezpečné prostředky pro tvorbu elektronických podpisů, v České republice tato povinnost doposud nebyla stanovena. Nutno také uvést, že nařízení eIDAS službu ověřování platnosti elektronických podpisů/pečetí řadí mezi služby vytvářející důvěru.

Jednou z největších výzev pro spoléhající se strany bude zřejmě vypořádání se situacemi, kdy obdrží elektronický dokument, který je podepsán kvalifikovaným elektronickým podpisem, a který je založen na kvalifikovaném certifikátu, jež byl vystaven v jiném členském státě EU a neobsahuje jednoznačný identifika-

⁴ LSP – large scale project

tor osoby známý pro spoléhající se stranu. Spoléhající se strany často tento jedinečný identifikátor využívají pro jednoznačnou identifikaci osoby. Pro jednoznačnou identifikaci osoby bude sloužit elektronická identifikace, kdy pomocí jedinečných osobních identifikačních údajů bude možné jednoznačně identifikovat danou osobu. Nařízení eIDAS sice přiznává možnost uvádět další atributy v certifikátech, ale za podmínky, že tyto atributy nejsou povinné a nesmí být jimi porušena interoperabilita a uznávání kvalifikovaných elektronických podpisů. Zároveň ve čl. 28 stanovuje, že kvalifikované certifikáty nepodléhají žádným závazným požadavkům, které přesahují požadavky přílohy I. nařízení eIDAS – v kvalifikovaném certifikátu pro elektronické podpisy musí být uvedeno alespoň jméno podepisující osoby nebo pseudonym. Spoléhající se strany rovněž budou muset počítat se skutečností, že kvalifikovaný poskytovatel služeb vytvářejících důvěru bude mít k dispozici časovou lhůtu pro zneplatnění certifikátu až 24 hodin (do 24 hodin od obdržení žádosti o zneplatnění musí kvalifikovaný poskytovatel služeb vytvářejících důvěru vydávající kvalifikované certifikáty toto zneplatnění zveřejnit).

Nařízení eIDAS zavádí na úrovni EU nový pojem – elektronická pečeť. Elektronická pečeť tak, jak je definována v nařízení, není 100 % identická s naší elektronickou značkou. Jedním z důvodů je, že certifikát pro elektronickou pečeť lze vydat pouze právnické osobě (viz definice 24 pečeti osoby). V tomto ohledu nařízení eIDAS jasně vymezuje rozdíl mezi fyzickou a právnickou osobou, kdy fyzická osoba se může elektronicky podepisovat a právnická osoba může elektronicky pečet. Elektronická pečeť není elektronický podpis pro právnické osoby, jejím účelem je prokázání původu a integrity dat, se kterými je spojena (viz definice 25 elektronické pečeti). V ideálním případě by tedy důvěryhodný elektronický dokument pocházející od právnické osoby mohl obsahovat jednak elektronický podpis fyzické osoby oprávněné jednat v konkrétním případě, dále elektronickou pečeť právnické osoby a elektronické časové razítko poskytující důkaz o existenci dokumentu v čase.

Nařízení eIDAS znamená značný posun dopředu k dosažení jednotného digitálního trhu, nicméně také znamená nutnost přizpůsobení nejenom právních ráďů jednotlivých členských států. Toto přizpůsobení nebude jistě jednoduché a MV si je vědomo tohoto závazku. Z tohoto důvodu vzniká na MV projektová struktura a v rámci ní pracovní skupiny, které mají za úkol provést analýzu a návrh úprav tak, aby byl dosažen soulad s nařízením eIDAS.

Administrativní audit je příspěvkem k vyšší efektivitě i bezpečnosti

Ing. Miroslav Čejka, vedoucí týmu Spisové služby GORDIC spol. s r. o.

Proč se některé dokumenty vyřizují déle než jiné? Pracuje naše organizace efektivně? Nemáme kostlivce ve skříni? Odpověď na tyto otázky není tak složitá, jak by se mohlo zdát. Všechny potřebné informace již organizace zpravidla má. Teď již stačí se na ně jen správně podívat.

DRMS systémy výrazně posunuly původní historické hranice spisové služby, která byla jen prostým evidenčním nástrojem, do digitální reality, mnohdy ještě neprobádané. Jedná se o jednu z nejbouřlivěji se rozvíjejících oblastí současného světa, i když tak trochu schovanou před zraky veřejnosti i médií. DRMS se tedy stará o správu dokumentů a záznamů a schraňuje informace o pohybech dokumentů. Řeší také dodržování zákonných i interních lhůt, činnosti jednotlivých osob a jejich vytížení, způsoby zabezpečení dokumentů proti neoprávněným přístupům, bezpečnostní incidenty, atp. Zaznamenané údaje jsou dostatečně zajímavé na to, aby nezůstaly jen tak ležet bez využití.

Evidujeme skutečně potřebné informace

I proto je tu Administrativní audit. Představuje informační nástroj pro zvýšení efektivního fungování organizace s využitím reálných dat, která není nutné pracně a nákladně pořizovat, protože zatím poměrně nečinně ležela na vašich serverech. Jsou to vaše data z reálného provozu, tedy zcela zdarma a navíc přesně popisující realitu běžného dne.

Jedná se například o možnost statistického vyhodnocení skutečných toků dokumentů přes konkrétní osoby a organizační jednotky. Výběrem požadovaných dokumentů, např. podle typu dokumentu, klíčových slov či filtrováním podle odesílatele zjistíte skutečné toky v organizaci, včetně doby vyřizování na jednotlivých „uzlech“.

Tím možnosti Administrativního auditu zdaleka nekončí. Postupným rozklikáváním se můžeme dostat až na detailní informace o čase stráveném jednotlivými osobami nad konkrétním dokumentem. A třeba i odhalovat anomálie, odchylky od obvyklého či požadovaného pohybu dokumentu či ke zjištění, že dokument byl vyřizován nestandardním způsobem.

Vizualizací oběhu určitých typů dokumentů na pozadí organizační struktury organizace lze přehledně identifikovat například nestandardní oběh určitých faktur během jejich schvalování. Anebo naopak, i přestože dokumenty putují správně po nastavené trase, je jejich pohyb zásadně brzděn některými přetíženými místy, zatímco jiné paralelní trasy jsou nevyužité.

Vyšší efektivita, ale i bezpečnost

Nesmíme zapomenout na to, že kybernetická bezpečnost se stává novou, rodící se oblastí, která nutně postupně přejde do každodenního slovníku každé organizace. Správné nastavení a zejména udržení kybernetické bezpečnosti (a to nejen kvůli nové legislativě) začne hrát dominantní roli pro „sebezáchovu“ každé organizace i celého státu. I do této oblasti poměrně razantním způsobem zasahuje Administrativní audit. Identifikace nestandardních stavů a bezpečnostních hrozeb, které také přináší, se stane nepostradatelným nástrojem pro analýzu úrovně kybernetické bezpečnosti organizace a podkladem pro její udržování a průběžné vyhodnocování.

Administrativní audit v podobě softwarového nástroje může být už dnes integrální součástí informačního systému. Pokud používáte ke své práci systém GINIS, můžete pracovat s Administrativním auditem nad svými online daty. Nepotřebuje tedy žádnou další investici do integračních rozhraní či datových extraktů z jiných systémů, ani není nutné data přelévat do jiných databází či datových skladů.

V každé době, zejména pak v dnešní době digitální platí, že organizace je natolik efektivní, nakolik efektivně dokáže zvládnout toky svých informací. Přínos řešení Administrativního auditu je tedy tak velký, nakolik si ceníte efektivního a bezpečného fungování své organizace.

Fujitsu, místo plastu lidská dlaň

Martin Černý, Senior project manager, Fujitsu Technology Solutions s.r.o.

Bezpečnost je dnes jedním z hlavních témat, o nichž diskutuje naše společnost. Zhoršující se situace v Evropě nutí soukromou i veřejnou sféru přemýšlet nad jednoduchým a účinným řešením, které by dokázalo s jistotou poskytnout přístup jen oprávněným osobám. Je vcelku jedno, jestli jde o obranu proti nebezpečí terorismu, průmyslové špionáži, nebo jen ochranu vlastního domu. Někdy se stává, že nejméně zabezpečeným článkem Vaší rodiny jsou děti, zapomínají klíče, snáze je někdo požádá o pomoc, jsou prostě bezstarostné a důvěřivé.

Biometrické zabezpečení na bázi PalmSecure podobné problémy efektivně vyřeší. Díky nové technologii, která dokáže rozpoznat jedinečný obrazec krevního řečiště dlaně ruky jednotlivce, je nyní možné jednoznačně a mnohem bezpečněji ověřovat totožnost člověka při vstupu do zaměstnání, přímo u jeho počítače, nebo třeba při odemykání domovních dveří. Ověření probíhá během několika vteřin, bezkontaktně, pouhým přidržetím ruky nad snímačem.

Obraz cév je u každé osoby jedinečný a jeho podrobnou strukturu lze použít k vytvoření jedinečného biometrického identifikátoru. Bezdotykové ověření je hygienické a neinvazivní, takže má oproti ostatním biometrickým metodám mnoho výhod. Není nutné nikam přikládat bradu, znovu a znovu nastavovat snímač, nebo řešit například narušení struktury otisku prstu. Krevní řečiště v dlani je totiž od určitého věku neměnné a stačí tak jedno sejmутí obrazu.

Vyspělý ověřovací algoritmus zajišťuje vysokou přesnost a všestranné využití. Prolomení tohoto algoritmu je téměř nemožné, což umožňuje vysokou úroveň zabezpečení. Technologie je založená na více než dvou desetiletích zkušeností společnosti Fujitsu s rozpoznáváním obrazu krevního řečiště.

Zařízení pro vytváření obrazu dlaňových cév od Fujitsu představuje ověřovací systém, který využívá nejnovější poznatky biometrických technologií a jejich zabezpečení. Reaguje na celosvětovou poptávku vlád i soukromého sektoru.

Nový systém pro vytváření obrazu cév společnosti Fujitsu pracuje na principu zachycení obrazu dlaňových cév pomocí infračervených paprsků. Odkysličený hemoglobin v dlaňových cévách tyto paprsky pohlcuje, čímž snižuje jejich odrážení. Zobrazené cévy tak vytvoří černý vzor. Aby bylo možné potvrdit totožnost jedince, je tento obraz cév porovnán s již dříve registrovaným vzorem.

Protože jsou cévy uloženy uvnitř těla a mají velké množství znaků, podle kterých je lze rozlišit, je téměř vyloučené zfalšovat totožnost jedince. To představuje velmi vysokou úroveň zabezpečení. Snímač navíc dokáže rozeznat vzorec jen v případě, kdy odkysličený hemoglobin cévami aktivně proudí. Nemůžou tak fungovat některé scénáře, jako z amerických filmů, kdy by se někdo snažil o prolomení zabezpečení instituce pomocí useknuté ruky.

Technologii PalmSecure je možné nasadit v nejrůznějších oblastech včetně bezpečnostních služeb, finančních a bankovních služeb, zdravotnictví, komerčních společností i vzdělávacích zařízení. PalmSecure lze využít k povolení vstupu do zabezpečených prostor, přihlášení do počítačů nebo serverových systémů, přístupu k prodejním místům, bankomatům nebo kioskům, ověřování identifikace a dalším činnostem v závislosti na odvětví.

Jednou ze zajímavých novinek na bázi PalmSecure je software PalmSecure OmniPass, který poskytuje nejlepší řešení ve své třídě pro přihlášení zabezpečení, řízení přístupu a ochrany dat pro podnikovou sféru. PalmSecure OmniPass Client Edition je navržen tak, aby poskytoval vysoce přesné a neinvazivní řešení biometrické autentizace, Client Edition nabízí snadný způsob, k ověření totožnosti uživatele, zajištění ochrany dat před nepovolanými osobami.

V Single Sign-On (SSO) softwarovém řešení lze zvýšit produktivitu koncových uživatelů tím, že je eliminována zdlouhavá správa hesel a zároveň poskytnuta IT oddělení lepší administrativní kontrola. Uživatelé tak nejsou nuceni neustále držet v paměti hesla skládající se z velkých a malých písmen, čísel a dalších spe-

ciálních znaků. Často se pak totiž stává, že taková hesla zapomenou a přidělávají práci IT oddělení. Přitom samozřejmě nemohou pracovat sami, což firmu stojí další prostředky.

PalmSecure OmniPass Client Edition nabízí dva režimy provozu:

Samostatný produkt (Standalone) a verze pro podnikání (Enterprise)

Standalone Edition je ideální pro malé a středně velké firmy, které chtějí zabezpečení informací a přesné ověřování každého zaměstnance. Může jít o právnické firmy, nebo třeba úzce specializované softwarové vývojáře, kteří potřebují mít svá data zabezpečena unikátním způsobem.

Enterprise Edition je určena pro velké firemní nasazení, které potřebují centralizovanou správu a kontrolu. Jde například o velké banky, kde bezpečnostní politiky nutí pracovníky, aby se při odchodu od počítače odhlásili. Je už jedno, jestli vyrážejí na hodinový oběd, nebo jestli jdou jen za kolegou do kanceláře za rohem. Místo dlouhého zapisování hesla znovu a znovu by přitom stačilo jen přiložit dlaně a heslo by bylo zbytečné. Někteří zaměstnanci také nemusejí své paměti na hesla plně důvěřovat a tak si zapisují ta svá na různé papírky, které nechávají třeba ve stole. To je další bezpečnostní riziko, jež může zkušený člověk zneužít.

Využití databáze služby Active Directory od společnosti Microsoft jako centrálního úložiště také firmám umožňuje flexibilní prostor pro bezpečné ukládání pověření uživatelů. PalmSecure OmniPass je na integrované podnikové úrovni schopno protokolovat jednotlivé události, což umožňuje zaměstnancům, jasnou kontrolu uživatelských operací, které pomáhají v souladu s právními předpisy, jako je HIPAA, Sarbanes-Oxley a Gramm-Leech Bliley.

Klíčové vlastnosti jsou:

- **PalmSecure přihlášení pomocí biometrie krevního řečiště v dlani**
Krevní řečiště v lidské dlani je unikátní a jedinečný biometrický údaj s velmi vysokou přesností definující každého jednotlivce. Záměna je prakticky vyloučena. Pro přihlášení do systému jsou využity snímače těchto biometrických dat PalmSecure.
- **Administration Console**
Centrální aplikace pro jednoduchou správu všech nastavení
- **Kompatibilní s Microsoft Active Directory a eDirectory**
Umožňuje napojení, integraci a komunikaci s LDAP Db Active Directory
- **Rychlé a snadné zápisy**
Pořízení biometrických předloh (šablon) je velmi jednoduché a intuitivní. Veškerá data lze velmi jednoduše a velmi efektivně nahrát do databázi a pomocí Administration Console je přehledně spravovat.
- **Autentizace, která neobtěžuje**
Systém místo komplikovaných hesel využívá velmi uživatelsky přívětivého přiložení pouhé dlaně.
- **Šifrované úložiště pro ukládání šablon**
Šablony jsou bezpečně uloženy a zašifrovány, je zde tedy použita ochrana v případě pokusu o kompromitaci systému
- **Schopnost na úrovni Enterprise – manažerské sledování událostí**
Tato výjimečná vlastnost umožňuje centralizovanou správu a jednoduchou tvorbu reportů.
- **Single Sign-On konektivita**
SSO tedy automatické přihlášení do různých systémů bez nutnosti opakovaného ověřování (heslo je nahrazeno přiložením dlaně).

Implementace .NET portálu na cloudové platformě Microsoft Azure

David Hláček, YOUR SYSTEM, spol. s r.o.

O projektu

Cílem projektu je implementovat nový portál zdravotní pojišťovny. Současný portál je provozován externím subjektem, náklady na provoz se pohybují v jednotkách milionů měsíčně. V rámci snižování provozních nákladů se předpokládá návrh in-house řešení portálu, které funkčně plně nahradí současné řešení.

Portál lze rozdělit na 3 komponenty:

- **Veřejný portál** – poskytnutí informací všeobecné veřejnosti
- **Extranet** – výměna dokumentů mezi partnery, zdravotnickými subjekty a registrovanými lékaři
- **Intranet** – rozhraní pro zaměstnance pojišťovny

Náklady na realizaci by neměly překročit současný náklad na roční provoz portálu.

Dle projektového plánu měl portál vzniknout v co nejkratším možném čase. Předpokládaný termín zahájení, alespoň částečného provozu, byl stanoven na začátek třetího kvartálu roku 2015, tedy do půl roku od zahájení.

Vývoj portálu musel začít okamžitě. Pro naplnění cílů projektu, bylo potřeba využít zrychlené metodiky projektového řízení.

Zvažované varianty

Ve výchozí situaci bylo zvažováno několik modelů.

V aplikační oblasti se jednalo zejména o tyto modely:

- **využití enterprise CMS systému na technologiích J2EE** (produkt LifeRay), databáze Oracle EE
- **využití Microsoft Sharepoint pro implementaci portálu**
- **vývoj vlastní aplikace v prostředí .NET**

V oblasti infrastruktury:

- pořízení hardware dostatečně výkonného pro provoz portálu v období 4 let
- pronájem výpočetního výkonu formou cloudu

Zhodnocení

Využití enterprise CMS systémů (vč. Microsoft Sharepoint) by si vyžádalo další náklady na pořízení licencí a případné podpory.

Další, dosud nezmíněnou možností, by bylo vypsát veřejnou soutěž na dodávku kompletního portálu, a to včetně HW a SW platformy. Tato možnost nebyla využita, z důvodu rizika, které představovala možná uzavřenost systému, která by omezila či znemožnila jednoduchý rozvoj nových funkcionalit. Zdravotní pojišťovna by se tak mohla dostat do obdobné situace, v jaké se dnes nachází.

Rozhodnutí padlo na vlastní vývoj portálu v prostředí Microsoft .NET. Hlavními důvody byla zkušenost vývojářů s projektem obdobného rozsahu, možnost nezávislosti na konkrétním dodavateli a vlastní odpovědnost za budoucí rozvoj.

Nebylo možné dostatečně přesně navrhnout HW parametry pro vysoce dostupnou infrastrukturu, která by byla schopná uspokojit požadavky na odezvy aplikace. A také nebylo možné s dostatečnou přesností kvantifikovat licenční požadavky na uspokojení všech požadovaných funkcionalit. Bez těchto znalostí nešlo vyspe-

cifikovat objednávku na dodávku hardwarového a softwarového vybavení pro účely provozování produkčního prostředí ani požadavky na vývojové a testovací prostředí.

Z těchto důvodů se zdálo jako nejvhodnější řešení využít pronájem výpočetního výkonu a licencí. A samozřejmě možnost využít cloudové řešení.

Cloud nabídl okamžitý přístup k výpočetnímu výkonu formou pronájmu. Platforma jako služba (Paas) navíc umožnila vývojářům soustředit se na vývoj, a úlohy spojené s administrací a konfigurací systému ponechat na poskytovatele cloudu.

Vzhledem ke zvolené architektuře Microsoft .NET padlo rozhodnutí využít cloud Microsoft Azure.

Microsoft v rámci Visual Studio pro MSDN poskytuje kredit v hodnotě cca 75 EUR (který se obnovuje na měsíční bázi) pro okamžitý přístup ke cloudovým službám Microsoft Azure. To umožnilo zahájení vývojových prací ještě před vyřešením obchodních záležitostí.

Realizační fáze

Výzvy projektu:

- Jak uspokojit funkční a nefunkční požadavky?
- Jak navrhnout architekturu produkčního řešení, bez znalosti velikosti „v současnosti ještě neexistující aplikace“?

V první fázi bylo třeba:

- navrhnout aplikační architekturu
- zvolit vhodné komponenty, v souladu s enterprise architekturou
- navrhnout způsob implementace funkčních požadavků
- zajistit integraci na stávající infrastrukturu

Z důvodu krátkých termínů, bylo přistoupeno k rozhodnutí, že budou některé komponenty portálu realizovány cestou reuse současných komponent. S cílem jejich budoucí implementace do nového prostředí.

Sizing

V rámci návrhu architektury bylo potřeba vydefinovat takové požadavky na provoz, které zaručí odezvy portálu v požadovaném čase. V tomto případě, zátěž generují uživatelé, aktuálně pracující se systémem. A toto množství je možné predikovat.

Předpokládali jsme rozdělení dne na čas pracovní (od 8 do 18 hodiny) a čas klidu (mimo pracovní dobu a víkend). V rámci pracovního dne byla špička v časovém intervalu do dvou hodin.

Díky modelu „pay-as-you-go“ bylo možné postupovat následujícím způsobem:

- v pracovní době pronajímat výpočetní výkon o 18 ti virtuálních instancích
- v rámci špičky pronajímat výpočetní výkon až do celkového poolu 24 virtuálních instancí
- mimo pracovní dobu a o víkendech pronajímat 2 virtuální instance na oblast portálu (celkem 12 virtuálních instancí, za předpokladu 3 oblastí portálu, každá oblast je komponentně rozdělená na prezentační roli (webová role) a aplikační roli (worker role).

Při pořizování vlastní hardwarové infrastruktury by bylo nutné vycházet z maximalistické varianty a počítat s takovou velikostí infrastruktury, která by uspokojila odezvy v době špičky. Z toho nám plynul jasný a jednoznačný benefit pro využití cloudových služeb.

Architektura v cloudu

V souvislosti s rozvojem cloudových služeb vznikají nové best practices, při návrhu architektury v souladu s aplikační architekturou komponentních platformních služeb v cloudu. Zejména se jedná o nové metody při návrhu vysoké dostupnosti a škálovatelnosti služeb. Dokonce se objevují i radikální návrhy.

„Zapomeňte na všechno, co dosud víte o enterprise architektuře a začněte na zelené louce.“

Při návrhu aplikační architektury jsme využili zejména následující best practices:

- **Event-driven, non-blocking I-O programování**
Jednoduše řečeno, aplikace požádá na základě události o poskytnutí vstupů a pokračuje dál v exekuci. Až metoda data zpracuje, zavolá zpátky a data poskytne.
- **Frontování (Queues)**
Cloudové služby zpracovávají data z fronty dle aktuálních možností. V případě neúspěšného zpracování dat, nedojde k zahození požadavku, ale je zpracován další.
- **Cache**
Využívání cache pro ukládání stavových informací. Příkladem je session aktivního uživatele portálu. V případě ukládání na lokálním úložišti cloudové služby dojde při selhání ke ztrátě stavu.

Cloudové komponenty portálu

Pro provozování portálu v prostředí .NET je pro nás výhodnější platforma Azure, která nabízí Cloudovou Službu (Cloud Service). Tato služba byla zvolena jako primární komponenta v souvislosti s navrženou architekturou portálu.

Cloudová služba umožní deployment vlastní aplikace, formou automatizovaného nasazení na předkonfigurovaný virtuální server s operačním systémem a aplikačním frameworkem (v případě webové role i ISS). V rámci nasazení na několika instancích využijeme službu load-balancingu nad těmito instancemi. Odpovědnost za běhové prostředí a nad operačním systémem přebírá Azure, který zajišťuje jeho aktuálnost (provádění aktualizací) a funkčnost (identifikace a odstraňování závad). Pro účely vysoké dostupnosti jsme pro každou službu využili alespoň dvě paralelní instance cloudové služby.

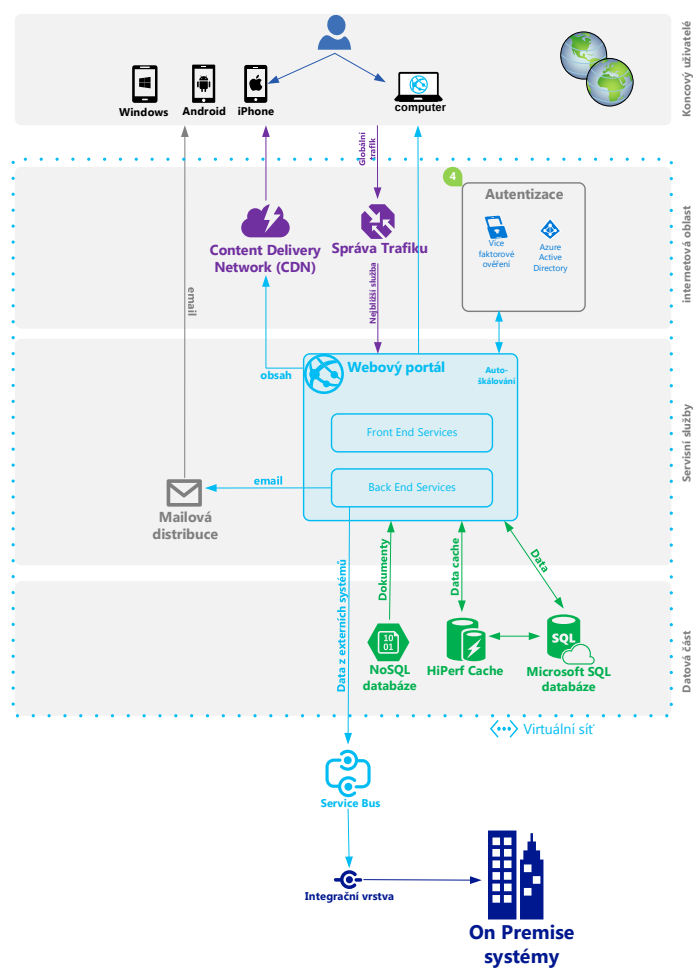
Využití dalších komponent a jejich účel v rámci navržené architektury bude prezentován, následuje alespoň jejich výčet:

Základní služby

- **Cloud Services / Cloudové služby**
- **SQL Database / Databáze SQL**
- **Virtual Machines / Virtuální počítače -**
- **DocumentDB -**
- **Redis Cache / Mezipaměť Redis**
- **Storage -**
- **Virtual Networking**
- **VPN**
- **CDN**
- **Service Bus**
- **Backup**
- **Active Directory**

Podpůrné služby

- Visual Studio Online
- Scheduler
- Automation
- Application Insights aplikací
- Operation Insights
- Azure Search



Obrázek 1 Architektura portálu

Závěr

Využití benefity volného kreditu v rámci vývojového prostředí Visual Studio umožnilo začít s okamžitým vývojem.

In-house vývoj portálu umožní zákazníkovi lepší flexibilitu a vlastní odpovědnost za další vývoj. Forma pronájmu výpočetního výkonu a licencí za cloudové služby, umožní minimalizovat počáteční náklady (CAPEX).

Projekt se v současnosti nachází ve fázi vývoje. Předpokládá se náběh do pilotního provozu počátkem 3Q 2015. Cílem projektu je poskytnout plně funkční náhradu za současné řešení od následujícího roku.

Dovolujeme si Vás pozvat na krátkou prezentaci, v rámci které Vám přiblížíme všechny aspekty. Tedy od výchozí situace, přes výběr variant řešení, postupu realizace a seznámíme vás s aktuálním stavem. Dozvíte se, proč nakonec vyhrál cloud a v jaké podobě.

Software pro podporu krajského krizového řízení a plánování, risk managementu, využití bezpilotních dronů ve spojení s technologiemi Microsoft

Ing. Rostislav Hlosta, vedoucí odboru Business Development, VÍTKOVICE IT SOLUTIONS a.s.

'C3M - UAV' je integrované řešení pro podporu krizového řízení, havarijního plánování a vyhodnocování rizik, využívá technologie společnosti MICROSOFT. Řešení rozšiřuje komunikační schopnosti krizového štábu, pomáhá plánovat jednotlivé situace, vyhodnocovat, analyzovat jednotlivé postupy a tím chránit majetek a obyvatelstva v kritických situacích, jako jsou záplavy, lesní požáry, narušení elektrické energie nebo dodávky pitné vody, únik chemikálií nebo hromadné dopravní nehody.

Součástí navrhovaného řešení je SW pro řízení rizik ARM (Active Risk Manager) společnosti SwordActiveRisk a bezpilotní letecké drony společnosti ROBODRONE, UAV - Unmanned Aerial Vehicles, které v případě potřeby monitorují on line situaci přímo v terénu před zásahem, během zásahu a po ukončení akce.



Přínos systému C3M spočívá v jednotném uživatelském rozhraní i identických pracovních postupech používaných při vytváření a zpracování dokumentace jak v nekrizovém, tak i krizovém období a v dostupnosti všech potřebných informací a dokumentů na jednom místě (z pohledu uživatele). Tím je vytvořen důležitý předpoklad pro vysokou efektivitu nakládání s informacemi a dokumenty během krizové situace.

Při práci s informacemi a dokumenty spravovanými systémem lze využívat podpory geografického informačního systému. Uživatel si může prostorovou informaci zobrazit na digitální mapě (za předpokladu, že jsou k dispozici místopisná data), zakreslit v mapě zaplavenou či ohroženou oblast, únikovou trasu, případně může připojovat libovolný výřez digitální mapy k evidované informaci a mít tak obrázek mapy k dispozici i pro uživatele, kteří nemají do GIS přístup.

Moduly systému C3M:

- plány a procedury
- deník dispečera
- evidence a seznamy
- vizualizace
- komunikační konzola IKK
- • GIS klient



Informační systém pro krizové řízení a plánování společnosti VITKOVICE IT SOLUTION, a.s. je využitelný i v situacích, které nedosahují svojí závažností kritérií pro vyhlášení krizového stavu, tj. v situacích, které jsou klasifikovány pouze jako mimořádné události, kupř. v případech výskytu:

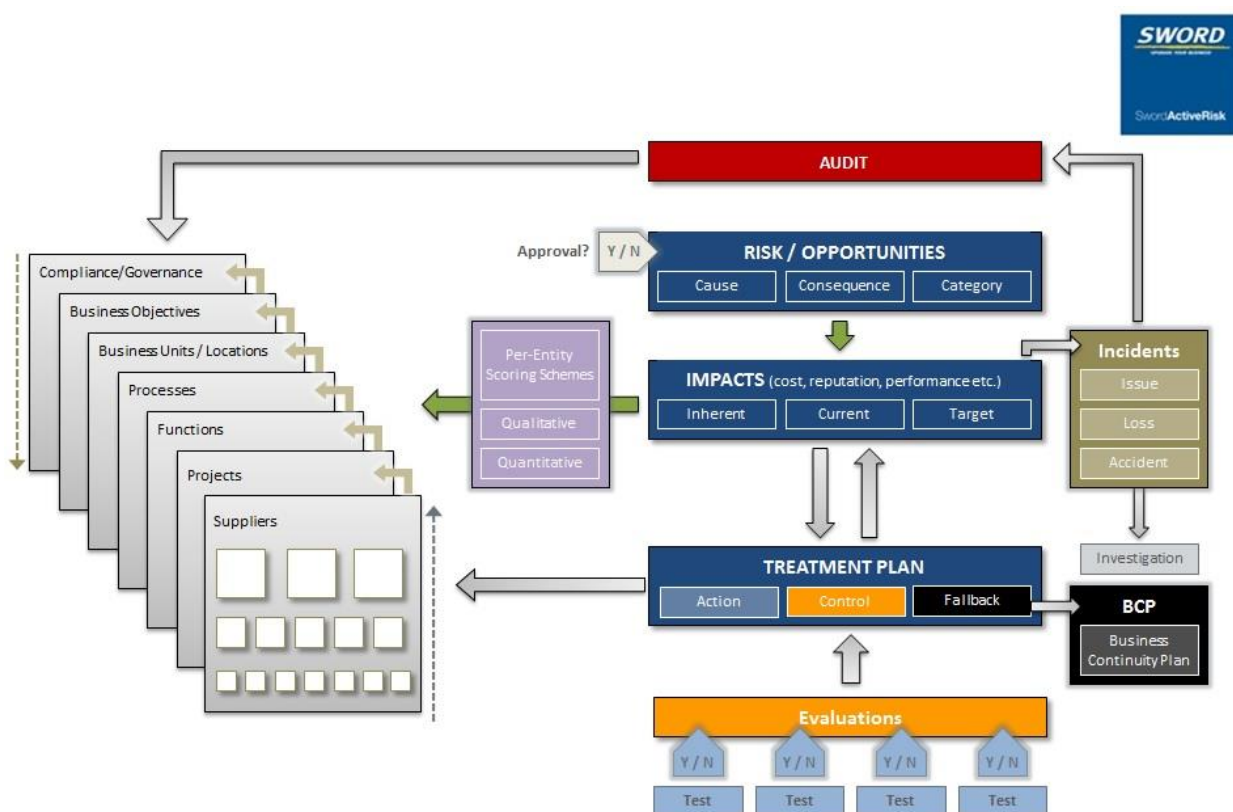
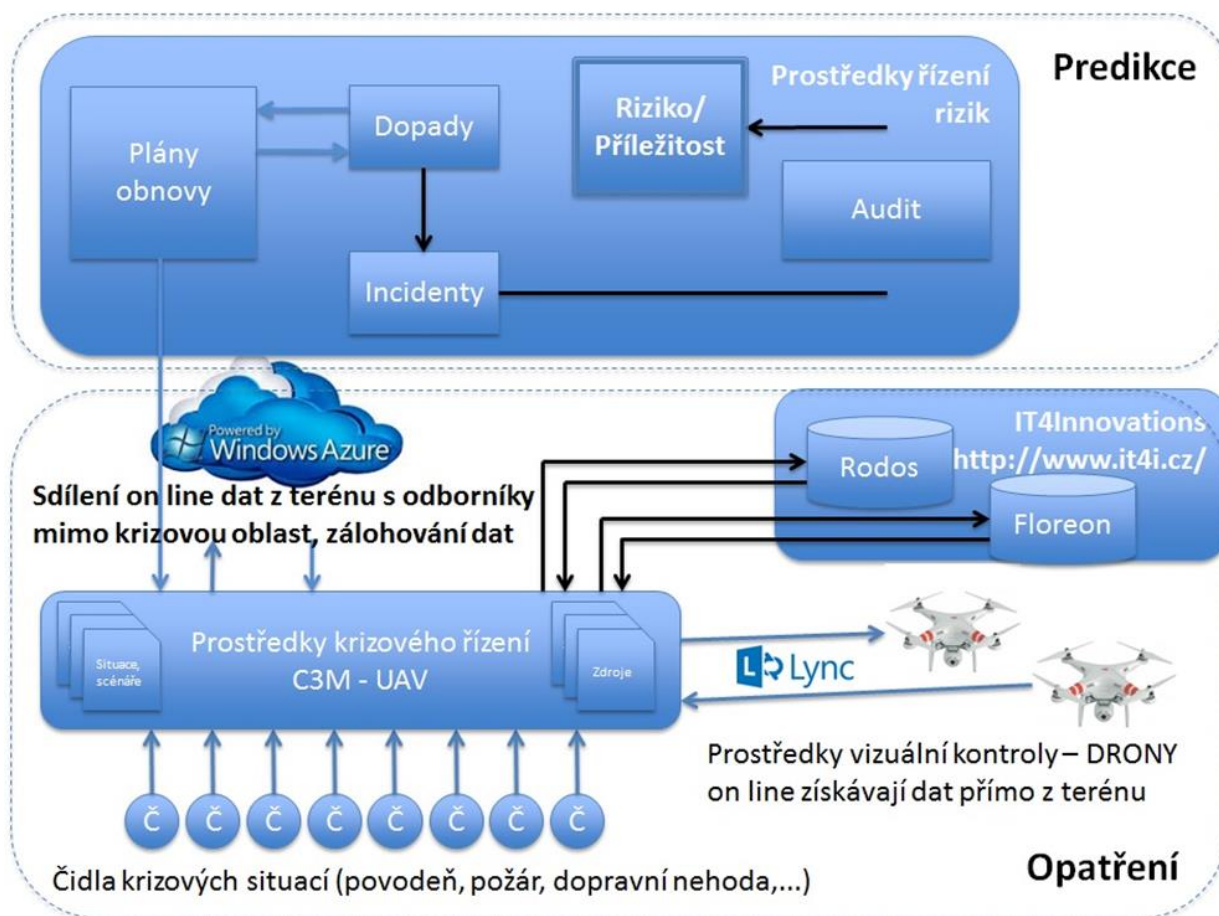
- povodně malého rozsahu,
- dopravní nehody,
- úniku nebezpečných chemických látek,
- požáru, vč. lesního,
- sněhové kalamity apod.

Esenciální role při zhodnocování monitorovacích dat (aktuálních i historických) **přísluší expertním algoritmům**, schopným posoudit jejich relevanci, odvodit z nich významné závislosti, odhalit určité trendy a signalizovat v přiměřeném čase výskyt některých kritických hodnot. Tyto procesy se nemusí opírat jen o data pocházející z hladinoměrů a srážkoměrů, ale že mohou konzumovat (zhodnocovat, korelovat) také údaje pocházející z jiných zdrojů. Systémem vybaveným implementací expertních algoritmů, odpovídajícím výpočetním výkonem a vhodnými rozhraními pro vstup externích požadavků a poskytování výsledků ve standardní podobě je systém FLOREON+.

Systém FLOREON+ je integrovaný systém, který poskytuje řešení pro monitorování, modelování, predikci a podporu řešení krizových situací. V současné době je nasazen na území Moravskoslezského kraje, ale díky své modularitě a otevřenosti umožňuje snadné rozšíření i na ostatní regiony jakož i jeho flexibilní doplňování o nové modely a oblasti simulací pro potřeby krizového řízení. Postupným rozvojem původního řešení se projekt Floreon+ rozšířil o další tematické oblasti, jako je např. řešení problematiky úniků nebezpečných látek nebo sledování vývoje dopravní situace během krizových situací (ve spolupráci s dalšími projekty Národního superpočítačového centra IT4Innovations).

Na úrovni simulace povodňového rizika představuje systém Floreon+ komplexní analytický nástroj, který je schopen automatizovaně řešit srážko-odtokový proces včetně operativního napojení na hydrodynamické procesy (simulace a predikce hladin v korytech toků i mimo hlásné profily kategorie A a B). Dalším důležitým faktorem je i fakt, že systém Floreon+ produkuje geografická data.

Velmi důležitým faktem řešení C3M – UAV, společnosti Vítkovice IT Solutions je **využití bezpilotních Dronů k dalšímu upřesnění aktuální situace v terénu a SW pro řízení rizik ARM (Active Risk Manager)** společnosti SwordActiveRisk.



Komponenty a členové týmu C3M - UAV:

Microsoft:

Posláním a cílem společnosti Microsoft je pomáhat lidem a firmám po celém světě plně využít jejich potenciál.

Microsoft Azure je globální cloudová platforma podnikové třídy, která nabízí výpočetní, úložné, datové, síťové a aplikační služby.

Lync Online je služba zprostředkovávající audio a video konference umožňující komunikaci v reálném čase. Funkce Lyncu Online: Získávání **informací o stavu v reálném čase** – včetně fotografií, stavu dostupnosti a informací o místě – a navíc ještě zdokonalené zasílání rychlých zpráv, díky kterému se spojíte s ostatními efektivněji než kdy dříve.

www.microsoft.com



KRIZOVÝ INFORMAČNÍ SYSTÉM – C3M

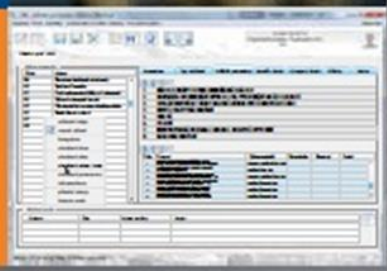
C3M ■ KRIZOVÝ INFORMAČNÍ SYSTÉM C3M

Podpora havarijního a krizového plánování, krizového řízení, tvorby krizové dokumentace.
V desktopové verzi se jedná o uzavřený systém ve formě klient/server aplikace.

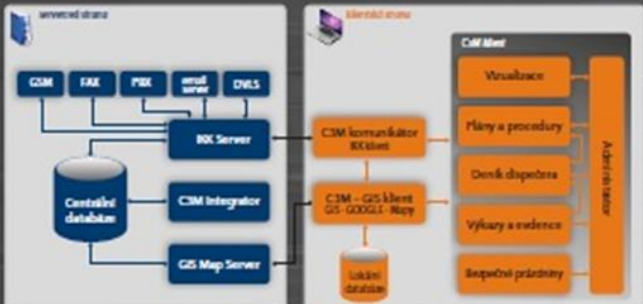
Informační systém C3M je softwarový nástroj, který slouží jako podpora práce krizových manažerů a ostatních osob podílejících se na krizovém řízení a plánování. Systém C3M se soustřeďuje jak na prvotní fáze prevence a přípravy, tak i na fáze reakce a obnovy. Shromažďuje a rychle poskytuje informace potřebné k řešení mimořádných událostí a situací a umožňuje zaznamenávat a sledovat průběh řešení těchto událostí.

Přínos systému C3M spočívá v jednotném uživatelském rozhraní a identických pracovních postupech používaných při vytváření a zpracování dokumentace v nekrizovém i krizovém období a v dostupnosti všech potřebných informací a dokumentů na jednom místě (z pohledu uživatele). Tím je vytvořen důležitý předpoklad pro vysokou efektivitu nakládání s informacemi a dokumenty během krizové situace.





SCHEMA SYSTÉMU C3M



Risk management, implementace SW ARM

Společnost SwordActiveRisk je přední dodavatel SW pro řízení rizik ARM (Active Risk Manager). Společnost SwordActiveRisk působí na trhu již 25 let a je dodavatelem SW pro řízení rizik pro různá průmyslová odvětví. Jejich řešení je možné implementovat v průmyslu, energetice, infrastruktuře, státních organizacích a dalších odvětvích – více na <http://www.sword-activerisk.com/industries/>.

Mimo hlavní produkt ARM společnost dodává 40 specializovaných produktů pro řízení rizik pro odvětvová řešení.

Produkt ARM je v souladu s normou ISO 31000 – Risk management.



FLOREON +

Systém Floreon+ je nástroj pro monitorování, modelování, predikci a podporu řešení krizových situací, a to především se zaměřením na výpočetně a datově náročné simulace. Webově orientovaný systém umožňuje díky své modularitě a otevřenosti snadnou integraci různých tematických oblastí, regionů i dat. Jeho využití je především na úrovni podpory procesů krizového řízení, a to jak v rámci operativy, tak z pohledu simulací.

Systém aktuálně integruje:

- Oblast predikce povodňových situací.
- Modelování úniku nebezpečných látek.
- Sledování aktuální dopravní situace.



<http://floreon.cz>

Centrum RODOS

Centrum pro rozvoj dopravních systémů RODOS je největším současným subjektem působícím v oblasti aplikovaného výzkumu v odvětví dopravy se zaměřením na monitorování, řízení silniční dopravy a jejího financování. Centrum RODOS tvoří tři největší technické vysoké školy v ČR, jedna veřejná výzkumná instituce a šest podniků, které patří mezi přední dodavatele a výrobce v oblasti IT technologií, software, sběru dat a zavádění inteligentních dopravních systémů do praxe na českém trhu. V průběhu řešení projektu jsou vyvíjeny nové koncepty řízení, ovlivňování, podpory a financování mobility. Dlouhodobým strategickým cílem centra je vytvoření komplexní informační nadstavby nad silniční dopravou s využitím nových nástrojů dopravní informatiky a její integrace do stávajících telematických systémů. V rámci plnění cílů centra výzkumné týmy pracují s nástroji Supercomputingu.

Naším strategickým cílem je vytvoření pevného a dlouhodobého partnerství odpovědných orgánů, výzkumných institucí a soukromých podniků, které posune vývoj technologií a dopravních systémů do bodu, kdy jejich denní využívání pomůže realizovat dlouhodobé vize spojené s inteligentní a udržitelnou mobilitou. V konečném důsledku jsou to koncoví uživatelé, kdo by měli, po zavedení výsledků centra do praxe, ve svém denním životě rozpoznat reálné zvýšení kvality svých přepravních procesů. Doprava se musí zaměřovat na účastníky provozu a jakýkoli systém (či kombinace systémů) ignorující tuto prostou skutečnost bude

mít omezenou životnost. Jsou to socioekonomické výsledky, dosažené s přispěním činnosti centra RODOS, co se bude v dlouhodobém horizontu skutečně počítat.



www.it4i-rodos.cz

IT4Innovations Národní superpočítačové centrum

Národní superpočítačové centrum IT4Innovations realizuje výzkum zejména v oblastech superpočítání a vestavěných výpočetních systémů. Provozuje nejmodernější technologie a služby v této oblasti a zpřístupňuje je českým i zahraničním výzkumným týmům z akademické oblasti i průmyslu. Od svého počátku je součástí mezinárodní sítě superpočítačových center PRACE a členové jeho týmu jsou mezinárodně uznávanými odborníky. Partnery projektu jsou Vysoká škola báňská – Technická univerzita Ostrava, Ostravská univerzita, Slezská univerzita v Opavě, Ústav geoniky Akademie věd ČR a Vysoké učení technické v Brně. V současné době centrum provozuje superpočítač Anselm. Velký cluster, který bude uveden do provozu v roce 2015, se zařadí mezi sto největších superpočítačů na světě. Vybudování centra IT4Innovations je financováno prostřednictvím Operačního programu Výzkum a vývoj pro inovace, 85% je financováno z prostředků Evropské unie a 15% ze státního rozpočtu České republiky.

IT4Innovations®
národní@it4i.eu
superpočítačové
centrum1##01010

www.it4i.cz

ROBODRONE

Robodrone je bezpilotní letoun (UAV - Unmanned Aerial Vehicles) řízený na dálku operátorem nebo létající samostatně pomocí letových plánů. Jednotlivé typy Robodrone představují šesti- až osmivrtulové univerzální platformy s nosností 5 až 50 kg, určené k pátracím a záchranným operacím, monitorování průmyslových a zemědělských objektů, geodetickým pracím nebo pro filmařské účely. Víceúčelová modulární konstrukce letounu, která umožňuje rychlé a operativní osazení výstroje podle momentální potřeby. Robodrony se vyznačují minimálními požadavky na obsluhu a nízkými celkovými náklady vlastnictví.



www.robodrone.com

VÍTKOVICE IT SOLUTIONS a.s., člen holdingu VÍTKOVICE Machinery Group, poskytuje komplexní řešení v podobě produktů a služeb na základě požadavků zákazníka v mnoha IT oblastech. Společnost se zaměřuje na oblasti řídicích systémů, integrovaných bezpečnostních systémů a systémů pro podporu krizového řízení a plánování.

www.vitkovice.cz

Rychlý mobilní internet a televizní signál mohou nerušeně existovat vedle sebe

Ing. Miroslav Charbuský, Český telekomunikační úřad

Před rokem odstartoval zkušební provoz prvních základnových stanic v sítích LTE. Tato technologie umožňuje mobilní vysokorychlostní připojení k internetu. Výrazně vyšší přenosová rychlost a odezva umožní využívat mobilní síť novým způsobem, na jaký jsme dosud nebyli zvyklí (např. přenosy videa ve vysokém rozlišení).

Mobilní operátoři získali kmitočty pro síť LTE v pásmech 800 MHz a 1800 MHz v aukci, jejíž součástí byl i závazek do 30 měsíců pokrýt řídce osídlené oblasti a do sedmi let mít pokrytí kompletní. Naplňují se ale očekávání Českého telekomunikačního úřadu, že mobilní operátoři budou budovat síť 4. generace rychleji, než jim ukládají podmínky aukce. Čeští spotřebitelé se tak dočkají kvalitního pokrytí mobilním vysokorychlostním internetem dříve.

Spuštění sítě LTE předcházela proces digitalizace televizního vysílání. Opuštěním analogové technologie v roce 2011 vznikl v rádiovém spektru prostor pro nové moderní služby. Ty tak vysílají na kmitočtech, které dříve byly doménou televizního signálu. S tím se mohou v některých výjimečných případech pojít problémy označované jako rušení televizního příjmu. Pravděpodobnost takové situace se zvyšuje v okolí základnové stanice LTE v pásmu 800 MHz, v oblastech příjmu televizních kanálů 59 a 60 (sousedí s pásmem vyhrazeným pro LTE), při použití aktivní pokojové antény či jakékoliv jiné náhražkové antény, nebo při nevhodné konfiguraci anténního systému.

V případě rušení televizního signálu bude obraz tzv. „kostičkovat“ nebo se nebude vůbec zobrazovat. Tehdy je vhodné na stránce start-lte.ctu.cz ověřit, zda v blízkosti místa příjmu televizního signálu není spuštěna nová základnová stanice LTE v pásmu 800 MHz ve zkušebním provozu. Právě povinný nejméně dvouměsíční zkušební provoz vysílačů v pásmu 800 MHz umožňuje včas odhalit takové případy. ČTÚ pak může při zjištění rušení TV signálu provozovatelům základnové stanice nařídít úpravu jejích technických parametrů nebo její úplné vypnutí do doby, než bude rušení odstraněno.

Dosavadní praxe ukazuje, že se nenaplnily katastrofické scénáře prezentované některými provozovateli sítě DVB-T, že budou zarušeny tisíce přijímačů s milionovými náklady na ochranná opatření. ČTÚ za loňský rok přijal celkem 1548 hlášení o rušení příjmu. Na více než 3000 základnových stanic, které byly uvedeny do provozu, připadalo 195 BTS, u kterých se potvrdilo, že v důsledku jejich provozu dochází k rušení televizního příjmu. V takovém případě jdou náklady na odstranění příčin rušení na vrub provozovatele příslušné základnové stanice.

Ne vždy je ale při výskytu kostičkujícího obrazu na vině vysílač pro rychlý internet. Z měření, které ČTÚ provádí, vyplývá, že více než polovinu závad v příjmu signálu způsobují nedostatky přijímacích zařízení. V dalších 30 % případů se žádné rušení nezjistí.

Interaktivní úřad

Ing. Jiří Ileček, programátor, analytik GORDIC spol. s r. o.

Kam směřují peníze z našeho rozpočtu? Jak hospodaří naše příspěvkové organizace? Kdo naší organizaci dodává například v oblasti bytové výstavby? I na tyto otázky si snadno může zodpovědět každý občan s přístupem k internetu, a to díky aplikaci Interaktivní úřad, umístěné na webových stránkách města, kraje či jiné organizace veřejné správy.

- Umožňuje široké veřejnosti udržovat si stálý přehled o fungování organizace.
- Posiluje důvěru občanů k vedení města a správě veřejných prostředků.
- Je symbolem moderního, otevřeného a přátelského úřadu 21. století.
- Otevřený komponentní systém s možností rozšiřování portfolia pohledů

Přehledná a srozumitelná prezentace údajů o fungování různých agend úřadu, kterou si každý občan, úředník nebo manažer může zobrazit ve svém internetovém prohlížeči. Aplikace umožňuje nahlédnout na tato data poutavou grafickou formou a v potřebném míře detailu, kterou určuje sama organizace. K dispozici jsou základní obecné přehledy z oblastí rozpočtu, hospodaření příspěvkových organizací, smluvních vztahů, zpracování dokumentů, ale i detailnější pohledy, mnohdy vycházející ze specifické metodiky. Vzhledem k přímému napojení na informační systém správy dokumentů je tato prezentace maximálně efektivní, umožňuje prezentovat i ta nejaktuálnější data uložená v informačním systému a nevyžaduje žádné dodatečné náklady spojené s propojením na zdroje dat. Kromě pasivní prezentace informací je k dispozici i nástroj pro komunikaci s občany, kteří se formou elektronického minireferenda mohou vyjádřit k aktuálním otázkám fungování organizace.

GeoInfoStrategie

(Strategie rozvoje infrastruktury pro prostorové informace v České republice do roku 2020)

RNDr. Eva Kubátová, odbor eGovernmentu, Ministerstvo vnitra ČR

Abstrakt:

V rámci příspěvku bude podána informace o schválení *Strategie rozvoje infrastruktury pro prostorové informace v České republice do roku 2020* (GeoInfoStrategie), která vznikala pod koordinací Ministerstva vnitra ve spolupráci Českého úřadu zeměměřického a katastrálního a ministerstev obrany, životního prostředí, pro místní rozvoj, dopravy, v konečné fázi projektu i ministerstev financí a zemědělství, na základě usnesení vlády České republiky ze 14. listopadu 2012 č. 837.

GeoInfoStrategie byla schválena usnesením vlády České republiky ze dne 8. října 2014 č. 815, kterým bylo zároveň uloženo vypracování Akčního plánu GeoInfoStrategie a jeho předložení vládě České republiky do 30. června 2015, zajištění finančních prostředků pro první dva roky její implementace, i vypracování strategie rozvoje infrastruktury pro prostorové informace navazující (po roce 2020).

Stručně budou zmíněna klíčová témata GeoInfoStrategie, která představují návrhovou část dokumentu:

- Optimalizace regulačního rámce v oblasti prostorových informací,
- Nastavení účinné koordinace oblasti prostorových informací,
- vytvoření Národní sady prostorových objektů jako zdroje garantovaných referenčních geodat nejvyšší úrovně podrobnosti, definované kvality a stanovených vlastností pro vybrané objekty reálné-ho světa; množina abstrakcí objektů s garancí identifikace a prostorové polohy na celém území státu,
- Vybudování Národní integrační platformy pro prostorové informace jako technologické platformy pro integraci a publikování sdílených služeb pro prostorové informace,
- Vybudování Národního geoportálu jako ústředního rozcestníku na dostupné služby a data primárních poskytovatelů a současně rozhraní pro automatizovaný přístup k prostorovým i atributovým datům pořizovaným a aktualizovaným veřejnou správou,
- Zajištění služeb veřejné správy nad prostorovými daty, a to pro všechny druhy subjektů, s využitím sdílených služeb, poskytovaných prostřednictvím Národní integrační platformy pro prostorové informace a objektů Národní sady prostorových objektů,
- Umožnění využívání prostorových informací třetími stranami jako nutné podmínky rozvoje služeb s vysokou přidanou hodnotou a podpory konkurenceschopnosti sektoru ICT služeb v České republice,
- Publikování otevřených prostorových dat a otevřených služeb nad prostorovými daty,
- Zajištění systematického a soustavného rozvoje lidských zdrojů, vzdělávání a vědy, výzkumu a inovací v oblasti prostorových informací,
- Publikování prostorových dat a služeb nad prostorovými daty respektujících mezinárodní závazky a mezinárodní interoperabilitu.

Bude podána informace o budoucí implementaci GeoInfoStrategie na základě Akčního plánu, jehož vypracování pod koordinací Ministerstva vnitra ve spolupráci s výše uvedenými subjekty se chýlí do konečné fáze a jehož obsah bude v rámci prezentace stručně zmíněn.

Portal for ArcGIS

Ing. Radek Kuttelwascher, vedoucí oddělení technické podpory prodeje, ARCDATA PRAHA, s.r.o.

Prostředky ArcGIS pro publikaci webových map a služeb pamatují již dlouhou historii. Pomineme-li opravdu dřevní doby webového mapování v podobě ArcView IMS nebo MapObject IMS z konce devadesátých let, pak výrazný pokrok zaznamenal až na přelomu tisíciletí tehdy nový produkt ArcIMS. Jeho nástupce, tehdy již plnohodnotný serverový GIS založený na jádru ArcObjects, se v podobě ArcGIS Server objevil zhruba o pět let později, v roce 2004. Přestože se ArcGIS for Server za deset let výrazně modernizoval, přesto to byl stále nástroj určený především pro GISové administrátory.

Portal for ArcGIS je nadstavba ArcGIS for Server, jejímž cílem je mimo jiné i zpřístupnit potenciál serveru a jeho webových map i širší GISové veřejnosti. Portal for ArcGIS umožňuje jednoduše vyhledávat, používat, sdílet i vytvářet služby, webové mapy a aplikace. Vedle správy mapového obsahu poskytuje nástroje pro správu uživatelů a přináší nástroje pro zabezpečený přístup ke geografickým datům. Portal for ArcGIS slouží i jako úložiště geografických dat a řady dalších souborů. Využívá přímo infrastrukturu organizace a data tak nemusejí opustit zabezpečené prostředí firemního intranetu. Je tedy vhodný především pro společnosti, které používají citlivá a vysoce důvěrná data, ale své využití najde kdekoli, kde je důležitá kontrola nad všemi složkami IT infrastruktury.

Portal for ArcGIS umožňuje:

- správu prostorových dat,
- tvorbu map a aplikací a jejich sdílení s ostatními členy organizace i mimo organizaci,
- vytváření skupin uživatelů pracujících na společných projektech,
- podporu spolupráce při vytváření a používání geografických dat v organizaci,
- řízení uživatelských účtů pomocí interních uživatelských účtů nebo Windows Active Directory a LDAP (podpora SAML a Cross-domain Web Single Sign On).

Jaké jsou tedy hlavní vlastnosti portálu?

Přátelské uživatelské prostředí mapového serveru

Portal for ArcGIS poskytuje stejné uživatelské prostředí jako Esri uživatelům dobře známý ArcGIS Online, tentokrát ovšem na vlastní infrastruktuře. Oprávnění uživatelé tak mohou vytvářet, organizovat a sdílet mapový obsah a propojovat tento obsah s uživateli formou připravených aplikací.

Aplikace

Pro distribuci dat a webových map obsahuje Portal for ArcGIS i několik hotových aplikací. Jsou to např. Esri Maps for Office, Operations Dashboard for ArcGIS, Collector for ArcGIS, Explorer for ArcGIS a další. Pro vytvoření specifické webové aplikace poslouží Web AppBuilder for ArcGIS, případně AppStudio for ArcGIS pro účely vytváření nativních aplikací pro nejrůznější mobilní zařízení.

Snadné generování webových map

Webové mapy umožňují uživatelům vytvářet „mash up“ mapových služeb a definovat jejich chování. Webová mapa pak může být opakovaně použita v mnoha různých aplikacích určených pro různá zařízení nebo zapouzdřena do webových stránek. Webová mapa usnadňuje a urychluje cestu geografických dat ke koncovému uživateli.

Řízení přístupu k prostorovým datům

Portal for ArcGIS hraje úlohu centrálního uzlu platformy ArcGIS. Řídí přístup uživatelů nebo klientských aplikací k jednotlivým položkám serveru a chrání tak obsah před neoprávněným přístupem.

Dohledový systém GINIS upozorňuje s předstihem na hrozící průšvihy

Bc. Jan Kuttich, programátor GORDIC spol. s r.o.

Ačkoliv by název této aplikační nadstavby mohl na první pohled evokovat její zaměření na sledování správné funkcionality HW a SW komponent vašeho informačního systému, je to v tomto případě poněkud jinak.

Základním cílem Dohledového systému GINIS je dohled se zaměřením na konkrétní služby, jejichž provádění přímo souvisí s výkonem působnosti dané organizace. Není tedy primárně zaměřen na monitorování technologických komponent, ale na kontrolu dodržování termínů a kvality různých procesních postupů.

Jinými slovy, jeho smyslem je provádět průběžné a průkazné vyhodnocování činnosti organizace a s předstihem upozorňovat na nesplněné limity tak, aby se předcházelo nedodržení stanovených pravidel a metodiky.

Dohledový systém je dodáván samostatně jako nadstavba událostního systému. Tu tvoří sada specializovaných obslužných akcí a kontrolních sestav určených pro vlastní kontrolu plnění nastavených interních procesů v jednotlivých agendách. Uvedená sada obslužných akcí a sestav je jinak též nazývána souhrnným označením „kontrolní chody“.

Typickými představiteli kontrolních chodů jsou např. „Kontrola na neproučtované doklady ovlivňující přiznání k DPH“, „Kontrola dodržení termínového plánu procesu realizace veřejné zakázky“, „Kontrola chybějící specifikace na položkách akvizičních plánů u připravovaných a podepsaných smluv“ a řada dalších. Výsledky těchto kontrolních chodů lze následně zobrazit přímo odpovědným osobám v příslušných aplikacích, hromadně avizovat prostřednictvím e-mailových zpráv nebo automatizovaně eskalovat na vědomí nadřízeným pracovníkům.

Díky těmto vlastnostem může Dohledový systém bezesporu přispět jak ke zrychlení a zkvalitnění plnění jednotlivých pracovních úkolů, tak k zefektivnění činnosti vlastní organizace jako celku.

Srovnání elektronické značky a elektronické pečete

Mgr. Tomáš Lechner, Ph.D., Vysoká škola ekonomická v Praze, Národohospodářská fakulta, Katedra práva

Úvod

Jedním ze základních předpokladů použití informačních a komunikačních technologií ve veřejné správě je uzákonění bezpečnostních prvků pro elektronické dokumenty (bližší viz [1] a [2]). Na základě stále ještě platné Směrnice Evropského parlamentu a Rady 99/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy mají jednotlivé členské státy Evropské unie implementovány do svých národních právních řádů odpovídající normy obsahující definice elektronického podpisu a pravidla pro jeho tvorbu, použití a ověřování. Zejména z důvodu určité roztržitosti těchto národních řešení a za účelem zvýšení důvěryhodnosti elektronických transakcí na vnitřním trhu a podpory jednotného digitálního trhu a přeshraničních digitálních služeb bylo v roce 2014 schváleno a publikováno v Úředním věstníku Evropské unie Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

Toto nařízení, známé pod zkratkou eIDAS, se plně použije ode dne 1. července 2016, kdy zároveň dojde ke zrušení výše citované Směrnice. Nařízení eIDAS zavádí svou vlastní definici elektronického podpisu, která se ale zásadně neliší od stávající právní úpravy v České republice. Kromě toho definuje elektronickou pečeť a časové razítko. Též posledně zmíněný institut je již delší dobu v českém právním řádu zaveden a nařízení eIDAS jej zásadním způsobem nemění. Jinak je to s elektronickou pečeti, která je jistou obdobou stávající elektronické značky podle českého zákona o elektronickém podpisu, avšak zcela stejné tyto instituty nejsou. Jejich srovnáním na základě českého zákona o elektronickém podpisu a nařízení eIDAS se zabývá tento příspěvek.

Elektronická značka

Zákon o elektronickém podpisu byl v České republice schválen v roce 2000 a účinnosti nabyl již 1. října téhož roku. V první verzi zákona byl definován pouze institut elektronického podpisu, a to v různých úrovních, jako elektronický podpis a zaručený elektronický podpis. Významná novela zákona v roce 2004 v podobě zákona č. 440/2004 Sb., kterým se mění zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů rozšířila instituty definované v zákoně o elektronickou značku a elektronické časové razítko. Další z novel zákona o elektronickém podpisu v podobě zákona č. 167/2012 Sb., kterým se mění zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů, a další související zákony, přinesla samostatné definice třetí úrovně uznávaného elektronického podpisu a uznávané elektronické značky.

Aktuální znění zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (dále jen „zákon o elektronickém podpisu“) definuje elektronický podpis jako „údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě“ [§ 2 písm. a) cit. zákona]. Druhou úroveň elektronického podpisu je následně definovaný zaručený elektronický podpis, který musí navíc splňovat požadavky podle § 2 písm. b) cit. zákona, které jsou následující:

Zaručený elektronický podpis „je jednoznačně spojen s podepisující osobou, umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě, byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou, a je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat“.

Uznávaný elektronický podpis je definován v § 11 odst. 3 zákona o elektronickém podpisu jako „zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a obsahujícím údaje, které umožňují jednoznačnou identifikaci podepisující osoby“.

Pro elektronickou značku připouští zákon o elektronickém podpisu pouze dvě úrovně, elektronickou značku bez přívlastku a uznávanou elektronickou značku. Elektronickou značkou se podle § 2 písm. c) cit. zákona rozumí „údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky:

- jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu,
- byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou,
- jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat“.

Již tato definice tedy vyžaduje pro elektronickou značku bez jakéhokoliv dalšího přívlastku náležitosti, které jinak odpovídají zaručenému elektronickému podpisu z hlediska výše zmíněných úrovní elektronického podpisu. Podle ustanovení § 11 odst. 4 zákona o elektronickém podpisu se uznávanou elektronickou značkou rozumí „elektronická značka založená na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb“.

Základní rozdíl mezi uznávaným elektronickým podpisem a uznávanou elektronickou značkou je specifikován § 3 a § 3a zákona o elektronickém podpisu. Jestliže pro elektronický podpis platí, že pokud se nepokáže opak, má se za to, že se podepisující osoba před podepsáním datové zprávy s jejím obsahem seznámila, pak pro elektronickou značku platí, že pokud označující osoba označila datovou zprávu elektronickou značkou, má se za to, že tak učinila automatizovaně bez přímého ověření obsahu datové zprávy a vyjádřila tím svou vůli. Poslední část tohoto souvětí příhodně komentuje R. Polčák, když říká: „Důslednou gramatickou interpretací cit. ustanovení dospíváme mimo jiné i k vtípnému závěru, že zákonodárce zde poprvé v historii přiznává existenci vůle právnické osoby a možnost, že je tato vůle projevována přímo (nikoli tedy prostřednictvím statutárních orgánů nebo zástupců)“ – viz [3], str. 195.

Zákon o elektronickém podpisu ještě pro uznávanou elektronickou značku definuje požadavky na soulad s originálem (§ 4 cit. zákona), povinnosti označující osoby (§ 5a cit. zákona), náležitosti kvalifikovaného systémového certifikátu (§ 12a cit. zákona) a prostředky pro vytváření elektronických značek (§ 17a cit. zákona).

Elektronická pečeť

Jak již bylo zmíněno, nařízení eIDAS definuje elektronický podpis, přičemž stejně jako stávající zákon o elektronickém podpisu, připouští několik úrovní: „obyčejný“ elektronický podpis, zaručený elektronický podpis a kvalifikovaný elektronický podpis. Tím posledním se podle definice uvedené v čl. 6 cit. nařízení rozumí „zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy“. Nařízení eIDAS tedy nepoužívá pro tuto nejvyšší úroveň elektronického podpisu (nejvyšší z hlediska důvěryhodnosti) přívlastek uznávaný, ale kvalifikovaný. Z hlediska významu jsou si však tyto úrovně poměrně blízké, samozřejmě s tím významným rozdílem, že uznávaný bezpečnostní prvek je uznáván v rámci českého právního prostoru, zatímco kvalifikovaný bezpečnostní prvek podle nařízení eIDAS je uznáván v rámci celého evropského právního prostoru.

Podle nařízení eIDAS se elektronickou pečetí rozumí „data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu“. Stejně jako pro elektronický podpis jsou definovány úrovně zaručený elektronický podpis a kvalifikovaný elektronický podpis, tak nařízení eIDAS definuje tyto úrovně pro elektronickou pečeť.

Zaručenou elektronickou pečetí se podle čl. 3 cit. nařízení rozumí „elektronická pečeť, která splňuje požadavky stanovené v článku 36“, které konkrétně jsou, že zaručená elektronická pečeť „je jednoznačně spojena s pečetící osobou, umožňuje identifikaci pečetící osoby, je vytvořena pomocí dat pro vytváření elektronických pečetí, která může pečetící osoba s vysokou úrovní důvěry použít k vytváření elektronické pečetě pod svou kontrolou, a je k datům, ke kterým se vztahuje, připojena takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat“.

Kvalifikovanou elektronickou pečetí se pak rozumí „zaručená elektronická pečeť, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť“. Kvalifikovaný prostředek pro vytváření elektronických pečetí musí přiměřeně splňovat technické normy a požadavky podle přílohy II nařízení eIDAS. Kvalifikovaný certifikát pro elektronickou pečeť musí být vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru, musí spojoval data pro ověřování platnosti elektronické pečetě s určitou právní osobou a potvrzovat název této osoby a musí splňovat technické požadavky dané přílohou III nařízení eIDAS.

Dále platí, že pečetící osobou je pouze právní osoba. Podle čl. 35 nařízení eIDAS platí u kvalifikované elektronické pečetě „domněnka integrity dat a správnosti původu těch dat, s nimiž je kvalifikovaná elektronická pečeť spojena“. Dále je přímo stanoveno, že „elektronické pečetě nesmějí být upírány právní účinky a nesmí být odmítána jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické pečetě“.

Stejný článek ještě definuje platnost v celém prostoru EU slovy: „Kvalifikovaná elektronická pečeť založená na kvalifikovaném certifikátu vydaném v jednom členském státě se uznává jako kvalifikovaná elektronická pečeť ve všech ostatních členských státech.“

Srovnání obou institutů

Při srovnání obou institutů se soustředíme pouze na nejvyšší úroveň důvěryhodnosti, tj. budeme srovnávat uznávanou elektronickou značku a kvalifikovanou elektronickou pečeť.

Začneme nejprve z více technologického konce. Pokud chce označující osoba vytvořit uznávanou elektronickou značku, potřebuje kvalifikovaný systémový certifikát vydaný akreditovaným poskytovatelem certifikačních služeb, přičemž už z principu kvalifikovaného systémového certifikátu plyne, že jej vydal kvalifikovaný poskytovatel certifikačních služeb. Vše samozřejmě v intencích přívlastku „kvalifikovaný“ používaného zákonem o elektronickém podpisu a nikoliv nařízením eIDAS, kde má přívlastek „kvalifikovaný“ silnější význam. Pokud chce pečetící osoba vytvořit elektronickou pečeť, potřebuje k tomu rovněž specifický certifikát. Nařízení eIDAS nepoužívá žádného zástupného přívlastku, ale celé určující sousloví „kvalifikovaný certifikát pro elektronickou pečeť“. Z hlediska obsahu jsou požadavky na oba typy certifikátů odpovídající, jak ukazuje Tab. 1. Jediné rozdíly jsou v tom, že u kvalifikovaného systémového certifikátu lze uvést omezení pro použití kvalifikovaného systémového certifikátu, přičemž tato omezení musí být zjevná třetím stranám [§ 12a písm. h) zákona o elektronickém podpisu], zatímco u kvalifikovaného certifikátu pro elektronickou pečeť toto možné není, a dále v tom, že kvalifikované certifikáty pro elektronickou pečeť musí obsahovat více údajů pro ověřování elektronické pečetě.

Co se dále pro oba typy certifikátů liší, jsou požadavky na vydavatele a to ve stejném duchu, v jakém se liší požadavky na vydavatele všech typů kvalifikovaných certifikátů podle zákona o elektronickém podpisu a požadavky na vydavatele všech typů kvalifikovaných certifikátů podle nařízení eIDAS. Klíčem je definice služeb vytvářejících důvěru, které přináší právě, jako novinku, nařízení eIDAS a které v souvislosti s elektronickými pečetěmi spočívají ve vytváření, ověřování shody a ověřování platnosti elektronických pečetí a certifikátů souvisejících s těmito službami. Tyto služby podléhají orgánům dohledu a musí splňovat velmi mnoho různých požadavků stanovených nařízením eIDAS a souvisejícími právními předpisy, z nichž některé jsou teprve připravovány. Za to mohou kvalifikovaní poskytovatelé služeb vytvářejících důvěru využívat Značku důvěry EU (viz čl. 23 Nařízení eIDAS).

Požadavky na kvalifikovaný systémový certifikát podle § 12a zákona o elektronickém podpisu	Požadavky na kvalifikovaný certifikát pro elektronickou pečeť podle přílohy III nařízení eIDAS
Kvalifikovaný systémový certifikát musí obsahovat	Kvalifikované certifikáty pro elektronické pečeti obsahují:
a) označení, že je vydán jako kvalifikovaný systémový certifikát podle tohoto zákona,	a) označení, alespoň ve formě vhodné pro automatické zpracování, že se certifikát vydává jako kvalifikovaný certifikát pro elektronickou pečeť;
b) v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen,	b) soubor dat jednoznačně identifikujících kvalifikovaného poskytovatele služeb vytvářejících důvěru, který vydává kvalifikované certifikáty, včetně alespoň členského státu, v němž je poskytovatel usazen, a – v případě právnické osoby: název a případné registrační číslo uvedené v úředních záznamech, – v případě fyzické osoby: jméno osoby;
c) jednoznačnou identifikaci označující osoby, případně prostředku pro vytváření elektronických značek,	c) alespoň jméno pečeti osoby a případné registrační číslo uvedené v úředních záznamech;
d) data pro ověřování elektronických značek, která odpovídají datům pro vytváření elektronických značek, jež jsou pod kontrolou označující osoby,	d) data pro ověřování platnosti elektronických pečeti, která odpovídají datům pro vytváření elektronických pečeti;
e) elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný systémový certifikát vydává,	g) zaručený elektronický podpis nebo zaručenou elektronickou pečeť kvalifikovaného poskytovatele služeb vytvářejících důvěru, který certifikát vydává;
f) číslo kvalifikovaného systémového certifikátu unikátní u daného kvalifikovaného poskytovatele certifikačních služeb,	f) identifikační číslo certifikátu, které musí být jedinečné pro daného kvalifikovaného poskytovatele služeb vytvářejících důvěru;
g) počátek a konec platnosti kvalifikovaného systémového certifikátu,	e) označení začátku a konce doby platnosti certifikátu;
h) omezení pro použití kvalifikovaného systémového certifikátu, přičemž tato omezení musí být zjevná třetím stranám.	–
–	h) údaj o místě, kde je bezplatně k dispozici certifikát, na němž je založen zaručený elektronický podpis nebo zaručená elektronická pečeť podle písmene g);
–	i) údaj o umístění služeb, které lze využít k zjištění platnosti kvalifikovaného certifikátu;
–	j) pokud jsou data pro vytváření elektronických pečeti spojená s daty pro ověřování platnosti elektronických pečeti obsažena v kvalifikovaném prostředku pro vytváření elektronických pečeti, příslušnou poznámku, alespoň ve formě vhodné pro automatické zpracování.

Tab. 1: Srovnání požadavků na obsah kvalifikovaného systémového certifikátu podle zákona o elektronickém podpisu a kvalifikovaného certifikátu pro elektronickou pečeť podle nařízení eIDAS, pořadí v tabulce je určeno českým právním předpisem. Označení písmen dle jednotlivých předpisů bylo zachováno.

Nařízení eIDAS jasně specifikuje, že pečeti osobou může být pouze právnická osoba, zatím co § 2 písm. f) zákona o elektronickém podpisu říká, že označující osobou může být „fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou.“ Nařízení eIDAS tedy jasně říká, že fyzická osoba může pouze podepisovat, zatím co právnická osoba pouze pečeti. Takto je tedy v tomto předpisu určen zásadní rozdíl mezi elektronickým podpisem a elektronickou pečetí, i když to samozřejmě není rozdíl jediný. Naproti tomu zákon o elektronickém podpisu umožňuje vytvářet elektronické značky i fyzickým osobám, i když v praxi se s tímto postupem setkáme jen zřídka (pokud vůbec). Zcela přirozeně spíše z praktických a procesních důvodů je v podstatě dodržován stejný rozdíl, jaký prikazuje nařízení eIDAS.

Pokud se nyní podíváme a čistou základní definici obou srovnávaných institutů, tak nařízení eIDAS vynechává pojem datová zpráva. Místo toho používá spojení „data v elektronické podobě“, přičemž toto spojení již nemá potřebu blíže vymezovat. To zákon o elektronickém podpisu využívá hojně pojem datová zpráva,

který poněkud složitě definuje jako „elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na technických nosičích dat, používaných při zpracování a přenosu dat elektronickou formou, jakož i data uložená na technických nosičích ve formě datového souboru“ (§ 2 písm. d) zákona o elektronickém podpisu]. Jen těžko si lze představit elektronická data, která uvedené podmínky nesplňují, takže nejde ani tak o vymezující podmínky, jako spíše o popisné vysvětlení elektronických dat. Rozdíl v tomto přístupu je tedy jednoznačně poplatný době vzniku obou právních předpisů a postupujícímu rozvoji informační společnosti.

Asi nejdůležitější bude srovnání právních účinků elektronické pečeti (čl. 35 nařízení eIDAS) s odpovídajícím ustanovením § 3a zákona o elektronickém podpisu. Pro uznávanou elektronickou značku platí presumpce automatizovaného vytvoření bez přímého ověření obsahu zprávy, čímž je vyjádřen rozdíl od elektronického podpisu, jímž fyzická osoba podepisuje dokument v digitální podobě. Avšak dále je v zákoně o elektronickém podpisu určitým způsobem vyjádřeno, že se předpokládá, že označující osoba chtěla danou datovou zprávu označit. Nic takového nařízení eIDAS pro kvalifikované elektronické pečeti neříká. Zde platí pouze domněnka správnosti původu dat, s nimiž je kvalifikovaná elektronická pečeť spojena. Onen významný rozdíl elektronického podpisu a elektronické značky explicitně vyjádřený v zákoně o elektronickém podpisu je takto nezbytně definován právě proto, že elektronickou značku může vytvořit i fyzická osoba. Nařízení eIDAS se striktním rozdělením „podpis-fyzická osoba“ a „pečeť-právní osoba“ nezbytně potřebě tohoto vyjádření vyhnulo. Nicméně, jak již bylo zmíněno, neříká ani nic o vůli právní osoby, která pečeť vytvořila. Z toho by se mohlo zdát, že elektronická pečeť je do jisté míry slabším nástrojem (prokazuje méně), než elektronická značka. Avšak z praktického pohledu potřeby vyjádření důvěryhodnosti tomu tak není, protože ačkoliv elektronická pečeť nevyjadřuje vůli pečeti (označující) osoby, klade mnohem větší důraz na proces ověřitelnosti a tedy celkové důvěryhodnosti, se kterou je spojována.

Sumárně bychom tedy mohli říci, že elektronickou značku může použít více subjektů (právní i fyzické osoby) a její použití je na rozdíl od elektronické pečeti vyjádřením vůle, zatím co elektronickou pečeť mohou použít pouze právní osoby, není spojena s vyjádřením vůle pečeti osoby, ale je spojena s domněnkami integrity dat a správnosti původu a je použitelná ve všech členských státech EU. Sílu kompenzující absenci vyjádření vůle (vtipně komentované u elektronické značky ve výše citovaném příspěvku R. Polčáka) u elektronické pečeti specifikuje první odstavce čl. 35 cit. nařízení, který si zde pro jeho důležitost dovoluji na závěr zopakovat:

„Elektronické pečeti nesmějí být upírány právní účinky a nesmí být odmítána jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické pečeti.“

Závěr

Srovnání uznávané elektronické značky a kvalifikované elektronické pečeti ukazuje, že oba tyto instituty mají celou řadu společných atributů, mezi kterými dominuje obdobný právní statut. Ani jeden tento bezpečnostní prvek není elektronickým podpisem ve smyslu podpisu, tedy nevyjadřuje fakt, že by se pečeti osoba před připojením pečeti či označující osoba před označením s pečeti/označovaným textem seznámila. Tedy ani v jednom případě neplatí, že se nelze zprostit odpovědnosti za pečeti/označovaný text. Shoda s vlastnoručním podpisem platí výhradně pro uznávaný (dle zákona o elektronickém podpisu) či kvalifikovaný (dle nařízení eIDAS) elektronický podpis.

Nicméně mezi těmito instituty (uznávanou elektronickou značkou a kvalifikovanou elektronickou pečetí) jsou určité rozdíly. Mezi nimi dominuje možnost pečeti omezena jen na právní osoby, zatím co označovat uznávanou elektronickou značkou mohou, jak právní, tak fyzické osoby. A také fakt, že pro uznávanou elektronickou značku je explicitně stanoveno, že „pokud označující osoba označila datovou zprávu, má se za to, že tak učinila automatizovaně bez přímého ověření obsahu datové zprávy a vyjádřila tím svou vůli“ (§ 3a odst. 2 zákona o elektronickém podpisu), což pro elektronickou pečeť stanoveno není. Pro ni platí

pouze domněnka integrity dat a domněnka správnosti původu, která zase pro elektronickou značku stanovena není. Pro ni platí pouze, že lze původ následně ověřit.

Z hlediska ověřitelnosti je na tom elektronická pečeť lépe z důvodu širší spojitosti se službami vytvářejícími důvěru, které nařízení eIDAS nově definuje. Bylo by velmi špatné, kdyby to bylo jinak, když mezi vznikem cit. nařízení a zákonem o elektronickém podpisu uplynulo více než 10 let a nové nařízení si klade za cíl vylepšit stávající stav problematiky důvěryhodnosti elektronických dokumentů i v dlouhodobém horizontu.

Literatura

- [1] MATES, P., SMEJKAL, V. *E-government v České republice: Právní a technologické aspekty*. 2. podstatně přepracované a rozšířené vydání, Praha: Leges, 2012.
- [2] LECHNER, T. *Elektronické dokumenty v právní praxi*. Praha: Leges, 2013. 256 s. Praktik. ISBN 978-80-87576-41-0.
- [3] POLČÁK, R. Praxe elektronických dokumentů. In *XIX. Karlovarské právní dny*. Praha: Nakladatelství Leges, 2011
- [4] Sbírka zákonů, dostupné na WWW: <<http://aplikace.mvcr.cz/sbirka-zakonu>>.
- [5] Úřední věstník EU, dostupné na WWW: <<http://eur-lex.europa.eu/oj/direct-access.html?locale=cs>>.

Poděkování

Příspěvek je podporován grantem VŠE IGS F5/70/2014 „Aktuální problémy modernizace veřejné správy v ČR“.

Moderní zdravotnictví pro moderní obce

Peter Linhardt, eHealth senior consultant, NESS Czech s.r.o.

Hlavním úkolem elektronického zdravotnictví na té základní, každodenní úrovni je zajistit, aby občan/pacient umožnil každému lékaři, který mu bude poskytovat péči, přístup ke své kompletní zdravotní historii. Aby lékař mohl vidět, kdo a kdy pacienta ošetřil či léčil, jaké mu předepsal léky a jaké jsou výsledky laboratorních vyšetření. To umožní lékaři podstatně kvalifikovanější posouzení akutních příznaků onemocnění, vidět a znát souvislosti současných zdravotních problémů pacienta s těmi v minulosti. Ale také například předepsat léky, které nebudou mít vedlejší účinky následkem interakce s léky, které už pacient užívá.

Bez elektronického zdravotnictví lékař značnou část svého času na pacienta stráví pátráním a rozklíčováním laických a často zkreslených informací o nemocech a léčení pacienta: „Beru na to takové ty malé zelené, či žluté...“ Lékař se pak pouští do rizika při předepisování léku, který může vyvolat interakce s možnými důsledky pro zdravotní stav pacienta. Dnes bohužel je pacient jediným nositelem a informátorem o svém zdraví, medikaci a zdravotní minulosti, pokud s sebou vždy a všude nenosí kufřík (někdy spíš kufr) s kopiemi zdravotních nálezů, laboratorních vyšetření a receptů.

Řešení nabízí informatizace, elektronizace, která zasáhla už snad všechny části naší společnosti. Bez problémů dnes akceptujeme, že banka vede náš účet, že máme peníze v elektronické formě, zadáváme bankovní převody ze svého počítače nebo telefonu a víme, že máme soustavný přehled o stavu našich účtů vždy a všude. Dnes nenajdeme firmu, jejíž účetnictví, skladové hospodářství, nákup a prodej by nebyly vedeny v elektronické podobě. Objemy transakcí dosahují obrovských částek, i když konkrétní informace o nich jsou součástí obchodního tajemství společností, na kterém mohou být firmy někdy existenčně závislé. Ale podnikatelské subjekty, banky i občané vědí, že elektronická doba vyvinula technické prostředky k tomu, aby tyto firemní a finanční informace ochránila proti zneužití či pozměňování.

Informace o občanovi/pacientovi, o jeho zdravotním stavu, nemocech, léčení, lécích... představují jednu z nejcitlivějších, nejosobnějších kategorií osobních informací. Proto zavádění elektronizace do zdravotnictví, které vytváří, ukládá a zpřístupňuje zdravotní informace, šlo ruku v ruce s volbou nejvhodnějšího bezpečnostního konceptu. Tam musí na jedné straně umožnit získat, uložit a zpracovat citlivé pacientovy informace, na druhé straně umožnit přístup k těmto osobním a citlivým informacím pouze oprávněným osobám. Informatizace zdravotnictví je globálním problémem, řeší se ve většině vyspělých zemí a jednotlivé koncepty se liší ve formě ukládání a zpracování zdravotnických informací pacienta, v metodách jejich zpřístupňování, ve způsobech vzájemné komunikace lékařů a zdravotnických pracovníků. Bez ohledu na to, jaký koncept daná země či region zavádí a využívá pro podporu zdravotnictví, jeho elektronizace přináší jasné výhody, které pociťuje pacient, lékař i celý systém zdravotnictví.

Také proto u nás společnost Ness Technologies, která rozumí specifickým potřebám zdravotnictví, nabízí řešení, které zajišťuje základní poslání digitálního zdravotnictví – interoperabilitu. Tedy dostupnost kompletní zdravotní informace a historie pacienta pro lékaře a poskytovatele zdravotní péče. Tato dostupnost je šitá na míru lékaři, který má ze zákona přístup ke komplexní pacientově zdravotní historii (stejně jako dnes, kdy vede a spravuje pacientovu zdravotní kartu). Ale je to pacient, který dává souhlas a umožňuje přístup ke své elektronické zdravotní knížce jiným lékařům nebo třeba členům rodiny. Samozřejmě, možnosti přístupu může upravovat nebo zcela zrušit. Je tak plně zodpovědný za správu těchto přístupových práv. Při přístupu k databázím, které obsahují pacientovy zdravotní údaje, se lékař musí identifikovat elektronickým průkazem zdravotnického pracovníka a dalšími bezpečnostními prvky, které systém ověřuje, aby získal jistotu, že k datům přistupuje oprávněný uživatel. Většinou lékař v ordinaci, ambulanci, klinice nebo v nemocnici. Podobně se při přístupu k vlastním zdravotním záznamům musí identifikovat i pacient elektronickým průkazem, ať už občanským nebo průkazem pojištěnce.

Takto koncipované digitální zdravotnictví přináší pacientovi vyšší kvalitu poskytování zdravotní péče a zvyšuje jeho odpovědnost za vlastní zdravotní stav. Jeho zapojení do procesu organizace zdravotní péče vytváří podmínky pro to, aby se zdravotní péče stala postupně plně orientovanou na opravdové zájmy pacienta.

Mobilní aplikace pro turistu 3. tisíciletí

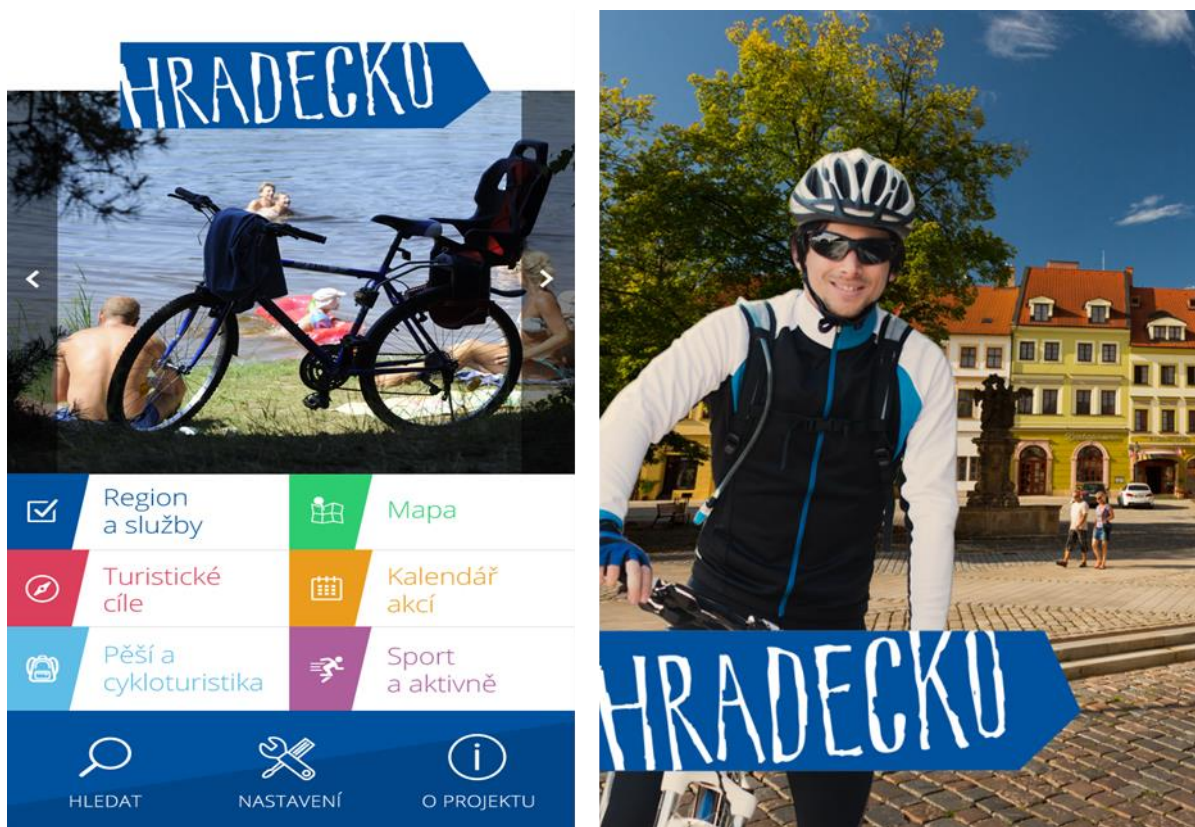
Ing. Daniela Mikšová Mandáková, Bc. Robert Průcha, Turistické informační centrum Hradec Králové



...správný cíl Vaší cesty

Mobilní aplikace TO Hradecko

Cílem této aplikace je vytvořit a začít provozovat prostředky k využití mobilních technologií (tj. mobilní aplikace) pro šíření on-line informací směrem k turistům (památky, navigace, související informace, akce v místě pobytu a v okolí).



Grafický návrh mobilní aplikace Hradecko

V současné době je více než polovina mobilních zařízení používaných aktivní populací v ČR takzvaně „chytrá“ (smartphones). Tento segment zařízení, kam kromě mobilů patří i tablety, konstantně roste. Hodnoceno pohledem obecného marketingu (sem spadá i turistický marketing), jde o nový a atraktivní komunikační kanál, jehož možné využití je nejspíš větší, než dnes dokážeme domyslet.

Proto je v tuto chvíli ten správný čas rozšířit a nasměrovat obsah příslušných webů (v případě tohoto projektu www.hradecko.eu) do mobilních zařízení. Ze zkušeností s obdobnými realizacemi vyplývá, že optimální způsob realizace jsou nativní mobilní aplikace (aplikace vyrobené přímo v prostředí operačních systémů telefonů a tabletů), doplněné přizpůsobenými, neboli responzivními (pro zobrazení a ovládání dotykovými displeji) webovými stránkami.

V současné době je nutné pro přijetí řešení širokou veřejností realizovat mobilní aplikaci pro tři hlavní etablované platformy:

- Android (operační systém společnosti Google, běžící na telefonech a tabletech Samsung, HTC, Asus atd.),
- iOS (operační systém společnosti Apple, běžící na telefonech iPhone a tabletech iPad – výrobce zařízení je shodný s výrobcem OS),
- Windows Phone (operační systém společnosti Microsoft, běžící na telefonech a tabletech Prestigio, HTC, Nokia Lumia atd.).

V rámci přípravy a realizace mobilní aplikace bylo nutné se zaměřit a vyřešit napojení na stávající informační zdroje - tím samozřejmě odpadne nutnost nákladně budovat a následně nákladně provozovat vlastní datovou základnu. Ta již existuje, a slouží v tuto chvíli pro turistické a informační weby poskytované veřejnosti v rámci Destinačního managementu Hradecko.

V aplikaci Hradecko naleznete informace o regionu a jeho službách (Turistická informační centra, ubytování, stravování atd.), turistické cíle (historické památky, přírodní atraktivity, naučné stezky atd.), kalendář kulturních akcí, informace pro pěší a cyklo turistiku (půjčovny a opravy kol, pěší trasy, cyklotrasy atd.), informace pro sportovní a aktivní vyžití (sportovní haly, koupaliště, sauny atd.) a samozřejmě mapu regionu s možností vyznačení vybraných objektů, pozice uživatele a vyhledání spojení.

Podpora více jazyků

Vzhledem k tomu, že potenciálními uživateli jsou i cizinci, je nutná multijazyčná podpora. Stávající fáze uvažuje se 6 jazykovými mutacemi – čeština, angličtina, němčina, polština, holandština a ruština. Aplikace bude primárně přepínat do příslušného jazyka podle jazyka operačního systému. Bude podporovat jazykové verze jak u aplikačních menu, tak i pro datový obsah (bude-li v příslušném jazyce k dispozici).

Doplňkové funkcionality

V souvislosti s vývojem trhu, vyhodnocením provozu mobilní aplikace a s potřebami uživatelů je možné do budoucna rozšiřovat vznikající mobilní aplikaci resp. její menu o další požadované funkcionality.

Realizace

Předpokládáme uvedení mobilní aplikace do praxe do konce června 2015 tak, aby mohla v plné míře sloužit uživatelům na letní turistickou sezonu. Dílo bude k dispozici formou zpřístupnění v obchodech s mobilními aplikacemi Google Play, App Store a Windowsphone.com a v síti internet na adrese m.hradecko.eu.



Zpracovatelem mobilní aplikace Hradecko je firma World Media Partners, s.r.o.

MUNZEE

V roce 2013 se Munzee, jako jedna z outdoorových her na hledání pokladů, dostala i do Hradce Králové. Tato hra se dá přirovnat ke geocachingu, jen místo krabiček hledáte pomocí GPS technologie známky s QR kódem.



V roce 2011 byla hra spuštěna poprvé v Kalifornii. Název hry je odvozen od německého slova pro minci – Münze. Původně totiž měly mít QR kódy kulatý tvar mincí. Postupem času dostaly tvar čtverce s „rozsypaným čajem“. Hráči Munzee vytvářejí pro ostatní známky, které umístí na veřejně dostupné místo a souřadnice místa zveřejní v celosvětové databázi na www.munzee.com. A pokud máte chytrý telefon s fotoaparátem a GPS, zdarma staženou aplikaci na www.munzee.com a datový tarif, tak nechybí nic k tomu, abyste začali hrát. Zápis nálezu totiž provádíte pomocí nasnímání QR kódu na nalezené „známce“, aplikace se připojí k databázi a ověří GPS souřadnice. Poté provede zápis a získáte body, se kterými soutěžíte o co nejlepší umístění v celosvětovém žebříčku.

A pokud nechcete jezdit až do Kalifornie, můžete si zahrát Munzee i v Hradci Králové a projít se procházkovým okruhem „Historickým Hradcem Králové“. V letošním roce předpokládáme rozšíření o další procházkový okruh – „Salon republiky“.

V závěru roku 2014 se podařilo v rámci projektu Hradecko – destinace pro turistu 3. tisíciletí rozšířit Munzee i na oblast Hradecka. Na 37 místech v rámci turistických atraktivit byly vylepeny známky s QR kódem a „lovci QR kódů“ mohli díky sejmutí dalších kódů poskočit v celosvětovém žebříčku úspěšnosti. V průběhu roku připravíme pro zájemce i propagační materiály – brožuru MUNZEE na Hradecku s rozkládací mapou, skládačku a trhací mapu se zakreslením turistických atraktivit na Hradecku.

Více informací na www.munzee.com, www.ic-hk.cz a www.hradecko.eu.

inCity

Do turistické oblasti Hradecko patří samozřejmě i krajské město Hradec Králové, které také předává informace turistům 3. tisíciletí.

Pokud tedy vlastníte chytrý mobilní telefon či tablet s operačním systémem Android či iOS, máte možnost čerpat ty nejčerstvější informace o Hradci Králové zcela zdarma. Prohlédnout si můžete kromě zpráv a aktualit i přehled akcí ve městě, pohodlně se dostanete i k turistickým informacím a nechybí ani praktická data o službách nabízených městem, jako je svoz odpadů či termíny čištění ulic. Stačí si stáhnout z virtuálního obchodu Google Play, respektive App Store aplikaci inCity.



Z funkcí, které aplikace nabízí, jmenujme například přehled aktualit, které jsou zveřejňovány na městském webu a automaticky se tak do aplikace dostanou. Za zmínku stojí i přehled akcí, který je čerpán z městského informačního a rezervačního portálu HKpoint.cz a samozřejmě turistické informace a atraktivita. Rovněž uživatel získá lepší přístup k údajům kulturních institucí a sportovišť ve městě, zároveň i možnost pohodlně zaplatit parkovné smskou. Všechny údaje o lokalitách ve městě jsou doprovázeny mapovými a navigačními funkcemi.

Aplikace byla spuštěna na jaře roku 2014 a díky její stoupající oblibě město plánuje její další rozvoj. V plánu je v tuto chvíli použití aplikace při cestování městskou hromadnou dopravou, při hledání v jízdních řádech či při nákupu SMS jízdenek. Aplikace bude v blízké budoucnosti obsahovat údaje i o cykloturistice.

Aplikaci inCity se vedle Hradce Králové mohou pochlubit i další města, jako například Český Krumlov, Olomouc, Karlovy Vary, Kutná Hora a další. InCity vytvořila firma Intelis z Písku.

Turista v mobilu

Turistické informace nenaleznete pouze v chystané mobilní aplikaci Hradecka, ale i v stále oblíbenější aplikaci Turista v Mobilu.



Jde o mobilního rádce, který Vám pomáhá při plánování výletů a návštěv zajímavých míst České republiky. A to nejen pěšky, na kole nebo na kolečkových bruslích, ale i na běžkách. Ihned budete mít přehled toho nejzajímavějšího a nejdůležitějšího, co je v dané oblasti k vidění a co se v okolí děje. Cíl Vaší cesty bude s Turistou v Mobilu vždy jistý a na červeně vyznačené trase Vám nic zajímavého neunikne. Aplikace Vám poskytne informace o městech a poradí, kam se vydat na výlet. To vše včetně fotografií daných míst, kontaktů, kulturních akcí v okolí a odkazů na webové stránky či důležitá telefonní čísla.

Turista v Mobilu stále roste, jelikož se na vývoji aplikace podílí sami uživatelé, místní obyvatelé i zkušení cestovatelé. Náměty či fotografie zajímavých míst můžete nahrávat do aplikace, nebo je můžete zasílat na e-mail turista@turistavmobilu.cz a po schválení budou zveřejněny. Aplikace je ke stažení zdarma v obchodu Google Play.

GEOFUN

Mobilní aplikace neslouží pouze k praktickým a turistickým informacím, ale také k zábavě. V Hradci Králové si dokonce můžete zahrát hru, co svět neviděl – GEOFUN. Jedná se o geolokační zábavnou hru nové generace, která vychází z populárního geocachingu, ale svou povahou je mnohem akčnější a dobrodružnější. Nestáčí pouze místo najít a „checknout se“, ale také plnit různé úkoly, které Vám průvodce během hry sdělí. Průvodcem je vždy někdo místní, který dané město či region výborně zná a dobře Vám poradí.

V rámci dobrovolného svazku obcí Česká inspirace vznikla v Hradci Králové první ze současných pěti her – Tour de Hradec Králové, kterou je nutné, jak již název napovídá, absolvovat na kole. Více však neprozradíme, zkuste si ji zahrát sami. Zbývajících hrami Vás provedou Eliška Rejčka, detektiv Holub a na nedalekém Chlumu dokonce kanonýr Jabůrek.



A jak to celé funguje? Aplikace GEOFUN je zdarma ke stažení v obchodech Google Play a App Store. Po instalaci a rychlé registraci se ve výčtu geosrand (úkolu) objeví hra pojmenovaná například Bitva u Chlumu 1866. Tu si stáhnete do svého chytrého telefonu a od této chvíle již není nutné mít internetové připojení. Stačí přijít se zapnutou aplikací na místo startu hry (přesný start hry je popsán v detailu geosrandy spolu s dalšími informacemi), zde aplikace na základě GPS souřadnic pozná, že jste na správném místě a celé dobrodružství může začít. Za každou splněnou geosrandu, a to i částečně, získáte body (geonky) do osobního konta (geokonta)

a podle získaných geonek se pak určuje Vaše geohodnost. Všichni hráči, kteří se do hry zapojí, mohou hrát o hodnotné ceny, víkendové pobyty, poukázky do restaurací, vstupenky apod.

V současné chvíli lze hrát geosrandy v městech, jako například Praha, Brno, Ostrava, Zlín, Cheb, Žatec a v mnoha dalších. Aplikace pochází z dílny World Media Partners, s.r.o.



Turisticky významné území Hradecko
Turistické informační centrum Hradec Králové
Gočárova 1225, 500 02 Hradec Králové
www.hradecko.eu
www.ic-hk.cz

SIEM a jak vyhovět podmínkám zákona o kybernetické bezpečnosti

Ing. Maroš Mihalič, Country Manager, Novell-Praha, s.r.o.

SIEM neboli Security Information and Event Management je oblast, kterou se teď mnohé organizace státní a veřejné správy budou muset hlouběji zabývat. Důvodem je nový zákon o kybernetické bezpečnosti, který klade důraz především na nutnost sběru informací o bezpečnostních incidentech z heterogenních prostředí.

Co tedy SIEM přesně je? Jde o ucelený, škálovatelný systém pro management bezpečnostních informací a událostí. Jeho úkoly jsou sběr, analýza, identifikace a vyhodnocení bezpečnostních událostí, které by nám měly sloužit jako podklad pro zdokumentování bezpečnostních incidentů. Se SIEM máte aktuální a nepřetržitý přehled o stavu bezpečnosti, který často zvládá samostatně reagovat na vzniklé hrozby.

Při samotném nasazení je nutné do hloubky analyzovat možnosti produktů, model licencování, počet EPS (Events Per Second), nároky na dostupnost, počet a typ zařízení, informačních systémů, data-bázového prostředí. Je dobré myslet předem na to, vůči jakým normám a standardům budeme reporty generovat. Ty nám mohou následně pomoci při samotných auditech. Samotná implementační fáze nasazení a její náročnost odrážejí požadavky security managerů. Po úspěšné implementaci následují dokumentace, zaškolení a rozvoj samotného řešení. IT prostředí je v čase dynamické a SIEM není výjimkou, spíše opak je pravdou. Značnou část tohoto procesu vám může usnadnit řešení NetIQ Sentinel, které zajišťuje jednoduchou a výkonnou správu zabezpečení. I další řešení společnosti NetIQ mohou zjednodušit chod vaší organizace a soulad s předpisy. Například NetIQ Identity Manager vám usnadní správu identit v celém jejich životním cyklu, zabrání vzniku mrtvých duší, sjednotí hesla do všech informačních systémů bez jakýchkoliv rizik.

NetIQ Sentinel – výkonná a jednoduchá správa zabezpečení

Úvod

Organizace výrazným způsobem transformují své infrastruktury IT a způsob jejich používání. Tyto změny přinášejí řadu problémů a výzev, které mohou negativně ovlivnit schopnost organizace zabezpečit podnikové prostředí. Technologie jako virtualizace, cloud computing a mobilita změnily způsob, jakým společnosti fungují. Umožňují uživatelům pracovat s informacemi a komunikovat mezi sebou novým, moderním způsobem. Pro analytiku informační bezpečnosti je stále náročnější monitorovat a udržovat bezpečnost.

Přehled produktu

NetIQ Sentinel nabízí společností okamžitý přehled o veškerých IT aktivitách, díky čemuž mohou eliminovat bezpečnostní hrozby, zdokonalit zabezpečení a automatizaci vynucování zásad v rámci fyzických, virtuálních i cloudových prostředí. Zjednodušuje tradiční správu bezpečnostních informací a událostí (SIEM) a řeší potíže při zavádění systému SIEM tak, aby mohly inteligentní zabezpečení využívat všechny organizace. NetIQ Sentinel společností nabízí také efektivnější řešení SIEM, a to díky přístupu k okamžitým informacím, detekci odchylek a monitorování aktivity uživatelů. Poskytuje totiž mechanismy včasného varování a přesnější vyhodnocování IT aktivit.

Představuje jediný systém plně integrovaný se správou identit, která umožňuje spojit uživatele s konkrétními aktivitami ve všech prostředích. Díky tomu mohou společnosti snadno identifikovat kritická rizika, výrazně zkrátit reakční dobu a rychle řešit hrozby a narušení zabezpečení, která by mohla mít negativní důsledky pro podnik. Řešení Sentinel díky okamžitým informacím umožňuje společností chránit se před vznikem pokročilých hrozeb, zdokonalit procesy zabezpečení a nepřetržitě vynucovat zásady.

Technické požadavky

HW požadavky: Min. čtyřjádrový Xeon procesor o taktu alespoň 2.5GHz, 4GB RAM a 500GB místa na pevném disku. 64bitový operační systém SLES 11.3 nebo RHEL 6.5. Sentinel lze provozovat jak na fyzic-

kém serveru tak virtualizovaně. Pro virtuální appliance nebo virtualizované instance lze použít hypervizory XEN, VMware, Microsoft Hyper-V nebo platformu Microsoft Azure.

NetIQ Identity Manager – Jedinečné řešení pro bezpečnou správu identit a přístupů

Úvod

Rozrůstající se společnosti musejí zajistit rychlý a bezproblémový přístup k novým aplikacím a službám pro neustále se zvyšující počet uživatelů. S těmito výzvami se vypořádávají implementací různých procesů, avšak jejich existující systémy pro správu uživatelů nejsou v měnících se podmínkách společnosti dostatečně flexibilní, například při zajišťování cloudových aplikací. Výsledkem je pomalá reakce na nové požadavky a nedostatečná kontrola nad tím, jak uživatelé přistupují k podnikovým systémům.

Přehled produktu

Identity Manager je jediným řešením umožňujícím bezpečnou správu identit a uživatelských účtů v rámci fyzických, virtuálních a cloudových prostředí na základě informací o identitě v reálném čase. Nabízí automatizovaný proces obsluhy, správa hesel, samoobslužnost uživatelů, automatizované toky úkolů, správa založená na rolích, delegovaná správa, sledování událostí v celém systému a tvorba reportů, seznam zaměstnanců společnosti a organizační schémata a grafické konfigurační nástroje. Pomocí NetIQ Identity Manageru můžete omezit náklady na správu a helpdesk, zredukovat bezpečnostní rizika, vytvořit produktivní podnikové vztahy, automatizovat komplexní procesy obsluhy s cílem poskytovat okamžitý přístup ke zdrojům, přidělovat uživatelům zdroje na základě rolí a politik, synchronizovat hesla a umožnit tak použití jednoho hesla pro všechny systémy, umožnit uživatelům získat nebo změnit jejich hesla pomocí samoobslužných webových funkcí, vytvářet a uplatňovat silné politiky pro hesla s platností v celém systému, dostávat upozornění v případech přidělení nepřiměřeného přístupu, snižovat náklady a zjednodušovat prostředí.

Technické požadavky

Minimální HW požadavky pro provoz Identity Manageru: Vícejádrový procesor o frekvenci minimálně 2 GHz, minimální velikost operační paměti 6 GB a alespoň 40 GB místa na pevném disku. Podporované operační systémy jsou SLES 11.3, Windows Server 2012 R2 a RHEL 6.5.



O společnosti NetIQ

Společnost NetIQ je globálním dodavatelem podnikového softwaru s výrazným zaměřením na úspěch svých zákazníků. Portfolio společnosti zahrnuje škálovatelná, automatizovaná řešení pro identity, bezpečnost, přístupy, správu, systémy a aplikace, služby a Workload Management, která pomáhají organizacím bezpečně poskytovat, měřit a spravovat počítačové služby ve fyzických, virtuálních a cloudových prostředích.

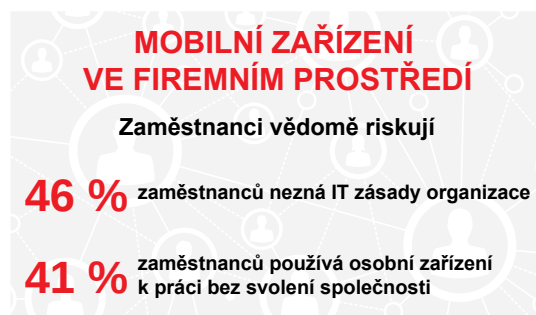


Vaše podniková síť je mnohem větší, než si myslíte

Dokážete říct, kolik zařízení, nad kterými byste měli mít kontrolu, se ve vaší společnosti vlastně vyskytuje?

Staráte se o IT oddělení společnosti nebo úřadu a myslíte si, že velikost vaší sítě odpovídá počtu zaměstnanců? Skutečnost může být úplně jiná a vaše síť mnohem větší, a to díky počtu zařízení, která pracovníci každý den používají. Běžný zaměstnanec v dnešní době vlastní alespoň dvě řešení, jež jsou schopná připojit se k síti (notebook, chytrý telefon, tablet). Musíte počítat i s osobními zařízeními (BYOD), která vlastní. O nákupech nových mobilních technologií oddělení IT často nevědí, a je tak možné, že jejich počet a pohyb se mohou za vašimi zády pomalu, ale rychle vymykat kontrole.

Jak tomu zabránit a navíc uchránit společnost před únikem dat při odcizení nebo ztrátě takového zařízení? Spravovat stále narůstající počet zařízení ručně je téměř nemožné. Na trhu je ale několik řešení, která vám mohou pomoci. Jedním z nich je Novell ZENworks Mobile Management, jenž poskytuje pokročilé nástroje pro správu zařízení a politik na iOS, Android, Symbian, Windows Mobile a dalších ActiveSync zařízeních – vše prostřednictvím jediné administrativní konzole. Tento produkt řeší veškeré problémy, před které jsou administrátoři a manažeři stavěni, včetně BYOD (Bring Your Own Device), zabezpečení, správy aplikací, správy hardwaru a softwaru, shody s předpisy a další. Možnost šifrování a vzdáleného uzamčení nebo vymazání dovoluje spravovat data na základě úrovně zabezpečení, kterou vaše společnost vyžaduje. Podpora LDAP umožňuje řešení Novell ZENworks Mobile Management pracovat s Active Directory, NetIQ eDirectory a ostatními LDAP adresáři.



Novell ZENworks Mobile Management

Rozšířte správu koncových stanic také o správu všech osobních a firemních mobilních zařízení prostřednictvím jediné administrativní konzole.

Úvod

Jak Mobilita a BYOD jsou trendy, které podle statistik neustále rostou. Zaměstnanci stále častěji používají ke své práci mobilní zařízení, která se připojují do firemní sítě. Ať už je to notebook, tablet, nebo chytrý telefon. Každé takové zařízení je nosičem často citlivých dat, která mohou pro společnost v případě ztráty nebo odcizení představovat nemalé riziko.



Přehled produktu

Novell ZENworks Mobile Management poskytuje pokročilé nástroje pro správu zařízení a politik na iOS, Android, Symbian, Windows Mobile a dalších ActiveSync zařízeních – vše prostřednictvím jediné administrativní konzole. Tento produkt řeší veškeré problémy, před které jsou administrátoři a manažeři staveni, včetně BYOD (bring your own device), zabezpečení, správy aplikací, správy hardwaru a softwaru, shody s předpisy a další. Možnost šifrování, a vzdáleného uzamčení nebo vymazání dovoluje spravovat data na základě úrovně zabezpečení, kterou vaše společnost vyžaduje. Podpora LDAP umožňuje řešení Novell ZENworks Mobile Management pracovat s Active Directory, NetIQ eDirectory a ostatními LDAP adresáři.

Technické požadavky

Minimální HW požadavky: 32bitový Xeon procesor nebo lepší, minimálně 2 GB RAM a 3 GB místa na pevném disku. Operační systém Microsoft Windows Server 2003 a novější, Microsoft SQL Server 2008 a novější.

Je veřejný cloud opravdu tím správným místem pro podnikové dokumenty?

Největším nebezpečím pro firmu je zaměstnanec sám. Víte, kam vaši zaměstnanci ukládají smlouvy, prezentace a interní dokumenty?

O riziku ztráty dokumentů uložených v nezabezpečených cloudových úložištích se mluví neustále už několik let. Třetina organizací tento problém ale stále neřeší a velká část ani netuší, jakým způsobem zaměstnanci s firemními dokumenty zacházejí a kde všude mohou jejich citlivá data kolovat. Pracovníci chtějí mít přístup ke svým dokumentům kdykoliv a odkudkoliv, a pokud jim společnost takový přístup nezajistí, najdou si vlastní cestu, jakou jsou právě veřejná cloudová úložiště. Řešením může být sice privátní virtuální síť (VPN), ale ta je často pomalá a nenabízí takový komfort a flexibilitu. Společnost Novell vyvinula nástroj Novell Filr, který umožňuje bezpečný a rychlý přístup a sdílení dokumentů bez toho, aby opustily vaše datové centrum. Pracuje s existující infrastrukturou a řídí se pravidly nastavenými IT oddělením. Sdílet a přistupovat je možné prakticky z jakéhokoli zařízení, a to jak v rámci společnosti, tak i směrem ven.



Novell Filr

Vytvořte nad Vašimi stávajícími datovými úložišti „cloudovou službu“, ke které mohou Vaši zaměstnanci přistupovat odkudkoli a z libovolných mobilních zařízení.

Úvod

Mobilita Synchronizace souborů a hostované služby se v posledních letech velmi rozšířily, ale jen málo jich umožňuje využít vaši vlastní vysokou úroveň zabezpečení a většina vyžaduje dodatečnou úroveň řízení. Proč synchronizovat a hostovat dokumenty někde jinde, když jsou již dostupné ve vašem firemním úložišti? Vše, co potřebujete, je dát uživatelům jednoduchý přístup kdykoliv a odkudkoliv.

Přehled produktu

Produkt Novell Filr vytvoří nad Vašimi stávajícími datovými úložišti cloudovou službu, ke které mohou Vaši zaměstnanci přistupovat odkudkoli a z libovolných mobilních zařízení. Tento koncept ponechává firemní data v bezpečí a pod kontrolou interního IT. Zároveň však poskytuje pro koncové uživatele efektivní

a pohodlnou práci se soubory kdykoli je potřebují. Data není třeba nikam migrovat, zůstávají uvnitř vaší společnosti, uživatelé k nim mají řízený a zabezpečený přístup ať už jsou kdekoli. Nad rámec standardních cloudových služeb umožňuje Novell Filr funkci sdílení souborů, i celých adresářů se zvolenými kolegy, či týmy. Odpadá tedy potřeba žádat ad-hoc přístup u správce datových úložišť nebo posílání potřebných dokumentů e-mailem. Vedoucí teamu jednoduše umožní přístup k potřebným dokumentům přes jediné tlačítko.

Technické požadavky

Novell Filr je distribuován jako virtuální appliance podporující následující hypervizory: Microsoft Hyper-V (Azure), XEN, VMware. Minimální HW požadavky jsou 12 GB RAM, 4 procesory a dva virtuální disky o celkové kapacitě 65 GB.

O společnosti Novell

Jako lídr v oblasti podnikových aplikací přináší Novell řešení, díky kterým jsou pracovní prostředí produktivnější, bezpečnější a snadno spravovatelná. Podporuje tisíce organizací po celém světě prostřednictvím technologií pro spolupráci, mobilitu, zabezpečení koncových zařízení a souborové a síťové služby. Díky produktům jako Novell GroupWise, Novell ZENworks, Novell Open Enterprise Server, Novell Filr a Novell iPrint mohou zákazníci dosáhnout vyšší úrovně produktivity a zároveň minimalizovat náklady, složitost a rizika spojená s jejich IT infrastrukturou. Na českém trhu se pohybuje již 20 let. Patří mezi 15 největších dodavatelů softwaru na světě. Zaměstnává přes 4500 lidí a spolupracuje s více než 3000 partnery.

Novell®

www.novell.cz.

Fungování základních registrů

Ing. Michal Pešek, ředitel; Mgr. Marek Hejduk, pracovník pro vztah s veřejností, Správa základních registrů

1. Cokoliv jste chtěli vědět o základních registrech a báli jste se zeptat?

Jak to vypadalo v praxi předtím, než fungovaly základní registry? Když jste si například měnili adresu trvalého pobytu, museli jste tuto změnu hlásit každému úřadu či instituci zvlášť. S tímto byla spojena vysoká míra byrokracie a zatížení veřejné správy řadou tištěných formulářů, které bylo třeba pracně vyplňovat. Úředník trávil spoustu času nad ověřováním platnosti různých údajů. Bylo to náročné tedy jak pro úředníka, tak i pro občana.

Jak to tedy přesně vypadalo?

- Data v databázích státní správy byla roztříštěná, nejednotná, multiplicitní.
- Neexistovala možnost sdílet údaje v evidencích.
- Ne vždy pro výkon veřejné správy byly k dispozici údaje, na které bylo možné se spolehnout.
- Občan při jednání s úřady musel údaje ke své osobě několikrát opakovaně dokládat.

To vše se po spuštění základních registrů mění k lepšímu. V současné době základní registry velmi významně ulehčují komunikaci mezi úřady a občanem a mezi úřady navzájem.

Občane, máš ponětí, co vůbec jsou a jak fungují základní registry? Je to jednoduché, základní registry máme celkem čtyři – registr obyvatel; registr osob; registr územní identifikace, adres a nemovitostí a registr práv a povinností.

Registr obyvatel (správcem je Ministerstvo vnitra ČR) vede referenční údaje⁵ o všech fyzických osobách a to konkrétně jméno a příjmení, datum narození, adresa místa pobytu, státní občanství, atd.

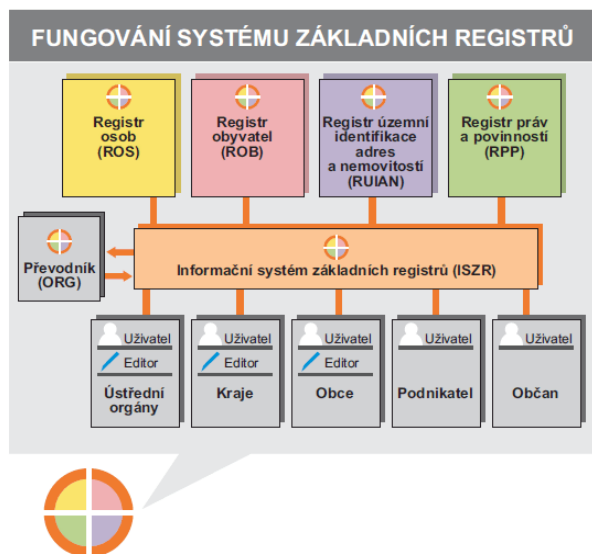
- Registr osob (správcem je Český statistický úřad) slouží primárně k evidenci právnických osob a podnikajících fyzických osob. Vedenými referenčními údaji jsou především obchodní firma či název, datum vzniku nebo zániku z evidence podle jiných právních předpisů, právní forma, datová schránka, atd.
- Registr územní identifikace, adres a nemovitostí (správcem je Český úřad zeměměřický a katastrální) slouží k evidenci územního členění státu. Vedou se referenční údaje o stavebních objektech, pozemcích, ulicích, katastrálních územích, atd.
- Registr práv a povinností (správcem je Ministerstvo vnitra ČR) vede působnosti orgánů veřejné moci⁶ v jednotlivých agendách, jinými slovy, stanoví oprávnění jednotlivých orgánů veřejné moci.

Jde tedy o bezpečnou databázi, která sjednocuje data vedená úřady o občanech a státních i nestátních subjektech. Základní registry představují mechanismus, který jako jediný nabízí relevantní a nezpochybnitelná data – referenční údaje. Nezní to všechno jako Velký bratr? Ochrana osobních údajů i bezpečnost dat je zajištěna díky důležité součásti systému ORG – převodník, který zajišťuje ochranu osobních údajů uložených v základních registrech. Tento systém využívá vygenerovaný identifikátor místo rodného čísla, tím pádem nemůže dojít ke zneužití osobních údajů. V neposlední řadě klíčovým prvkem celého fungování systému základních registrů je Informační systém základních registrů, který zajišťuje sdílení dat a oprávnění přístupu k datům pro oprávněné uživatele či editory.

⁵ Státem garantovaný správný údaj obsažený v příslušném základním registru, který orgán veřejné moci využívá při své činnosti.

⁶ Orgán veřejné moci – státní orgán, územně samosprávný celek a fyzická nebo právnická osoba, byla-li jí svěřena působnost v oblasti veřejné správy.

Schéma fungování základních registrů:



Základní registry veřejné správy představují jeden ze základních pilířů moderního eGovernmentu, tj. procesu elektronizace veřejné správy. Je třeba podotknout, že orgány veřejné moci, občané a další subjekty již v současné době berou systém základních registrů České republiky jako součást moderního fungování veřejné správy. Cílem fungování základních registrů je zefektivnění a využití možností současných technologií pro online přístupy téměř kdykoli a odkudkoli. Současně však základní registry musí splňovat a zajistit efektivní, bezpečnou a transparentní výměnu přesných a aktuálních referenčních údajů.

Kromě zvýšení efektivity státní správy, kdy úředník nemusí zjišťovat, která data jsou aktuální a správná, dochází také ke zrychlení procesu vyřízení žádostí, tedy ke snížení byrokratické zátěže. Daleko méně času strávíte za přepážkou úřadu. Stát pracuje čím dál tím efektivněji, vy šetříte čas i peníze.

Produkční provoz systému základních registrů byl zahájen v souladu se zákonem č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů a dalšími souvisejícími právními předpisy vztahujícími se k problematice základních registrů, dnem 1. 7. 2012. Tímto datem byl neodvratně zahájen dlouhodobý a v některých procesech i trvalý proces zefektivnění veřejné správy.

Jakým způsobem se získávají údaje ze základních registrů?

Orgán veřejné moci získává referenční údaje, tj. právně závazné údaje ze základních registrů prostřednictvím svých agendových informačních systémů⁷.

- orgán veřejné moci se prostřednictvím svého agendového informačního systému připojí k Informačnímu systému základních registrů;
- následuje proces ověření oprávnění dotazu prostřednictvím Registru práv a povinností, tzn., zda je agendový informační systém zaregistrován, zda má daný úředník na daném úřadě právo dotazovat se na předmětné údaje obsažené v příslušném základním registru;
- jestliže je vše v pořádku, následuje zpracování vlastního dotazu prostřednictvím základních registrů a následuje žádaná odpověď, kterou je možno zasílat také do datových schránek.

Jedná se o zjednodušení komunikace občana s úřady a mezi úřady navzájem, ale i o zefektivnění práce úředníka. Ten pro svou práci bezesporu potřebuje informace, které často získává či získával mnoha různými cestami. Nyní existuje model, který umožňuje získání těchto informací pomocí jednoho jediného dotazu.

⁷ AIS – Informační systém veřejné správy, který slouží k výkonu agendy.

Ocenit fungování základních registrů by však měli především občané a podnikatelé, neboť mohou mnohem rychleji vyřizovat na úřadech své požadavky, nemusí opakovaně vyplňovat své identifikační údaje a zároveň mají přehled o údajích, které o nich vede stát. Tyto údaje jsou v rámci státní správy a samosprávy sdíleny. Data jsou uložena na jednom místě, ze kterého se jakékoliv změny automaticky aktualizují do ostatních systémů. Ačkoliv se komerčním subjektům údaje automaticky neposkytují, občané mají možnost na základě žádosti poskytnout souhlas s poskytováním údajů i jiným fyzickým nebo právnickým osobám. V takovém případě se například změna trvalého pobytu promítne kromě systémů státní správy a samosprávy již druhý den také do informačních systémů komerčních subjektů (banka, spořitelna, dodavatel plynu, elektrické energie, vody atd.), které určil sám občan. Zajímavým přínosem základních registrů je také povinnost státu informovat občana a podnikatele o všech skutečných přístupech k jejich údajům v základních registrech.

2. Ostrý provoz systému základních registrů byl spuštěn 1. 7. 2012. Jsou to již více než dva roky, co základní registry slouží orgánům veřejné moci a dalším subjektům a ulehčují tím fungování veřejné správy. Jak byste shrnul toto období fungování základních registrů v hlavních bodech?

Vzhledem k tomu, že se jedná o 6 projektů spojených do jednoho řešení, které nejen funguje, ale je hlavním dodavatelem referenčních dat pro stát, lze říct pouze to, že stát umí koordinovat, řídit a dokončit projekty 6 ti dodavateli a spustit v jednom dni. Hlava eGovu Ondřej Felix si zaslouží nejen ocenění digitálního šampiona, ale projektového leadera, díky němuž jsme na popředí rozvoje eGovu v EU a možná i na světě.

Od počátečních nesmělých krůčků udělal systém základních registrů velký pokrok – to je nakonec jasné i ze stručné rekapitulace současného stavu provozu systému základních registrů:

Po 32 měsících provozu, tedy ke dni 28. 2. 2015, Správa základních registrů eviduje **2 761 orgánů veřejné moci**, které požádaly o připojení **3 895 agendových informačních systémů**.

Základní registry v současné době využívá **aktivně 2 526 OVM**, které za 32 měsíců provozu uskutečnily celkem přes **550 milionu transakcí**.

V informačním systému o informačních systémech veřejné správy zaregistrovalo k 28. 2. 2015 alespoň jeden svůj AIS celkem 3 273 OVM.

Všechna klíčová OVM jsou připojena k základním registrům, spolupracují se ZR a čerpají aktuální změny z registrů. Připojeny jsou např. krajské úřady, všechna statutární města. Kromě Ministerstva zahraničních věcí, které přistupují výhradně přes Czech POINT, jsou připojena všechna ministerstva.

V současné době všech 7 zdravotních pojišťoven v České republice pravidelně využívá údaje ze základních registrů.

To nejsou jen čísla, ale garantovaný rychlý přístup k ověřeným datům o občanech, podnikatelích, adresách, budovách atd., která sdílí pomocí služeb celá státní správa a samospráva.

3. Jaké jsou současné priority Správy základních registrů v dalším rozvoji eGovernmentu?

Po více než ročním provozu se SZR soustřeďuje na zefektivnění vlastních procesů pro plnění zákona č. 111/2009 Sb., o základních registrech, certifikace řízení IT a bezpečnosti a implementace vlastních řešení podporu státní správy v oblasti všech základních registrů. V návaznosti na strategii 2014+ se budeme soustředit primárně na vytěžování dat ze ZR formou implementace nových služeb, jako jsou nové AISY, podpora voleb a vydávání dat formou volebních seznamů ze ZR, dynamické formuláře a služby pro jiné osoby neboli třetí strany, kde očekáváme využití dat tzv. komerční sférou při dodržení současné legislativy.

Dále je nutné se soustředit na zaručenou a bezpečnou komunikaci občana se státem, ať to bude využitím technologií občanských průkazů a ztotožnění občana místo vyplňování formulářů, soustředění na zdravotnictví, veřejnou správu ve formě správních a daňových řízení, nebo správu majetkových hodnot státu.

V neposlední řadě bych zmínil O. Felixem uvedenou digitalizaci datových fondů a jejich napojení na služby ZR, neboť ZR vedou pouze aktuální referenční data a většina služeb si vyžaduje data historická, i když platná, nebo vazby na jiný druh informací.

4. Co se SZR v posledních měsících podařilo?

- **Návrh novely zákona č. 111/2009 Sb., o základních registrech**

Na MV ČR proběhlo vnitrorezortní připomínkové řízení k návrhu novely zákona o základních registrech, ve kterém SZR uplatňovala připomínky.

- **Volební seznamy**

SZR se podílela na zajištění funkcionality výdeje seznamu voličů v členění podle volebních okrsků, které byly využity k volbám konaným ve dnech 10.–11. 10. 2014. Z pohledu stávajících projektů jde o novou službu, která přináší zefektivnění fungování veřejné správy v procesu přípravy voleb pro jednotlivé volební obvody.

- **Kompozitní služby**

V souvislosti s úpravou kompozitních služeb a jejich vystavením na produkčním prostředí bude docházet k řízenému ukončování souběhu používání starých (E159 a E160) a nových (E171 a E172) kompozitních služeb. Podle informace MV ČR je předpokládáno pozastavení přímého přístupu do AISEO nejpozději ke dni 30. 6. 2015.

- **Tzv. „změnové sestavy“**

Na produkční prostředí byl nasazen změnový požadavek na zkrácení lhůty ke zpracování tzv. změnových sestav z dosavadních 15 kalendářních dní na 4 kalendářní dny.

- **Získání certifikátu**

SZR získala atest referenčního rozhraní informačního systému veřejné správy "ISZR - Informační systém základních registrů". Posuzovanými hledisky byly předání údajů o dostupnosti ISVS do IS o ISVS, soulad datových prvků vazeb s datovými prvky v informačním systému datových prvků a soulad realizace vazeb s technickou dokumentací služeb.

- **Návod pro občana**

SZR ve spolupráci s MV ČR připravila návod pro občana k problematice změny adresy trvalého pobytu. Návod popisuje, kam je v současné době třeba tuto změnu (ne)hlásit. Návod je k dispozici zde: <http://www.szrcr.cz/akce>.

5. Jaké velké projekty se v oblasti základních registrů plánují?

Uvedení ZR do provozu představuje pro ZR pouze první krok v oblasti elektronizace státní správy. K velkým výzvám, které jsou před SZR a základní registry stavěny patří především další a ještě širší integrace ZR do komunikační infrastruktury, která dovolí komunikovat prakticky všem AIS nejen se ZR, ale i mezi sebou. Znamená to mimo jiné rozšiřování počtu AIS, které budou publikovat nereferenční údaje.

Prvotní úkol ZR spočíval v technologickém propojení a poskytování dat. Dalším krokem je zkvalitňování a rozšiřování poskytovaných služeb tak, aby byly dostupné co největšímu počtu orgánů veřejné moci s co nejmenšími náklady. Pro zajištění tohoto úkolu připravujeme nový systém, který umožní uvést nové služby, zjednoduší implementaci služeb nových a nabídne nové, veřejné informace, které budou dostupné široké veřejnosti i komerčním subjektům. Jedná se o data, která jsou v různých formách dostupná již dnes, ale nejsou poskytována centralizovaně a ve formě, přístupné pro integraci na úrovni aplikací.

Zajištění sdílení referenčních dat se netýká jen České republiky. V současnosti probíhá na úrovni EU příprava regulace v oblasti digitální identity a výměny údajů mezi členskými státy EU. SZR musí zajistit, aby ZR podporovaly tyto požadavky a byly schopny zajistit plnění nařízení EU.

Poskytování informací ze ZR není omezeno pouze na orgány veřejné moci – pokud se občan rozhodne, může zavázat ZR poskytovat jeho vybrané údaje komerčním subjektům. V této oblasti bude ZR dále zkvalitňovat a rozvíjet již poskytované služby.

ZR představují úhelný kámen systémů poskytujících data. Je proto nezbytné zajistit, aby služby ZR byly dostupné bez výpadku, 24 hodin denně, 365 dní v roce. Další oblastí v rozvoji ZR je další automatizace řízení přístupů ke službám ZR. Jedná se také o zvyšování automatizace zajištění bezvýpadkového provozu a monitoringu provozu ZR tak, aby byla zajištěna maximální dostupnost a bezpečnost služeb, prostřednictvím kterých jsou data ze ZR poskytována.

Primárním cílem SZR je splnit všechny úkoly, které jsou na ZR kladeny českou i evropskou legislativou a to s maximálním důrazem na hospodárné využití svěřených prostředků. Cestou k tomu je především automatizace, na kterou se SZR orientuje ve všech směrech rozvoje ZR.

Transparentní úřad

Tomáš Pitrocha, obec Domašov; Mgr. Tomáš Lechner, Ph.D., Triada, spol. s r. o.

Úvod

Strategický rámec rozvoje veřejné správy České republiky pro období 2014 – 2020 obsahuje mimo jiné cíl č. 3 „Zvýšení dostupnosti a transparentnosti veřejné správy prostřednictvím nástrojů e-Governmentu“. Tento strategický cíl obsahuje celou řadu související opatření a aktivit, mezi kterými je například koncepční zajištění fungování e-Governmentu a realizace projektů ICT anebo rozšíření, propojení a konsolidace datového fondu veřejné správy a jeho efektivní a bezpečné využívání dle jednotlivých agend i na principu open-data. Souhrnně lze říci, že je v rámci uvedeného cíle kladen důraz na využití stávajících nástrojů, mezi kterými jsou jmenovány datové schránky, síť kontaktních míst veřejné správy Czech PONT anebo základní registry, dále je kladen důraz na prohloubení otevřenosti a transparentnosti veřejné správy, a to zejména prosazováním principu open-data, a významné soustředění na realizaci bezpečnostních opatření v souladu se zákonem o kybernetické bezpečnosti.

Potenciál elektronických nástrojů pro zvýšení transparentnosti mohou úspěšně využívat i města a obce, a to bez ohledu na jejich velikost. V tomto příspěvku si ukážeme příklad menší obce, která úspěšně realizovala celou řadu lokálních elektronických nástrojů i vhodným efektivním způsobem využívá centrální nástroje e-Governmentu.

Obec Domašov

Obec Domašov leží 25 km severozápadně od Brna v mírném údolí náhorní plošiny na pokraji Českomoravské vrchoviny. Nejstarší zmínka o Domašově pochází z roku 1048 z tzv. darovací listiny Břetislava I., který původní statek věnoval klášteru Rajhradskému. Obec se nacházela poblíže císařské silnice, nyní silnice č. II/602.



Obr. 1: Letecký pohled na Obec Domašov.

V současné době má obec něco přes 600 obyvatel a 225 čísel popisných. V obci se nachází základní škola pro první stupeň, kterou navštěvují i děti z Říček, Javůrku, Litostrova a Rudky, i mateřská škola, v budově obecního úřadu je obecní knihovna, vybudované zdravotní středisko je obsazeno pouze zubní lékařkou

a pediatrickou poradnou, v obci je dále pobočka České pošty, soukromá prodejna potravin, cukrárna a tři restaurace. V obci úspěšně působí sbor dobrovolných hasičů. Dále je obec součástí DSO Domašovsko, které spojuje obce Domašov, Rudka, Říčky, Javůrek a Litostrov za primárním účelem zásobování obcí pitnou vodou a provozování společné ČOV k čištění odpadních vod. Obec je také součástí mikroregionu Domašovsko. Více informací o obci lze najít na jejich oficiálních webových stránkách dostupných na adrese <<http://obec.domasov.net/>>.

Obec má jedenáctičlenné zastupitelstvo, v čele obce stojí starosta Tomáš Pitrocha. Je zřízen finanční, kontrolní a kulturně-sportovní výbor. Obecní úřad Domašov tvoří starosta, místostarosta a samostatný referent.

Zvýšení transparentnosti prostřednictvím portálu iMunis.cz

Centrum sdílených služeb portálu iMunis.cz nabízí celou řadu zabezpečených služeb, z nichž některé slouží k zajištění povinných elektronických služeb, jako je třeba zveřejnění obsahu úřední desky způsobem umožňujícím dálkový přístup podle § 26 zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů, a některé jsou vítaným rozšířením služeb pro občany v rámci plnění funkce obce jako územně samosprávného celku, jako je např. služba iMunis SMiS anebo Rozklikávací rozpočet. Celkovou nabídku služeb portálu iMunis.cz ilustruje Obr. 2. Tyto služby jsou koncipovány tak, že zachovávají maximální bezpečnost ukládaných dat vzhledem k jednotlivým uživatelům. Portál iMunis.cz je provozován v režimu 7x24. Podstatný je také fakt, že datové centrum leží v České republice a jeho provoz tedy plně podléhá českému právnímu řádu. Uživatelé se tak v žádném případě nemusí bát o svá data, jejichž zabezpečení je na velmi vysoké úrovni.

Triada | Munis | iMunis | ISSS | DMO | Obec a finance | DVS | Solón

iMunis Centrum sdílených služeb

Úřední deska SMIS Evidence oznámení Webináře HelpDesk Rozklikávací rozpočet

Hlavní nabídka

O iMunis

- Úvod
- Přihlásit**
- Kontakt

Služby iMunis

- Úřední deska
- iMunis SMIS
- Evidence oznámení
- Webináře
- Helpdesk Munis
- Rozklikávací rozpočet

Další aktivity

Software

- Munis
- Solón

Konference

- ISSS
- Den malých obcí

Vydavatelství

- Obec a finance
- Deník veřejné správy
- Solón

iMunis – Úvod

Centrum sdílených služeb řešených přes portál iMunis.cz umožňuje sdílet a tím pádem i šetřit náklady na plnění povinností vyplývajících z legislativy. Služby jsou koncipovány tak, že zachovávají maximální bezpečnost ukládaných dat vzhledem k jednotlivým uživatelům. Přístup ke službám je buď přímo prostřednictvím webového klienta, nebo pomocí webových služeb, na které jsou navázány vnitřní informační systémy úřadu.

- Úřední deska** – zveřejnění obsahu úřední desky způsobem umožňujícím dálkový přístup podle § 26 zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů.
- SMIS** – hromadné rozesílání SMS zpráv prostřednictvím internetu. Okamžité a hromadné zaslání zpráv, které mohou být určeny různým okruhům příjemců a to podle charakteru informace. Tato služba je úspěšně provozována již více než dva roky.
- Evidence oznámení** – řešení povinností podle zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů.
- Webináře** – moderní a interaktivní forma seminářů probíhající pomocí internetu.
- HelpDesk Munis** – technická podpora pro uživatele IS Munis.
- Rozklikávací rozpočet** – jednoduchá a srozumitelná prezentace hospodaření měst, obcí a dobrovolných svazků obcí na internetu

ISSS

- ISSS 2015 – přípravy vrcholí
- ISSS 2015 – osmnáctý ročník renomované konference

IS Munis

- Vyhlášení výsledků soutěže o 3 tablety Lenovo IdeaTab
- Pomáháme tvořit Důvěryhodný úřad
- Rozklikávací rozpočet**
- Novinky v IS Munis verze 3.22
- Proběhlo pravidelné školení našich partnerů
- Setkání uživatelů IS Munis na konferenci ISSS

TRIADA

Kontakt © 2015 Triada, spol. s r. o., Praha, webmaster@imunis.cz

Obr. 2: Úvodní obrazovka portálu iMunis.cz s přehledem nabízených služeb.

Obec Domašov využívá služeb portálu iMunis.cz v návaznosti na vnitřní informační systém Munis, který pokrývá většinu agend vedených městskými a obecními úřady. Ze služeb, které obec Domašov využívá, si zde popíšeme dvě, a to Úřední desku a Rozklikávací rozpočet.

Jak již bylo zmíněno, služba Úřední deska slouží pro zajištění zveřejnění obsahu úřední desky způsobem umožňujícím dálkový přístup podle správního řádu. Tato služba je napojena na vnitřní modul IS Munis – Úřední deska, který zajišťuje evidenci úřední desky a přípravu podkladů pro vyvěšení včetně převodu jednotlivých dokumentů do formátu PDF. Data jsou dávkově synchronizována na portál iMunis.cz, což minimalizuje nároky na připojení a optimalizuje celý proces. Data jsou uložena v datovém skladu zmíněného portálu, z nichž pak probíhá odpovídající zveřejnění. Ukázka zveřejněného obsahu pro Obec Domašov je na Obr. 3.

Obec

Úřední deska – Stav k 3. 3. 2015 11:00:04

[Aktuální úřední deska](#), [Vyhledávání](#), [Stav k datu](#), [Domácí stránka](#)
[RSS](#), [Acrobat Reader](#)

Nalezeny 3 záznamy. Poslední změna: 2.3.2015 20:34:35

Název	Značka	Typ	Původce	Zveřejněno od	Zveřejnit do	Rozh. dat. od	Dokumenty
Usnesení 6. zasedání ZO Domašov	UZ 6/2015	Usnes. Zastupitelstva	Obec	2.3.2015	19.3.2015	2.3.2015	dokument PDF (0,7 MB)
Výroční zpráva o poskytování informací za rok 2014	VZ 2014	Dokumenty	Obec	27.2.2015	16.3.2015	27.2.2015	dokument PDF (327 kB)
Oznámení o výkonu topografických prací - aktualizace ZABAGED v roce 2015	ZÚ-00453/2015-13600	Oznámení	Zeměměřický úřad	22.2.2015	22.3.2015	22.2.2015	dokument PDF (1 MB)

Upozornění: Zveřejněna jsou pouze vyvěšení od 1. 1. 2006, tj. od účinnosti zákona č. 500/2004 Sb. (správní řád). [Prohlášení o přístupnosti](#)
iMunis eDeska © 2006 Triada, spol. s r. o.

Obr. 3: Úřední deska obce Domašov – stav k 3.3.2015.

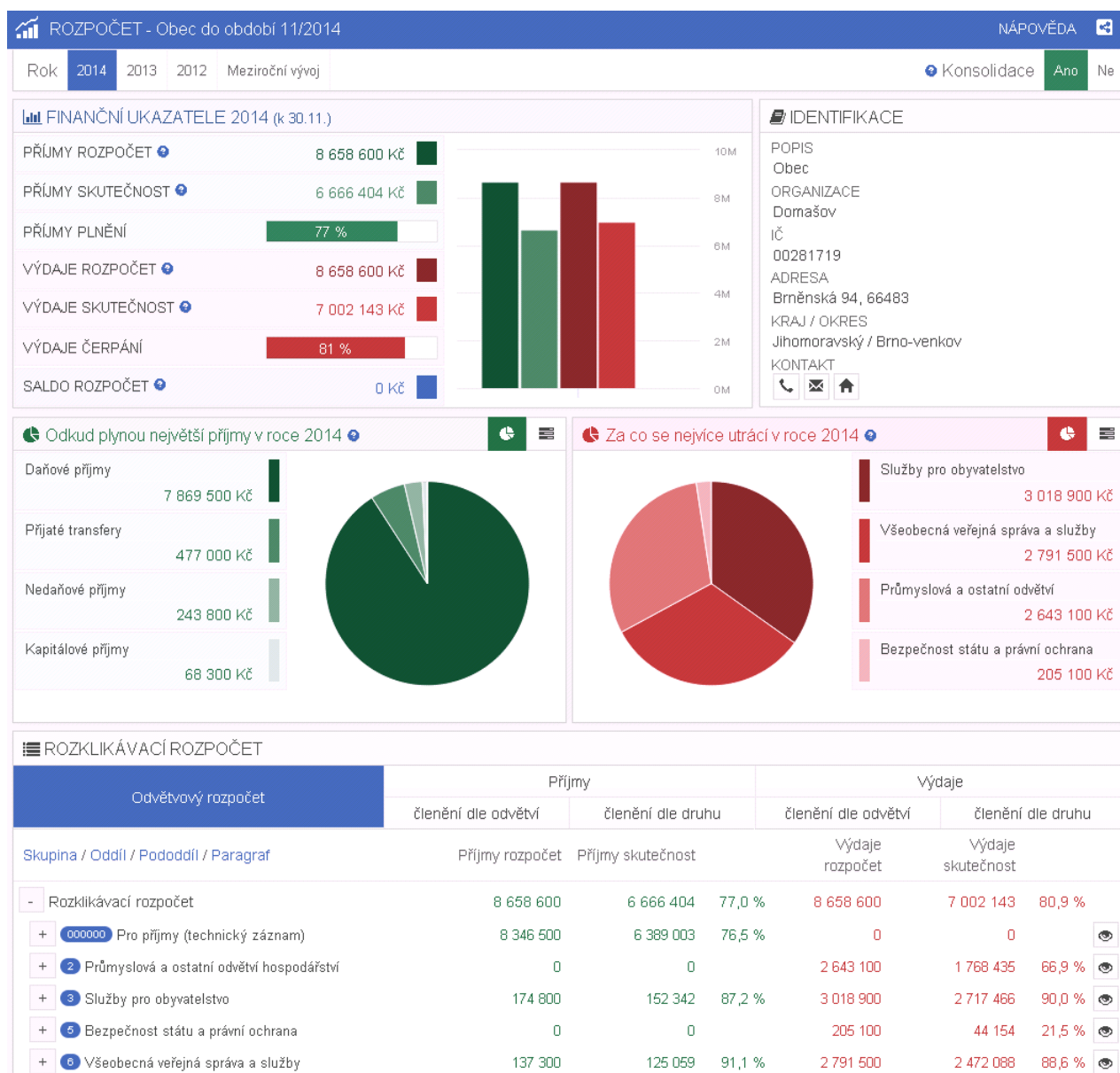
Další službou, kterou obec Domašov využívá, je Rozklikávací rozpočet, což je služba, pomocí které lze jednoduše a srozumitelně prezentovat hospodaření měst, obcí a dobrovolných svazků obcí na internetu. Je třeba zmínit, že tato forma prezentace rozpočtu a jeho čerpání a plnění není vyžadována zákony, ale je významným přínosem k posílení transparentnosti a otevřenosti obce. Tuto pozitivní a moderní cestu tedy obec Domašov zvolila a začala svým občanům nabízet velmi podrobný přehled o svém hospodaření. Ukázka Rozklikávacího rozpočtu obce Domašov je na Obr. 4.

Z pohledu občana je vždy důležité, aby zveřejňované informace byly přehledné, srozumitelné a úplné. Přehlednost je v rámci Rozklikávacího rozpočtu zajištěna jednak vlastním rozklikáváním, kdy si občan může zvolit požadovanou podrobnost prezentovaných informací, a jednak množstvím grafických ztvárnění, která skutečnost prezentují mnohem jasnějším způsobem než obyčejná čísla. Pokud si občan vybere konkrétní část rozpočtu, může vidět průběh rozpočtových změn a plnění či čerpání během jednotlivých měsíců roku. Dalším pohledem je meziroční srovnání. Samozřejmě, že tato meziroční porovnání mohou být zkreslena změnou metodiky účtování v jednotlivých letech, o čemž je ale občan v rámci Rozklikávacího rozpočtu náležitě informován.

Dostáváme se tím k druhé důležité vlastnosti Rozklikávacího rozpočtu pro občana, kterou je zmíněná srozumitelnost. Podle zákona je rozpočet členěn v třídění podle rozpočtové skladby, která obsahuje položky (druhé členění) a paragrafy (odvětvové členění). Toto členění však nebývá pro laickou veřejnost srozumitelné, což Rozklikávací rozpočet portálu iMunis.cz řeší způsobem, který nezatěžuje konkrétní obce a nenutí je připravovat různé specifické převodové můstky. Celé řešení se postaveno na tom, že umožňuje kromě přesného rozpočtového členění na třídy, seskupení položek, podseskupení položek a jednotlivé položky dle druhového členění, a na skupiny, oddíly, pododdíly a paragrafy dle odvětvového členění, také členění kombinovaná, které vhodným způsobem propojují oba pohledy a přináší pro občana srozumitelnější a přístupnější

ší výsledky. Jde zejména o tzv. Odvětvový rozpočet, který je členěný dle oblastí s přehledným zobrazením příjmů a výdajů na jednom místě. Navíc jsou všechny pohledy i části druhového a odvětvového členění komentovány, aby občan lépe rozuměl jejich významu.

Poslední z výše uvedených podstatných vlastností Rozklikávacího rozpočtu pro občany je úplnost, která významným způsobem souvisí též s aktuálností dat. Zajištěna je tím, že datová základna pro zveřejňování rozpočtu v nabízeném produktu je získávána z úplných měsíčních výstupů přenášných do datového skladu portálu iMunis.cz dávkovým způsobem. Nejde tedy o žádné specifické výběry dat, jejichž sestavování by mohlo být zatíženo chybou vedoucí k neúplnosti prezentovaných informací. Údaje zveřejněné prostřednictvím Rozklikávacího rozpočtu jsou stejně přesné a úplné, jako údaje uvnitř účetního informačního systému obce.



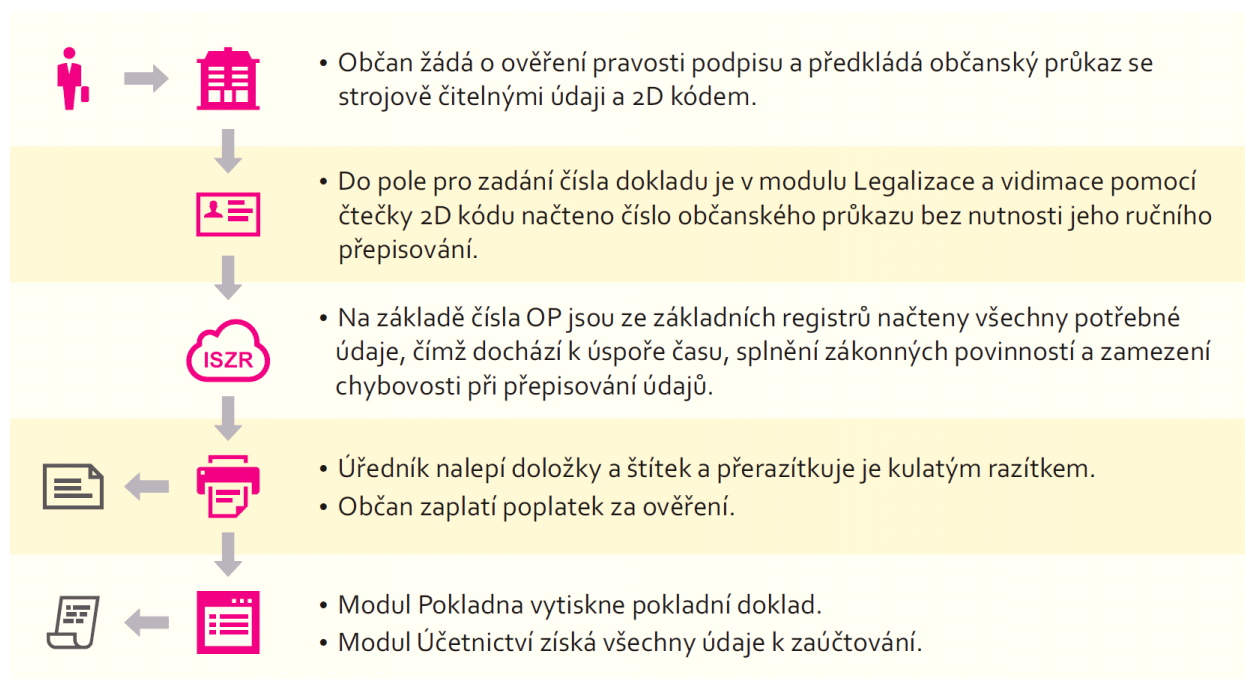
Obr. 4: Rozklikávací rozpočet obce Domašov, stav k 3. 3. 2015.

Prohlubování využití stávajících nástrojů e-Governmentu

Jak bylo zmíněno v úvodu, počítá Strategický rámec rozvoje veřejné správy České republiky pro období 2014 – 2020 s prohlubováním využití stávajících nástrojů, mezi kterými jsou jmenovány datové schránky, síť kontaktních míst veřejné správy Czech PONT anebo základní registry. Soustředíme se nyní na nejmladší z těchto nástrojů, kde lze asi globálně identifikovat největší dosud nevyužitý potenciál.

Základní registry poskytují referenční údaje, jejichž využití musí být též transparentní, což primárně znamená zdůvodněné. Tedy úředník smí tato data využívat jen v oprávněných případech, na druhou stranu však je nesmí ani přehlížet. Jinými slovy, referenční údaje je třeba v oprávněných případech použít, avšak stanovení těchto případů nemusí být zcela jednoduché a vychází z procesů, z nichž se skládá výkon jednotlivých agend. Tyto agendy jsou zaevidovány v Registru práv a povinností, jednom z čtyř základních registrů veřejné správy.

Procesní pohled na výkon agend je poměrně novou a moderní záležitostí, která umožňuje identifikovat slabá místa, kde by bylo třeba proces upravit, aby bylo dosaženo vyšší efektivity výkonu dané agendy. Vhodné využití referenčních údajů může být právě takovou úpravou, pokud je podloženo přímou vazbou z daného informačního systému využívaného pro podporu výkonu dané agendy. Jako příklad, lze uvést proces legalizace (ověřování pravosti podpisu) podle zákona č. 21/2006 Sb., o ověřování shody opisu nebo kopie s listinou a o ověřování pravosti podpisu a o změně některých zákonů (zákon o ověřování), ve znění pozdějších předpisů. V rámci informačního systému Munis slouží pro podporu tohoto procesu modul Legalizace a vidimace, který umožňuje tisk ověřovací doložky na štítky a vytvoření záznamu pro ověřovací knihu. Při využití tohoto modulu dochází k výraznému zvýšení efektivity poskytování služeb legalizace a vidimace, a to zejména díky možnosti opakovaných tisků doložek při jednorázovém ověřování více kopií nebo legalizaci více podpisů, dále díky možnosti využití jednou zadaných údajů při opakovaném ověřování a v neposlední řadě právě také díky vazbě na základní registry veřejné správy. Zjednodušení daného procesu ukazuje přehledně schéma na Obr. 5.



Obr. 5: Schéma procesu legalizace s využitím podpory vazby na základní registry.

Kromě vazby na základní registry je výhodou modulu Legalizace a vidimace informačního systému Munis jeho provázanost (volitelná) s dalšími moduly IS Munis jako je Pokladna a Účetnictví, což umožňuje

automatickou tvorbu příjmových pokladních dokladů, jejich tisk a následné automatické zaúčtování přijatého poplatku do účetnictví. Obec Domašov úspěšně využívá všechny tyto vazby, což znamená významnou úsporu času při celkové realizaci legalizace či vidimace.

Závěr

Informační systém Munis je vhodným nástrojem pro zvýšení efektivity výkonu agend vedených na městských a obecních úřadech. Jeho vazby na centrální nástroje e-Governmentu, jako je informační systém datových schránek, aplikace CzechPOINT anebo základní registry veřejné správy, jsou realizovány s důrazem na optimalizaci procesů, která je potřebná pro všechny velikostní kategorie obcí, avšak pro malé obce, kde je vysoká kumulace funkcí, je přímo nutností.

Vazbou vnitřního IS Munis se službami portálu iMunis.cz lze dosáhnout významného zvýšení transparentnosti a otevřenosti obce, čehož využila i obec Domašov. Nejnovějším počinem obce Domašov v této oblasti je využití služby Rozklikávací rozpočet, která zajišťuje jednoduchý a z hlediska správy nenáročný způsob zveřejňování hospodaření obce v přehledné grafické podobě.

Obec Domašov využívá informační systém Munis od společnosti Triada již dlouhá léta a pracujeme téměř se všemi jeho moduly. Úspěšnost užití je zvyšována prováděnými školeními, výbornou spoluprací s přidělenou správkyní ing. Barborou Mertovou a p. Vladanem Vlkem i pružnou reakcí na změny zákonů i na naše požadavky. Všem obcím můžeme tento informační systém i jeho nadstavbové funkce realizované prostřednictvím portálu iMunis.cz plně doporučit.

V elektronizaci, a tedy i bezpečnosti, medikačního procesu za Evropou zaostáváme

Ing. Simona Plischke, výkonná ředitelka, HC Logic, s. r. o.

Pochybení v podávání léků a celková neefektivita medikačního procesu mají mnohem větší rozměr, než si připouštíme. V českých zdravotnických zařízeních se proces medikace, na rozdíl od jiných procesů v nemocnici, za posledních několik desetiletí příliš neinovoval. Na poli bezpečnosti a efektivity tak máme co dohánět. Jakým směrem se v oblasti elektronizace medikačního procesu ubírají nejen vyspělejší země, ale i naši stře-do evropští sousedé?

Ordinace a podávání léků jsou vůbec nejčastější proces, který se v nemocnicích odehrává. Ačkoli jde o proces relativně jednoduchý, je považován za nejrizikovější proces v nemocnicích, protože pochybení během preskripce, přípravy a podávání léků patří k těm nejčastějším. Běžně nemocnice s např. 500 lůžky podá přes 1 600 000 léků za rok (při průměrných 9 lécích podaných pacientovi za den). Množství a typologii chyb, kterých se přitom dopouští, ovšem často ani nesleduje. I při správnosti podávání léků na úrovni 99,9 % by přitom v takové nemocnici došlo za rok k 1 643 medikačním chybám; 99,9% spolehlivost je ale ve stávajících podmínkách českých nemocnic nedosažitelná, mnohem reálnější je tak spolehlivost na úrovni 95 %. Při té se ale v uvedeném případě nemocnice dopouští ročně více než 82 000 medikačních chyb.

Podle Evropská asociace nemocničních lékárníků (EAHP) vzniká 39 % pochybení již při preskripci léku lékařem, 23 % v procesu logistiky a přípravy, tedy v lékárně či na odděleních, a zbývajících 38 % při podání léku sestrou. Ačkoli většina chyb v medikaci nezpůsobí pacientovi nežádoucí účinek, některá pochybení znamenají nejen zhoršení pacientova stavu, ale pro nemocnici také dodatečné náklady na jeho léčení. Tyto náklady přitom nejsou malé. Naopak, dosahují i několika desítek miliónů korun ročně, podle velikosti nemocnice.

Medikační chyby společenskou pozornost příliš nevzbuzují

Přestože zájem o pochybení ve zdravotnictví postupně narůstá, a to i díky mediálním kauzám posledních několika let, je v porovnání s oblastmi s vysokou mírou rizika stále výrazně menší. Zatímco v letecké dopravě, chemickém průmyslu či jaderné energetice dochází při neštěstí k hromadným ztrátám na životech a rozsáhlým majetkovým škodám, chyby ve zdravotnictví se týkají jednotlivců. Společenskou a politickou pozornost proto příliš nevzbuzují. To ovšem neznamená, že nejsou závažné a už vůbec ne, že se nedějí.

V českých nemocnicích se medikační proces v uplynulých desetiletích zásadněji neinovoval – uplatňuje se stále stejná manuální příprava léků decentralizovaná na odděleních. Oproti klinické části nemocnic, ústavní lékárny nevyužívají technologie běžné ve světě, jen zřídka je do medikačního procesu zapojen klinický farmaceut, aby dohlédl na správnost preskripce ze strany lékaře, možnosti ověřit správnost podání jsou limitované.

Příliš mnoho času sester je stráveno rutinními úkoly souvisejícími se správou lékové zásoby (objednávání, přejímka, popisování a přelepování krabiček, přerovnávání balení apod.), přesto je skutečný objem a stav zásob léků na odděleních obvykle „velká neznámá“. Zpravidla neexistuje jakákoli forma evidence léků nacházejících se mimo ústavní lékárnu, protože kliniky skladovou evidenci nevedou, a to ani v „papírové“ podobě. Léky na odděleních, kterým hrozí expirace, se nabízejí v rámci vnitřní neoficiální „burzy“ jiným oddělením, např. e-mailem mezi sestrami. Tyto léky pak nelze z důvodu jejich netransparentního pohybu správně záúčtovat, a vykázat tak reálné náklady na léčbu daného pacienta.

Skutečná chybovost v medikaci se nesleduje, a tudíž nevyhodnocuje – chybám proto nelze bez změny systému ani příliš předcházet. Nezanedbatelným faktorem zvyšujícím rizikovost procesu je fakt, že sestry jsou v průběhu přípravy a podávání léků vyrušovány jinými pacienty či návštěvami pacientů, spěchají a po dlouhých směnách bývají unavené.

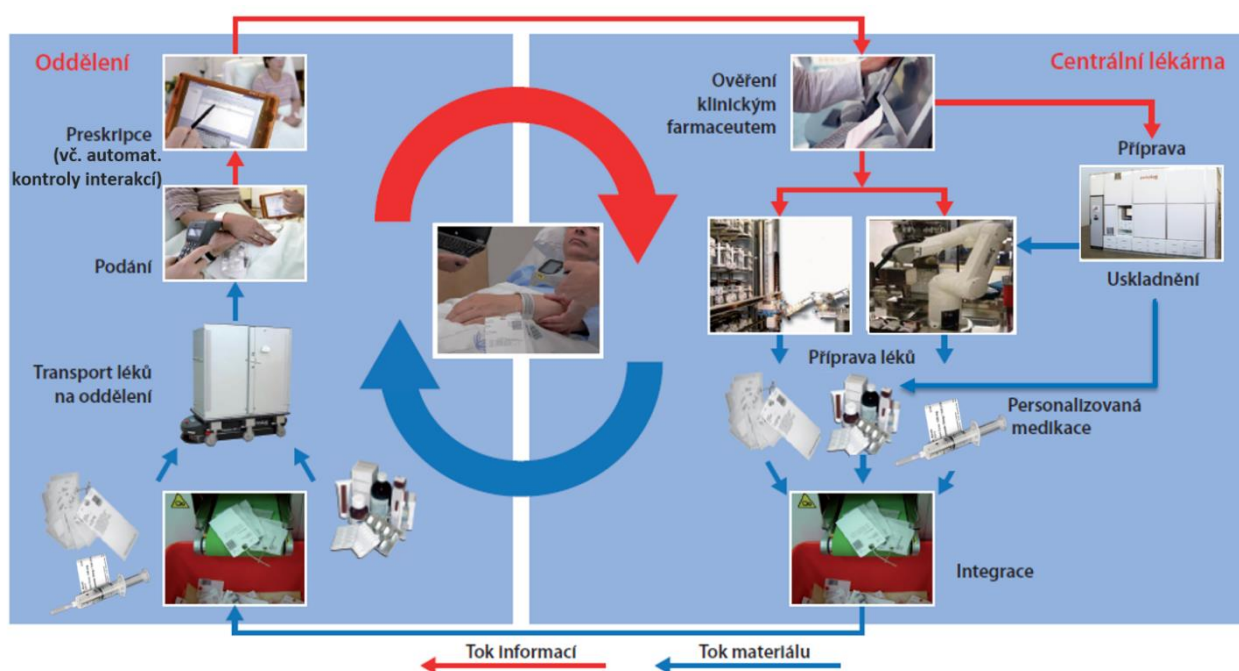
Medikační proces hodný 21. století

Bezpečnost procesu podávání léků se zvyšuje se zavedením nových technologií a inovativních přístupů. Ve vyspělých zemích je současnou nejbezpečnější a nejefektivnější praxí automatizovaný centralizovaný systém přípravy léků s využitím jednodávkových balení opatřených čárovým kódem. Právě využití čárových kódů na jednodávkách léků má z hlediska zvýšení bezpečnosti i celkové efektivity největší dopad. Omezení chybovosti touto cestou potvrdily mnohé studie – např. bostonská nemocnice Brigham and Women's udává snížení počtu chyb v síle léků o 41 %, pokles výskytu nežádoucích dopadů těchto chyb o 51 % a redukci chyb v čase podávání o 27 %. K vyznačování čárových kódů na jednodávkách léků nabádá i EAHP, podle té lze touto změnou snížit chybovost v medikaci o 41,4 %.

Základním celosvětově platným pravidlem v oblasti podávání léků je dodržení sedmi zásad: (1) správnému pacientovi je podán (2) správný lék, a to ve (3) správné dávce, ve (4) správný čas a (5) správným způsobem. Současně je o všem vedena (6) správná dokumentace a pacient dostane (7) správné informace o léku. Automatizovaná příprava jednodávek centralizovaná v ústavní lékárně v kombinaci s využitím softwarové kontroly interakcí léků při jejich preskripci lékařem a elektronické verifikace čárového kódu léku i pacienta před podáním u lůžka znamená maximální zvýšení bezpečnosti pacienta, a tedy splnění těchto zásad beze zbytku.

Takto inovovaný medikační proces tvoří uzavřený cyklus (viz obr.) a díky elektronizaci na všech jeho úrovních je integrován s procesem distribuce a správy léků.

Obr. Schéma bezpečného a efektivního medikačního procesu



Ve zkratce vypadá následovně: Lékař při elektronické preskripci využívá software na kontrolu interakcí léků. Klinický farmaceut ordinaci ověří, případně zkoriguje. V ústavní lékárně jsou léky roboticky přebaleny do sáčků obsahujících jednodávku konkrétního léku, na kterých je vytištěn čárový kód a další potřebné informace o léku (název léku, účinná látka, jeho síla, číslo šarže, datum expirace atd.). Systém přebaluje léky různých forem (tablety, ampulky, předplněné stříkačky, čípky apod.). Jednodávky jsou automaticky umístěny ve skladové části systému, přičemž velikost zásoby léků je elektronicky kontrolována na úrovni 5denní potřeby nemocnice. Robot z této zásoby pak podle preskripce lékaře připravuje „balíčky“ jednodávek léků pro jednotlivé pacienty na následujících 12–24 hodin. Sestry ve správnou dobu takto připravené léky podávají a skenují přitom kód pacienta i kód jednodávky.

Nepoužité léky oddělení vracejí do nemocniční lékárny, kde robot každou vrácenou jednodávku po nactení jejího čárového kódu navrátí na původní místo ve svém skladovacím prostoru a použije pro přípravu další terapie. Systém automaticky kontroluje zásobu léků (hlásí potřebu doplnění), expirační dobu léků (vybírání vždy starší léky před novějšími, případně prošlé léky vyřazuje) a zajišťuje celkovou skladovou evidenci. V každém okamžiku je zřejmé, kolik léků a kde přesně se v nemocnici nachází.

Léková zásoba v příručních skladech na odděleních je též ve formě jednodávek a slouží pro podávání léků při náhlé změně medikace, příjmu pacienta apod. Systém automaticky připravuje dávky pro doplnění těchto příručních skladů, a to podle stanovené velikosti (obvykle 4denní potřeba oddělení), aniž by sestry musely léky objednávat.

Dočkáme se?

Vedle zvýšení bezpečnosti pacienta, které je již samo o sobě pádným argumentem pro změnu, dochází i k úspoře nákladů nemocnice. A to jak díky možnosti snížení nákladů na léky (snížení zásob léků na odděleních, zamezení ztrát léků, jejich expiraci apod.), tak díky celkovému zefektivnění procesu. Množství léků v nemocnici je po logistické stránce optimální a systém řeší také obvykle nevyhovující skladovou evidenci na odděleních. Sestrám tak šetří čas, který tráví nejen přípravou léků, ale i administrací lékových skladů.

Takto pojatý proces medikace je díky elektronizaci na všech jeho úrovních integrován s procesem distribuce a správy léků do jednoho uzavřeného cyklu (viz obr.), který je zcela transparentní až do úrovně každé jednodávky. Řešení může fungovat jak v jednotlivých nemocnicích, tak v síti nemocnic na úrovni celého regionu. V českých nemocnicích zatím implementováno nebylo, ale vzhledem k potřebě zvyšovat bezpečnost a přitom snižovat náklady na zdravotní péči za zvažování rozhodně stojí. Obzvláště, když tato technologická a procesní změna ve stále větší míře proniká i do sousedních postkomunistických zemí.

Fujitsu – když vaše smysly nestačí

*Milan Podivín, Head of Direct Business - Commercial and Public Sector for CZ & SK,
Fujitsu Technology Solutions s.r.o.*

Technologické firmy se dnes snaží, aby jejich produkty byly co nejmenší a aby měly co nejvýkonnější hardware. Nové notebooky, telefony, servery. Každá nová generace jde o kus dál. Fujitsu však myslí i na ty, kterým technologie pomáhá se zapojit do normálního života.

S tím, jak populace západního světa stárne, stává se tento problém čím dál tím víc akutní. Děti už nezvládají péči o své rodiče, kteří tak zůstávají na sklonku života sami. V Japonsku, odkud společnost Fujitsu pochází, je situace ještě složitější, než v Západní Evropě. I proto vznikají nové technologie, jež mají stárnutí usnadnit a lidem v postproduktivním věku život co nejvíce usnadnit.

Jednou z takových novinek je „chytrá“ hůl. Vycházková hůl má zabudovanou satelitní navigaci, a na vrchním LED displeji tak může zobrazovat šipky, které dovedou uživatele k cíli. Kromě toho je však navržena i tak, aby monitorovala srdeční tep a teplotu. Hůl je možné připojit online a sledovat její pohyb pomocí GPS, 3G, nebo wi-fi. Pokud je například nutná změna směru, hůl zavibruje a objeví se směrová šipka.

Pohyb vycházkové hole je možné sledovat online a systém umí vysílat upozornění, pokud se domnívá, že uživatel mohl třeba spadnout. Fujitsu se touto cestou snaží pomoci seniorům zůstat mobilní co nejdéle. Tím pádem mohou dále zůstat součástí společnosti a třeba si i najít práci.

Ačkoliv je navržena, aby pomáhala starším lidem, je možné jí dát do ruky komukoli, kdo je nějakým způsobem zranitelný. Hůl posílá do hostitelského počítače zpět data, takže pečující osoba může v reálném čase sledovat pohyb uživatele a vyžádat si například zmiňované údaje o srdečním tepu. Pokud přístroj detekuje nepravidelný tep, automaticky kontaktuje tísňovou linku.

Společenský medvěd přináší „roboterapii“

Jiný druh pomoci stárnoucím a osamělým lidem nabízí takzvaný společenský medvěd. Plyšáci totiž už nemusejí být jen hračky pro děti do postele, když mají spát. Fujitsu Labs vyvinuly prototyp medvěda pro dospělé, který má uvnitř sofistikovaný hardware a reaguje na lidskou přítomnost. Tenhle plyšák má název „společenský robot s osobností“ a umí jednoduchá gesta, udrží oční kontakt a zvládá i základní rozhovor. Cílem je, aby chlupatý robot byl pomáhal při „roboterapii“ v geriatrické medicíně pro pacienty, kteří trpí stařeckou demencí.

Robot od Fujitsu připomíná například Pleo, zeleného robotického dinosaura, jenž zobrazoval základní emoce svému okolí. Přestože Pleo byl inovativní a technicky vyspělý, robot se nestal mainstreamovou senzací hlavně kvůli tomu, že byl primárně vymyšlen jako hračka.

Medvěd od Fujitsu naplňuje daleko hlubší účel. Jeho senzory umožňují jednoduchou gestikulaci, když například zvedá ruce a odpovídá na základní stimuly. Medvědi mají v nose miniaturní kameru, aby se mohli automaticky vzbudit z uspaného stavu, pokud v blízkosti vidí člověka. Hlasový syntetizér uvnitř tohoto zařízení vydává zvuk podobný hlasu mladého chlapce a je naprojektován tak, aby byl synchronizovaný s robotovým chováním.

Robotičtí plyšáci umějí až 300 pohybových vzorů včetně zvedání pacek, kývání hlavou a vykopávání nohama. Pohyby jsou kombinované s výrazy „emocí“, jež signalizují štěstí, smutek a rozzlobení. Vzhledem k tomu, že je možné robota propojit s počítačem přes USB port, lze také nahrávat nové pohyby. Medvěd se tak neustále „učí“ nové věci a svým vlastníkům tak může přinášet radost. Stárnoucí lidé určitě ocení, že ho není nutné krmit, nebo venčit, takže péče o něj se neliší od jakéhokoli jiného elektronického zařízení.

Práce očima pomáhá postiženým

Říká se, že oči prozradí často víc, nežli rty. Můžeme z nich vyčíst náladu, vnitřní motivy, nebo zájmy konkrétního člověka. Často nám pouhý pohyb očí osvětlí mnohé o záměrech někoho, kdo by o sobě neřekl vůbec nic.

Psychologové dlouhodobě zkoumají například vazbu mezi pohyby očí a emocemi. S vysokou úspěšností pak mohou říct, jestli někdo lže, nebo se snaží něco zatajit. Lidé totiž ve velké většině případů na pohyby očima vůbec nemyslí a dělají je instinktivně. Fujitsu se tedy zaměřilo na pohyby očí, aby vytvořilo technologii „Gaze tracking“ (Sledování pohledu), která zjišťuje, co lidé chtějí dělat a podporuje je, aniž by přitom obtěžovala.

Fujitsu Laboratories zkoumají a vyvíjejí metodu sledování zraku, tak, aby mohly sledovat lidský pohled ve chvíli, kdy člověk na něco zaměřuje svou pozornost. Počítače Fujitsu nabízejí funkci Gaze Assist, která automaticky za uživatele scrolluje, nebo zoomuje. Touto utilitou disponují počítače Fujitsu od října 2012.

Nicméně aby tato technologie mohla vůbec začít fungovat, muselo Fujitsu překonat dvě velké výzvy.

První z nich bylo vyvinutí kompaktního senzoru. Pokud by senzor, který se skládá z infračervené kamery a LED diod, byl příliš velký, bylo by těžké ho nainstalovat do různých zařízení a na nejvýhodnější místa.

Druhou výzvou bylo snížení nákladů na výrobu. Aby bylo možné sledovat pohled člověka s vysokou přesností, bylo nutné zabírat ostré obrazy oka. Nicméně při použití výkonné kamery a několika LED diod pro zabránění ostrého obrazu je senzor drahý a velký. Jinými slovy, když se vědci zaměřili na kompaktní a levný senzor, snímáný obraz byl neostří a přesnost byla horší. Ve výsledku bylo pak složité využití takového senzoru na trhu.

Nicméně skupina vědců z Fujitsu Laboratories vedená Satoshi Nakashimou nakonec slavila úspěch. Na jejich vlastním řešení, pro rozpoznávání obličejů a senzorů pro rozpoznávání lidské postavy, jeho tým vyvinul technologii, která dokázala sledovat lidský pohled s vysokou přesností, i když obraz nebyl zcela ostrý.

Základní metodou sledování pohledu pomocí kamery je identifikace určitého bodu v oku, který se pohybuje a určení referenčního bodu, který se nepohybuje. Následné použití pozičního vztahu mezi dvěma body umožňuje identifikovat směr a cíl, na nějž se uživatel kouká. To pohybově postiženým dovolí, aby zvládli různé druhy práce na počítači a používali k tomu pouze jejich oči.

Místo procesorů salát

Dalším z problémů dnešního světa je spotřeba energie. Jak jsme zmínili v úvodu, nový hardware je rychlejší, menší, ale také spotřebovává daleko víc elektřiny, než dříve. Kromě toho, že Fujitsu nabízí nejšetnější servery na trhu, se snaží také myslet dál do budoucna. Nedávno v opuštěné továrně na výrobu procesorů spustila pěstírnu salátu. Celý proces řídí cloudový serverový systém a vypěstovaná zelenina by měla být kvalitnější než ta z pole. Navíc ji lze takto pěstovat kdekoli, třeba i v podzemních garážích.

Cloudový systém Akisai má umožnit pěstovat zeleninu v prostředích, kde tradiční způsoby zemědělské činnosti nejsou možné, a zefektivnit pěstování ve stávajících farmách.

Fujitsu spustilo v červenci 2013 výzkumné centrum se dvěma skleníky o rozloze 352 metrů čtverečních a venkovními poli s rozlohou 1000 metrů čtverečních. Zeleninu zde pěstují v půdě, velké množství čidel snímá teplotu, vlhkost vzduchu, obsah CO₂, vlhkost zeminy, nasycenost půdy živinami, kyselost půdy, intenzitu slunečního svitu a další parametry, které cloudový systém vyhodnocuje a automaticky jimi řídí zavlažovací systémy a ventilační systémy, dává hnojiva, nebo aktivuje stínící systémy.

Jde to ale i ve vysloužilých kancelářských budovách. V únoru 2014 spustilo Fujitsu další ověřovací projekt, cloudovým systémem řízenou hydroponickou pěstírnu v opuštěné továrně na výrobu integrovaných obvodů v Aizu-Wakamatsu v prefektuře Fukušima. Zastavěná plocha je 2000 metrů čtverečních. Pilotním projektem je pěstování salátu ve vodním roztoku v nádobách v regálech. Každé patro má vlastní přívod vody

s živinami a osvětlení vlastními LED zářivkami. Vzduchotechnika je společná pro celou halu. Vše kontroluje velké množství čidel a samozřejmě řídí cloudový systém Akisai.

Systém je koncipován tak, aby dokázal vytvořit ideální podmínky pro růst konkrétního druhu zeleniny – jak z hlediska přístupu světla, tak vody, živin a vlastností vzduchu. V současnosti roste jeden salát do finální velikosti 50–60 dní, z pěstírny jich vyexpedují 3 500 denně. Většinu nákladů tvoří energie, ICT technologie tvoří jen 5 procent nákladů. Továrna má samozřejmě vlastní solární elektrárnu, čímž se snaží o co největší míru energetické nezávislosti. Díky plně kontrolovanému prostředí má být pomocí systému Akisai vypěstovaná zelenina zdravější a kvalitnější než z tradičních farem a pěstíren. Zároveň se výrazně sníží či zcela vyloučí použití pesticidů, navíc má mít zelenina menší obsah draslíku, takže by si na ní mohli pochutnat i lidé s nemocnými ledvinami. Zrovna u salátu je podíl draslíku nízký, ale například u luštěnin by mohlo být jeho snížení (bude-li možné) velmi příznivé.

Takto koncipovanou pěstírnu je možné vybudovat například v nevyužitém patře kancelářské budovy. To je třeba v případě Japonska s minimálními prostory vhodnými k zemědělství, upadávajícím venkovem a městy plnými mrakodrapů velmi zajímavé řešení.

Stoupá význam softwarové podpory finanční kontroly

Výhodou řešení GORDIC je integrace s ekonomikou a elektronickým schvalovacím procesem

Ing. Vladimír Přech, marketingový specialista, GORDIC spol. s r. o.

Oblast finanční kontroly organizací veřejného sektoru zahrnuje v současné době interní audit, veřejno-právní kontrolu, finanční kontrolu mezinárodních smluv a tzv. řídicí kontrolu, která je někdy za finanční kontrolu mylně zaměňována. Přesunutím řady povinností v oblasti kontroly na samotné organizace (posílení role interního auditu) stoupne také význam softwarové podpory těchto procesů.

Již dnes je základním stavebním kamenem této aplikační podpory v pojetí GORDIC specializovaný modul Finanční kontrola (FIK), který řeší interní audit, veřejnoprávní kontrolu a oblast následné řídicí kontroly.

Předběžná finanční kontrola je implementována do procesů financování organizace, tedy do Smluv, Knihy došlých faktur, Knihy odeslaných faktur a dalších aplikací. Předností řešení v pojetí společnosti GORDIC je plná integrace kontrolních prvků s ekonomickým informačním systémem, díky které odpadá duplicitní zadávání dat.

Důležitým prvkem řešení je také využití Elektronické podpisové knihy (EPK) a tedy zapojení finanční kontroly do obecného elektronického schvalovacího procesu organizace. Ten je již mnoha velkými úřady úspěšně využíván. Například na ministerstvu obrany je prostřednictvím EPK realizováno denně cca 3000 podpisů, Krajský úřad Středočeského kraje realizoval za poslední čtvrtletí roku 2014 v Elektronické podpisové knize více než 52 tisíc úkonů (posouzení, podpis, schválení). Elektronický schvalovací proces je navíc doprovázen avizací – důležitá upozornění chodí uživateli přímo do e-mailu.

Přínosy řešení Finanční kontroly GORDIC:

- systémové řešení požadavků zákona
- úspora času a práce
- eliminace duplicitního zadávání dat
- optimalizace rozpočtu vedoucí k úsporám
- operativní řízení hotovosti
- minimalizace rizika porušení rozpočtové kázně
- důkaz snahy o transparentnost organizace
- posílení důvěry občana k úřadu
- a k jeho vedení
- úspora času při tvorbě výstupů pomocí šablon
- snížení objemu interních tisků
- díky elektronizaci
- preventivní snížení rizika defraudace

Spisová služba nikoliv jako nutné zlo, ale jako užitečný pomocník

Bc. Irina Rálišová, MěÚ Sezemice; Mgr. Tomáš Lechner, Ph.D., Triada, spol. s r. o.

Úvod

Spisová služba je často považována za nutné zlo, které je třeba v některých případech bohužel realizovat, avšak v co nejmenší míře a s co nejvíce výjimkami, jak jen nám to legislativa dovolí. Přesně takový nesprávný přístup má bohužel mnoho veřejnoprávních původců, a to na všech úrovních veřejné správy. Nicméně přeci jen existuje pár světlých výjimek původců, kteří spisovou službu používají jako užitečný nástroj a pomocníka při plnění mnohých úkolů kladených na jednotlivé orgány veřejné moci. Jednu takovou dobrou praxi představuje právě tento příspěvek.

Různé možnosti výkonu spisové služby

Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů definuje výkon spisové služby jako zajištění odborné správy dokumentů vzniklých z činnosti původce, popřípadě z činnosti jeho právních předchůdců, zahrnující jejich řádný příjem, evidenci, rozdělování, oběh, vyřizování, vyhotovování, podepisování, odesílání, ukládání a vyřazování ve skartačním řízení, a to včetně kontroly těchto činností. Zároveň připouští dvě možnosti jejího vedení. Buď v elektronické podobě v elektronickém systému spisové služby, nebo v listinné podobě. Někteří veřejnoprávní původci mají přímo zákonem danou povinnost vést spisovou službu v elektronické podobě, např. organizační složky státu, vysoké školy, kraje a hlavní město Praha, jiní původci mají právo volby, jako např. obce. Nicméně i pro ně platí preferovaný způsob vedení spisové služby v elektronické podobě v elektronickém systému spisové služby.

Tento přístup preferování elektronického způsobu vedení spisové služby je poměrně mladý a jeho počátek je svázán s okamžikem realizace komunikace pomocí informačního systému datových schránek, který je podložen zákonem č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů, a který nabyl účinnosti 1. července 2009. Avšak i před tímto okamžikem existovali původci, kteří využívali pro podporu vedení spisové služby elektronické nástroje. Ačkoliv nešlo o elektronický způsob vedení spisové služby jako takový, ale pouze o elektronizaci dílčích úkolů a úkonů, jako je sledování oběhu dokumentů, přidělování čísel jednacích a zápis dokumentů do základní evidenční pomůcky – podacího deníku.

Když se podíváme na aktuální znění zákona a k němu prováděcího právního předpisu, který byl mimochodem novelizován k 1. lednu letošního roku, je zřejmé, že podací deník ve smyslu základní evidenční pomůcky je znakem vedení spisové služby v listinné podobě. V elektronické podobě je nahrazen evidencí dokumentů, která je přímou součástí elektronického systému spisové služby. Již z toho je zřejmé, že elektronický způsob vedení spisové služby není jen prostou transformací nástrojů původní listinné podoby do digitálního prostředí, ale že je odlišným specifickým a přesně popsaným samostatným způsobem vedení spisové služby. Tento fakt je však mnohými původci pomíjen.

Co tedy skutečně znamená vedení spisové služby v elektronické podobě? Znamená to, že musíme na vstupu transformovat všechny dokumenty do digitální podoby a už se nepotkáme s papírem? To rozhodně ne, tento strašák plné elektronizace je zase jen zkresleným pohledem těch, kteří se snaží hledat výmluvy, proč zrovna pro ně není elektronický způsob vedení spisové služby vhodný. A při tom pravý opak je pravdou. Pokud se původce, který má právo volby, rozhodne vést spisovou službu v listinné podobě, musí na vstupu všechny digitální dokumenty transformovat do analogové podoby, avšak pokud se rozhodne vést spisovou službu v elektronické podobě, transformuje do digitální podoby pouze vhodně vybrané analogové dokumenty, u kterých to má smysl. Důvod je zřejmý, zatím co vedení spisové služby v listinné podobě nemá,

jak zajistit evidenci digitálních dokumentů, tak elektronický systém spisové služby slouží, jak k evidenci digitálních dokumentů, tak k evidenci metadat (popisných údajů) o analogových dokumentech.

S přihlédnutím k vazbě na datové schránky a další nástroje e-Governmentu je vedení spisové služby v elektronické podobě jednoznačně doporučenímhodným způsobem. Vhodný elektronický systém spisové služby může navíc přinášet celou řadu výhod, které vlastní vedení spisové služby zjednoduší a navíc nabídne i další nástroje a možnosti. Některé z nich jsou povinné na základě Národního standardu pro elektronické systémy spisové služby, který vydalo Ministerstvo vnitra podle zmocnění uvedeném v zákoně o archivnictví a spisové službě, a některé jsou specifickou předností konkrétního produktu.

Město a Městský úřad Sezemice

Představme si nyní původce, který v současné době vede spisovou službu v elektronické podobě v elektronickém systému spisové služby. Jde o město Sezemice, které leží při řece Loučné nedaleko polabské dominanty, Kunětické hory. Patří k nejstarším sídlům Pardubického kraje. Osídlování území dnešních Sezemice a jejich blízkého okolí bylo předurčeno polohou toků řek Labe a Loučné, po jejichž březích vedly prastaré kupecké stezky. O pradávém osídlení okolí Sezemice svědčí četné archeologické nálezy v Sezemích, Kuněticích, Lukovně, Počaplech, Velkých Kolodějích a v blízkosti sousedních obcí. Nejstarší zaznamenaná písemná zpráva o Sezemích pochází z roku 1227. Tehdy velmož Kojata z rodu Habišiců odkázal ve své závěti ves Sezemice cisterciáckému klášteru v Sedlci u Kutné Hory. Jak dlouho Sezemice existovaly před tímto letopočtem a kdo Sezemice založil, zůstává zastřeno tajemstvím.

Zatímco na počátku druhé poloviny 17. století bydlelo v Sezemích 339 obyvatel, v dnešní době žije v Sezemích, včetně připojených obcí Dražkova, Kladiny, Lukovny, Počapel, Velkých Koloděj a Veské, celkem 3622 obyvatel.



Obr. 1: Pohled na Městský úřad Sezemice.

Město Sezemice je obcí I. typu, avšak vykonává také přenesenou působnost na úseku stavebního úřadu a na úseku matriky a evidence obyvatel. Městský úřad se člení na úseky – Podatelnu a Matriku a evidenci obyvatel a na odbory – finanční odbor, odbor stavebního úřadu a územního plánování a odbor správy majetku a životního prostředí. Celkový počet pracovníků v městském úřadu je 35, z nichž je 16 úředníků, kteří v současné době využívají elektronickou spisovou službu Munis ERMS. Dále elektronickou spisovou službu využívá starosta a místostarosta.

Historie a současnost využití elektronické spisové služby na MěÚ Sezemice

Již v roce 2004 jsme na Městském úřadě Sezemice začali používat elektronické nástroje pro podporu vedení spisové služby. Tehdy se jednalo o modul Kancelář informačního systému Munis, jehož součástí byla i elektronická podatelna. Koncem roku 2004 jsme zahájili zkušební provoz.

Primární motivací bylo řešení nástroje pro realizaci elektronické podatelny, ale nakonec jsme do elektronické podoby převedli celou evidenci podatelny. Došlo tím ke sjednocení pravidel pro příjem listinných i elektronických dokumentů, které je prvním a poměrně zásadním pozitivem elektronického způsobu vedení spisové služby.

Před zahájením ostrého provozu nového elektronického nástroje, jsme proškolili pracovníky úřadu. Aby toto školení mělo co nejsilnější dopad, zvolili jsme alternativu přímého školení, kdy jsme si pronajali od místní školy počítačovou učebnu, kde společnost Triada dočasně nainstalovala stejnou verzi spisové služby jako na úřadě, a naši pracovníci si mohli rovnou probírané postupy zkoušet na počítačích. Tento postup byl sice časově náročnější, než školení pouze s předváděním nových postupů lektorem, ale ve svém důsledku se investovaný čas na školení vrátil v úspoře času pracovníků, kteří při vlastní práci již zvládli naučené postupy v mnohem kratším čase a hlavně s menším počtem začátečnických chyb. Posledním krokem zavedení elektronické spisové služby byla příprava vzorů dopisů.

Následně došlo k propojení modulů informačního systému Munis se specializovaným programovým vybavením společnosti Vita software, které využívá stavební úřad. I tato vazba se ukázala, jako velmi užitečná při zvládání změn, které přinesl rok 2009.

V roce 2009 došlo k rozšíření modulů informačního systému Munis tak, aby v kompletu doplnily stávající nástroje a společně vytvořily „skutečný“ systém elektronické spisové služby podle v témže roce novelizovaného zákona o archivnictví a spisové službě. Od října 2009 pomocí něj všichni pracovníci přijímají a odesílají dokumenty přes elektronickou spisovou službu prostřednictvím datových schránek. Díky předchozímu využívání elektronických nástrojů, které již úředníci považovali za samozřejmé, nebylo pro nás zavedení nového informačního kanálu v podobě informačního systému datových schránek významně složitým krokem.

V následujících letech jsme postupně využívali další funkce implementovaného systému, mezi kterými pro nás byla nejpodstatnější druhotná evidence dokumentů podle jednotlivých témat. Tímto způsobem jsme vhodně seskupovali objednávky, žádosti o informace podle zákona č. 106/1999 Sb., spisy přestupkové komise apod. Kromě toho jsme zavedli plnou evidenci doruček, a to nejen těch elektronických poskytovaných informačním systémem datových schránek, ale i listinných. Díky tomu máme nejen přehled o všech doručkách, ale spisová služba automaticky počítá lhůty pro nabytí právní moci, které je pak možné následně k dokumentům vyznačit. Tvorba záznamů pomocí předpřipravených šablon a jejich následná konverze do výstupního formátu PDF/A byla již naprostou samozřejmostí a pouze jsme rozšiřovali a upravovali vzory dle aktuálních potřeb.

V roce 2014 jsme dále rozšířili konverzi přijatých listinných dokumentů do digitální podoby. K jednotlivým vybraným důležitým evidovaným listinným dokumentům doplňujeme jejich naskenovaná digitální ztvárnění. V témže roce nám byla dodavatelem nabídnuta možnost přejít na technologického nástupce stávajícího řešení, na elektronickou spisovou službu Munis ERMS. Na podzim došlo k převodu všech dokumentů za využití standardizovaného formátu podle Národního standardu pro elektronické systémy spisové služby a nasadili jsme plně tento nový systém. K proškolení uživatelů jsme využili opět stejný postup. Pronajali

jsme si od místní školy počítačovou učebnu, kde společnost Triada dočasně nainstalovala stejnou verzi nové spisové služby včetně aktuálních převedených dat a naši pracovníci si mohli rovnou probírané postupy zkoušet na počítačích. Tento postup se nám tak již podruhé vyplatil, neboť všichni pracovníci úřadu zvládli přechod na nový systém naprosto perfektně.

V současné době rozšiřujeme ve spolupráci s dodavatelem využití nové elektronické spisové služby Munis ERMS a podílíme se svými připomínkami i na jeho dalším rozvoji.

Závěr

Důležité je přistoupit k implementaci elektronické spisové služby pozitivním a jasně definovaným přístupem bez výjimek a zesložitujících dodatečných podmínek evidence. Podstatná je jednotnost pravidel, jasně dané povinnosti, kontrola zapisovaných údajů, jak implementovaným systémem, tak nadřízenými pracovníky, a nebát se využívat vše, co daný systém skutečně nabízí. Odměnou je pak úplný přehled o všech dokumentech, spisech i doručenkách a zjednodušení mnohých procesů nezbytných při vedení různých typů řízení.

Literatura

- [1] Národní standard pro elektronické systémy spisové služby, dostupné na adrese <<http://www.mvcr.cz>>.
- [2] Oficiální webové stránky města Sezemice, dostupné na adrese <<http://www.sezemice.cz>>.
- [3] I. Rálišová, T. Lechner, Jak poznáte správně implementovanou elektronickou spisovou službu, dostupné na adrese <<http://www.issc.cz>>
- [3] I. Rálišová, T. Lechner, Jak se obce připravují na Národní standard pro elektronické systémy spisových služeb, dostupné na adrese <<http://www.issc.cz>>

Výhody integrovaného informačního systému města

Vladislava Šarkadyová, MěÚ Ústěk; Mgr. Tomáš Lechner, Ph.D., Triada, spol. s r. o.

Úvod

Postupující rozvoj elektronizace veřejné správy, stále větší nároky na množství a rozsah zpracovávaných agend městskými úřady a přibývajících povinností elektronické komunikace s centrálními úřady znamenají též zvyšování nároků na informační systémy provozované městskými a obecními úřady. Otázka, zda je nějaký informační systém potřeba, je již tedy dávno vyřešena, ale zbývá otázka, jaký systém je nejvhodnější. Neexistuje univerzální odpověď, protože každý úřad je svým způsobem specifický, ale pro určitou velikostní kategorii měst, zejména od 2 do 15 tis. obyvatel, je jednoznačnou odpovědí, že by to měl být systém provázaný, co nejvíce komplexní a zároveň otevřený, aby nejlépe vyhověl všem požadavkům na něj kladených.

Město Ústěk a městský úřad

Město Ústěk leží v krajině severních Čech mezi Litoměřicemi a Českou Lípou na výrazném pískovcovém návrší v nadmořské výšce kolem 240 m na rozhraní CHKO České středohoří a Kokořínsko. V současné době má přibližně 2,7 tis. obyvatel. Ve městě je celá řada stavitelských a historických pamětihodností. Město Ústěk je nejmenší městskou památkovou rezervací v České republice. Historie města sahá velmi daleko, archeologické nálezy dokazují, že ostroh, na kterém město stojí, byl osídlen již v 10.–13. století. Ve 14. století získal Ústěk významnější postavení a také statut města. V dokumentech se uvádí, že se tak stalo v roce 1361. Jádrem města byla, a do současné doby je, nejširší část ostrohu kolem dnešního kostela sv. Petra a Pavla.

Poslední reforma územního uspořádání zařadila Ústěk do Ústeckého kraje. Město má pověřený obecní úřad, tedy plní funkci pověřeného města druhého stupně pro obce Ústěk, Liběšice, Chotiněves, Horní Řepčice, Lovečkovice, Levín a jejich místní části. Velikost celé spádové oblasti je přibližně pět tisíc obyvatel.

Rada města má 5 členů, Zastupitelstvo města je patnáctičlenné. Městský úřad má 4 odbory (finanční odbor, stavební odbor, odbor sociálních věcí a odbor vnitřních věcí) a samostatné oddělení vedení města a správce majetku.

Městský úřad má celkem 32 zaměstnanců, z čehož je 16 úředníků. Všichni pracují s implementovaným informačním systémem Munis.



Obr. 1: Město Ústěk.

Další informace o městě a městském úřadě lze najít na webových stránkách dostupných na adrese <http://www.mesto-ustek.cz/>.

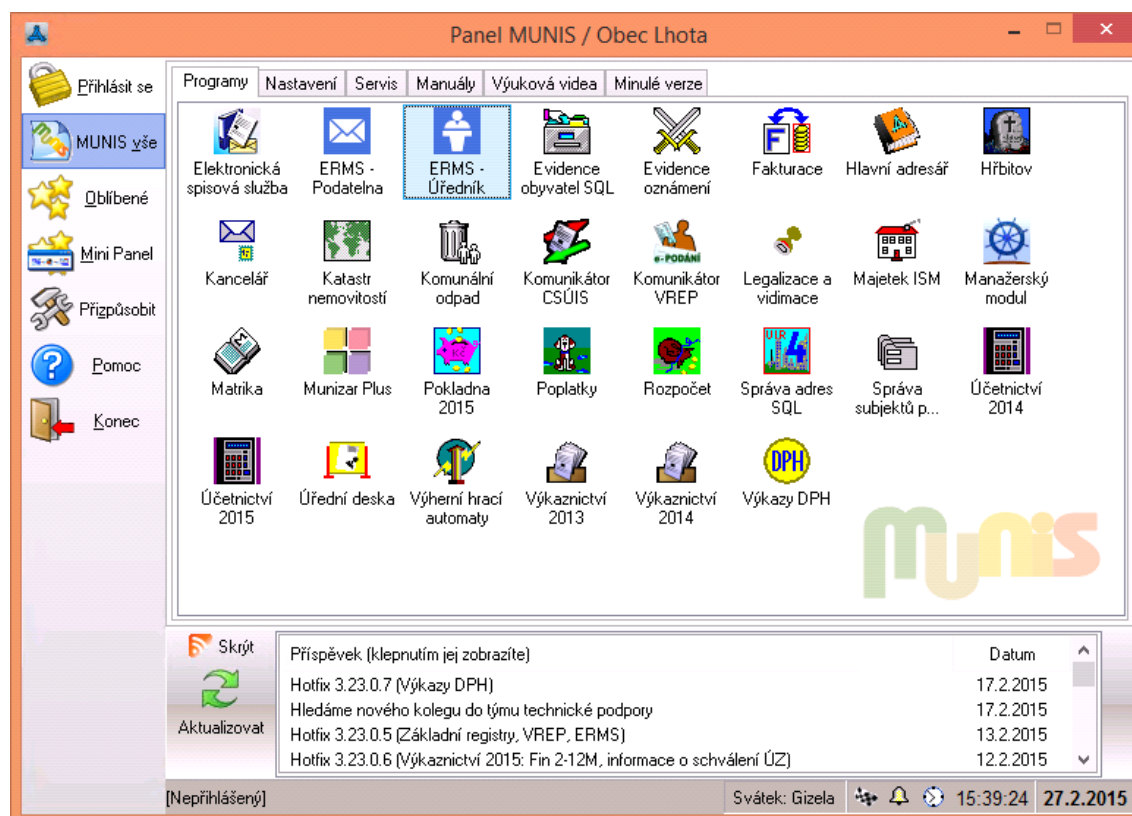
Informační systém Munis

Tvůrcem i dodavatelem informačního systému Munis je společnost Triada. Základními charakteristikami tohoto informačního systému je modulárnost, provázanost, otevřenost, variabilita, bezpečnost a jednoduchost ovládání. Za základní kámen tohoto informačního systému je považováno robustní datové jádro, jehož struktura a provoz jsou založeny na moderních technologiích a platformách s předpokladem dlouhodobé životnosti. Díky této architektuře lze i v budoucnu rozvíjet aplikace uživatelského rozhraní v souladu s moderními technologiemi bez velkých zásahů do datového jádra.

Modulárnost informačního systému Munis umožňuje volit skladbu podporovaných agend s ohledem na potřeby úřadu. Navíc jsou v systému dodržovány prvky jednotného ovládání, které usnadňují zvládání okamžiků zástupů při dovolených a nemocech. Bezpečnost systému je podporována systémem oprávnění a rolí. Jednotlivým uživatelům lze přidělovat práva, nebo skupiny práv, pro přístup k jednotlivým modulům, typům činností a či konkrétním dokumentům a dokladům.

Základní přehled ekonomických, evidenčních a správních agend IS Munis je následující: Elektronická spisová služba Munis ERMS, Evidence obyvatel a volby, Matrika, Legalizace a vidimace, Evidence oznámení, Úřední deska a eDeska, Majetek, Výherní hrací automaty, Katastr nemovitostí, Účetnictví a rozpočet, Výkaznictví, Komunikátor CSÚIS, Tvorba rozpočtu, Výkazy DPH, Fakturace, Bankovní služby, Mzdy, Personalistika, Elektronické výkaznictví ISP, VREP komunikátor, Pokladna, Poplatky aneb operativní evidence příjmů, Platební karty, Komunální odpad a Evidence hřbitova. Nad tím vším lze vytvářet statistické výstupy, přehledy a kontrolní sestavy pomocí modulu Manažerská nadstavba.

V rámci celkové stavby a provázanosti vnitřního informačního systému úřadu je pak IS Munis napojen na moduly dalších dodavatelů, např. Stavební úřad společnosti VITA SW, které tak s výše uvedenými agendami tvoří jednotný vzájemně komunikující informační systém. Dále je IS Munis pro vnější komunikaci napojen na všechny aktuální nástroje e-Governmentu jako jsou základní registry veřejné správy, informační systém datových schránek, Czech POINT, Czech POINT@Office anebo centrální systém účetních informací státu.



Obr. 2: Nabídka modulů informačního systému Munis.

Informační systém Munis je dále provázán se službami centra sdílených služeb portálu iMunis.cz. Služby tohoto portálu jsou koncipovány tak, že zachovávají maximální bezpečnost ukládaných dat vzhledem k jednotlivým uživatelům. Správcovský přístup ke službám je buď přímo prostřednictvím webového klienta, nebo pomocí webových služeb, na které jsou navázány jednotlivé specializované moduly IS Munis. Portál iMunis.cz je provozován v režimu 7x24. Datové centrum leží v České republice a jeho provoz tedy plně podléhá českému právnímu řádu. Uživatelé se tak v žádném případě nemusí bát o svá data, jejichž zabezpečení je na velmi vysoké úrovni. Přehled služeb nabízených tímto portálem je následující:

- Úřední deska – zveřejnění obsahu úřední desky způsobem umožňujícím dálkový přístup podle § 26 zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů.
- SMiS – hromadné rozesílání SMS zpráv prostřednictvím internetu. Okamžité a hromadné zasílání zpráv, které mohou být určeny různým okruhům příjemců a to podle charakteru informace.
- Evidence oznámení – řešení povinností podle zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů.
- Webináře – moderní a interaktivní forma seminářů probíhající pomocí internetu.
- HelpDesk Munis – technická podpora pro uživatele IS Munis.
- Rozklikávací rozpočet – jednoduchá a srozumitelná prezentace hospodaření měst, obcí a dobrovolných svazků obcí na internetu.

Využití IS Munis na MěÚ Ústěk

Z celkové nabídky modulů IS Munis využívá MěÚ Ústěk moduly: Evidence obyvatel, Matrika, Katastr nemovitostí, elektronickou spisovou službu realizovanou moduly Kancelář, PDF tisk, ePero, eDok a vazbou na CzechPOINT, ekonomické moduly Účetnictví a výkaznictví, Pokladna, Poplatky, Majetek, Fakturace, Bankovní služby a Komunální odpad. Dále je IS Munis provázán se stavebním úřadem společnosti Vita sw. Jako poslední začala být městem využívána služba Rozklikávací rozpočet.

Instalace informačního systému Munis proběhla na úřadě v srpnu roku 2009. Jako první následně proběhlo školení vedení spisové služby s vazbou na datovou schránku, která byla přesně v té době na základě pravidel daných zákonem č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, aktivována. Mezi další využívané moduly patřily na podzim téhož roku modul Poplatky a specializovaný modul Komunální odpad, který odpovídá způsobu výběru místního poplatku za provoz systému shromažďování, sběru, přepravy, třídění, využívání a odstraňování komunálních odpadů podle zákona č. 565/1990 Sb., o místních poplatcích, ve znění pozdějších předpisů.

Dalším modulem, do kterého byla převedena data z dřívějšího informačního systému, byla Evidence obyvatel, která slouží mimo jiné pro tvorbu volebních seznamů. V souvislosti se zvoleným způsobem výběru poplatku za komunální odpad je výhodné provázání těchto modulů, které je legislativně přípustné a z hlediska kontroly podkladů pro daný místní poplatek výhodné.

Ke konci roku 2009 ještě proběhlo připravení ekonomických modulů Pokladna a Účetnictví a výkaznictví. V pokladně byly připraveny potřebné vzory včetně vazeb na kontaci a do účetnictví byla převedena data z předchozího informačního systému tak, aby od 1. ledna 2010 mohl úřad plně využívat služeb IS Munis včetně výhod plynoucích z provázanosti jednotlivých modulů.

Hned v začátku roku 2010 byla na elektronickou spisovou službu napojena též aplikace Czech POINT, díky čemuž vydávané ověřené výpisy z informačních systémů veřejné správy získávají automaticky potřebná čísla jednací a jsou v souladu s legislativními požadavky ukládány do dokumentového úložiště, kterým pro elektronickou spisovou službu Munis je úložiště Munis DUL. Zároveň se rozjíždělo vedení všech ekonomických agend. První musela samozřejmě fungovat pokladna v návaznosti na operativní evidenci příjmů (modul Poplatky). Následně po uzavření roku 2009 a otevření roku 2010 byly nasazeny moduly Fakturace, Bankovní služby a Účetnictví a výkaznictví.

V II. Q. 2010 byl pak nasazen modul Matrika sloužící pro povinné souběžné vedení matričních knih pomocí výpočetní techniky dle § 6 zákona č. 301/2000 Sb., o matrikách, jménu a příjmení a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, a dále pro tisk matričních dokladů. Od roku 2015 lze pomocí tohoto programu též evidovat jednotlivé matriční doklady tak, jak to vyžaduje citovaný (dále novelizovaný) zákon.

Posledním z ekonomických modulů IS Munis, který byl v roce 2010 nasazen do užívání, byl modul Majetek, jehož vazba na účetnictví je velice potřebná s ohledem na povinné pravidelné odpisování určených druhů majetku.

Od roku 2011 již MěÚ Ústěk využívá implementované moduly IS Munis rutinně. Velkou výhodou jsou vazby mezi jednotlivými moduly, z nichž některé již byly naznačeny ve výše uvedeném popisu postupné implementace tohoto informačního systému. Po celou dobu implementace se o nás staral jeden vyčleněný pracovník společnosti Triada, Dan Mora, což přispělo k celkové spokojenosti, neboť se seznámil s našimi potřebami a specifiky našeho úřadu a mohl tak vždy adekvátně reagovat při řešení dalšího rozvoje užívání IS Munis, zejména úprav uživatelského nastavení, přístupových práv a tiskových výstupů.



Obr. 3: Rozklikávací rozpočet města Ústěk.

V roce 2015 jsme rozšířili vazbu IS Munis na základní registry zakoupením licence Munizar Plus, která umožňuje využití vazby na základní registry veřejné správy nejen pro účely výkonu specifických agend, pro něž máme pořízeny moduly IS Munis, ale též zcela volně prostřednictvím obecné integrované prohlížečky. Dále jsme zakoupili modul Legalizace a vidimace, jehož vazba na základní registry významným způsobem zjednodušuje proces legalizace. Ověřovací doložky tiskneme pomocí speciální štiťkové tiskárny.

Také jsme začali využívat službu Rozklikávací rozpočet, kterou lze jednoduše naplnit dávkově daty z IS Munis a která následně přehledným grafickým způsobem ukazuje nejen aktuální rozpočet, ale také jeho plnění a čerpání včetně meziročního vývoje, jak ilustruje Obr. 3.

Na závěr ještě několik přímých zkušeností z provozu IS Munis a vazeb mezi jeho moduly. Pro úřad našeho typu jsme v IS Munis našli naprosto odpovídající pracovní nástroj, vazby např. mezi modulem Pokladna při platbě místních poplatků a modulem Poplatky jsou velkou pomocí, taktéž vazba do evidence obyvatel.

Závěr

Na závěr lze konstatovat, že využití modulárního provázaného informačního systému přináší celou řadu významných výhod. Modulárnost lze ocenit zejména v době implementace a provázanost pak v každodenní praxi.

Praktické dopady modularity se na menším úřadě ukazují především v možnostech zastupování pracovníků v době nemoci, čerpání řádných dovolených a běžné fluktuaci zaměstnanců. Podobnost uživatelského rozhraní v jednotlivých modulech těmto potřebám vychází vstříc a zvládnutí ovládání nového modulu je tak zcela intuitivní.

Zavádění nových systémů do výkonu práce vždy zprvu přináší u těch, kteří budou systém pravidelně užívat, negativní postoj, ani u nás tomu nebylo jinak. Dnes s odstupem času a zkušenostmi, které jsme po dobu práce s IS Munis načerpali, mohu říci, že změna u nás proběhla k dobrému a ti, kterých se týkala, mají dnes postoj pozitivní. Velkým přínosem pro nás byl a stále je vyčleněný pracovník společnosti Triada.

MPSV podpoří rozvoj využití asistivních technologií.

RNDr. Jiří Schlanger, Ministerstvo práce a sociálních věcí ČR

Asistivní technologie je pro nás poměrně nový pojem. Za asistivní technologii považujeme jakýkoliv nástroj, zařízení, software nebo systém, využívající zpravidla moderní technologie s cílem posílit, udržet nebo zlepšit funkční schopnosti jedinců se speciálními potřebami, a tím jim usnadnit každodenní život a zlepšit kvalitu jejich života, samostatnost a soběstačnost. Za jedince se speciálními potřebami jsou zde považováni zejména senioři, osoby se zdravotním postižením a chronicky nemocní lidé.

Mezi programy podporovanými Evropskou unií je také program AAL (Ambient Asisted Living) – služby asistovaného života, který má za cíl prodloužit nezávislý život ve vlastním domácím prostředí stárnoucím lidem a lidem se zdravotním postižením s využitím neformální péče osob příbuzných a blízkých nebo profesionálů ve zdravotních a sociálních službách. Právě zde se uplatní i asistivní technologie.

Nevědomky se s asistivními technologiemi už setkáváme. Patří k nim například elektronická navigace nevidomých a slabozrakých nebo software, který umožňuje osobám s tímto postižením a omezením elektronickou komunikaci prostřednictvím počítače. To, co my čteme zrakem, zprostředkuje software nevidomému hlasem do sluchátek. Obdobně bychom mohli najít technologie pomáhající dalším cílovým skupinám v různém prostředí k různorodým aktivitám.

Asistivní technologie pomáhají nejen v běžném životě, ale i k zapojení se do studia a do práce v zaměstnání nebo podnikání.

Ministerstvo práce a sociálních věcí je rezortem odpovědným za začleňování osob znevýhodněných jak na trhu práce, tak i v běžném životě. Má naplňovat Národní plán pro pozitivní stárnutí a seniory, Národní plán pro vytváření rovných příležitostí pro osoby se zdravotním postižením, podílet se na Národním rozvojovém programu mobility pro všechny. Podpora rozvoje využití asistivních technologií je jedním z prostředků, jak řadu úkolů rezortu plnit.

Ministerstvo proto do již běžícího projektu Podpora procesů v sociálních službách, jehož partnery jsou Unie zaměstnavatelských svazů a Svaz měst a obcí začlenila novou aktivitu týkající se rozvoje asistivních technologií. Nová aktivita má za cíl zhodnotit současnou situaci v oblasti rozvoje a využívání asistivních technologií (nejen v prostředí sociálních služeb) a nastavit mechanismy pro jejich využití ve prospěch osob se zdravotním či sociálním znevýhodněním a jejich okolí.

Dílejšími úkoly jsou analyzovat aktuální stav využití asistivních technologií a možnosti dalšího rozvoje využití ICT (informační a komunikační technologie) a asistivních technologií pro inovace v oblasti vybraných veřejných služeb pro osoby se zdravotním postižením, v sociálních a zdravotních službách poskytovaných zejména ve vlastním prostředí příjemcům péče a služeb.

Dále provést šetření nákladů a cen u sociálních služeb využívajících asistivní technologie (např. tísňová péče). Dále kvantifikovat ekonomické přínosy a předpoklady zvýšení efektivity při využití asistivních technologií u neformální péče a sociálních služeb, včetně porovnání s vybranými zeměmi EU a vytvořit znalostní bázi pro využití asistivních technologií v oblasti neformální péče, sociálních služeb a v oblasti kompenzačních a inkluzních pomůcek.

V neposlední řadě pak stanovit principy rozvoje asistivních technologií a služeb postavených na těchto technologiích a skrze konkrétní návrhy legislativních změn integrovat tyto principy do podporovaných procesů modernizace v oblasti sociální péče.

Výstupem této části projektu bude dokument shrnující oblast asistivních technologií a možností jejich využití při poskytování sociálních služeb, u některých zdravotních služeb v prostředí neformální a domácí péče i pro kompenzaci handicapu u osob se zdravotním postižením. Bude rovněž obsahovat ekonomickou rozvahu využívání asistivních technologií, návrh na stanovení regulačního a procesního rámce pro využívání asistivních technologií a definování oblastí dalšího rozvoje asistivních technologií v ČR.

Na zpracování dokumentu se podílí více než 30 expertů z akademických pracovišť podnikatelských subjektů i poskytovatelů zdravotních a sociálních služeb. Mezi experty jsou i zástupci uživatelů asistivních technologií. Práce na dokumentu musí být dokončeny do poloviny roku 2015, aby se závěry mohly zapracovat do výstupů projektu Podpora procesů v sociálních službách do října 2015. Projekt Podpora procesů v sociálních službách je financován z prostředků Evropského sociálního fondu prostřednictvím Operačního programu Lidské zdroje a zaměstnanost a ze státního rozpočtu. Veškeré dění v projektu je průběžně zveřejňováno na stránkách projektu (www.podporaprocesu.cz).

Digitální model veřejné správy

PhDr. et Mgr. Zdeněk Šimek, IT vývojář MV ČR, Mgr. Eva Šimková Hefková, analytik MV ČR

Úvod

Digitální simulace by měly patřit k základním pilířům koncepční činnosti a rozhodování. Stejně jako jsou analýzy jevů a situací první fází zakládající legitimitu a relevantnost těchto aktivit, je předvídání důsledků plánovaných změn fází druhou, neoddělitelnou součástí koncepčního procesu.

Základní myšlenka

Digitální model veřejné správy (DMVS) je robustní software umožňující modelovat a simulovat změny ve veřejné správě a na základě toho sledovat obtížně domyslitelné důsledky změn různého rozsahu včetně změn kvalitativních. DMVS postaven na myšlence „co lze spočítat, mělo by být spočítáno“. Počítačové modelování by tedy – v konečném důsledku – mělo minimalizovat, respektive zcela eliminovat dohady o zjevně poznatelných skutečnostech.

Motivace

Základním impulzem k vytvoření DMVS byla snaha vyplnit chybějící místo na pomyslném „trhu“ veřejné správy a uspokojit tak poptávku odborníků, kteří se koncepčně podílejí na realizaci změn či návrhů. Záměrem bylo, aby měl každý specialista ve veřejné správě možnost snadno nahlížet do exaktních výsledků generovaných na základě určitých vstupních parametrů, které jsou většinou známe či ve vysoké míře předpokládány. A aby bylo zároveň možno studovat nejen reálné procesy, ale i simulovat modelové stavy. Ambicí DMVS však na druhou stranu není nahradit koncepční uvažování nebo samostatně generovat koncepční návrhy. Tento software pouze uděluje technickou oporu v aspektech, kde je systém veřejné správy principiálně spočitatelný.

Funkcionality

Funkcionality DMVS lze rozdělit do těchto obecných kategorií:

- **modelovací funkce**
 - simulování situací ve veřejné správě, koncepční a reálné modelování stavů a procesů, modelování správních obvodů úřadů, modelování systému veřejné správy; optimalizační hypotézy
- **kompletní funkce pro rozdělení příspěvku**
 - analýza, hledání řešení podle požadavku, variabilní metodika, řešení s procentuální představou rozložení, navýšení či snížení příspěvku na určitou kategorii úřadu atp.
- **databázové funkce**
 - tvorba databází a jejich export do obvyklých formátů (CSV) pro další využití
- **geoinformační funkce**
 - vrstvy map, vrstvy správních obvodů, bodové mapy, schematické mapy, rastrové mapy
- **vizualizace**
 - vizualizační nástroje pro srovnávání (obcí, příspěvků atp.), pro představu o situaci v ČR (zalidnění, nadmořské rozdíly, dostupnosti k úřadům, finanční mapa atp.)
- **statistické a doplňkové funkce**
 - podrobné statistické údaje, predikce vývoje počtu obyvatel ve správních obvodech a správních centrech, ekologická situace v obcích, historické statistiky

Principy fungování

DMVS je primárně založen na práci s **datovými registry**⁸, které obsahují datový materiál, datovou logickou strukturu a bodová pole map. Registry jsou v průběhu práce doplňovány ostatními nestrukturovanými datovými a textovými soubory (např. koeficienty pro výpočet příspěvku na přenesenou působnost nebo metodikou). Aktualizace registrů probíhá na uživatelské úrovni (např. počty obyvatel či rozloha území jsou automatizovaně načítány z Českého statistického úřadu). V DMVS při průběhu třídění datových matic – spojování obcí s místně příslušnými úřady podle předem definovaných pravidel – se mj. automaticky posčítají i velikosti správních obvodů včetně počtu úřadů, jež do správních obvodů obcí patří. Tím vznikne komplexní **logická mapa** veřejné správy.



Obrázek 1: Architektura dat v Digitálním modelu veřejné správy

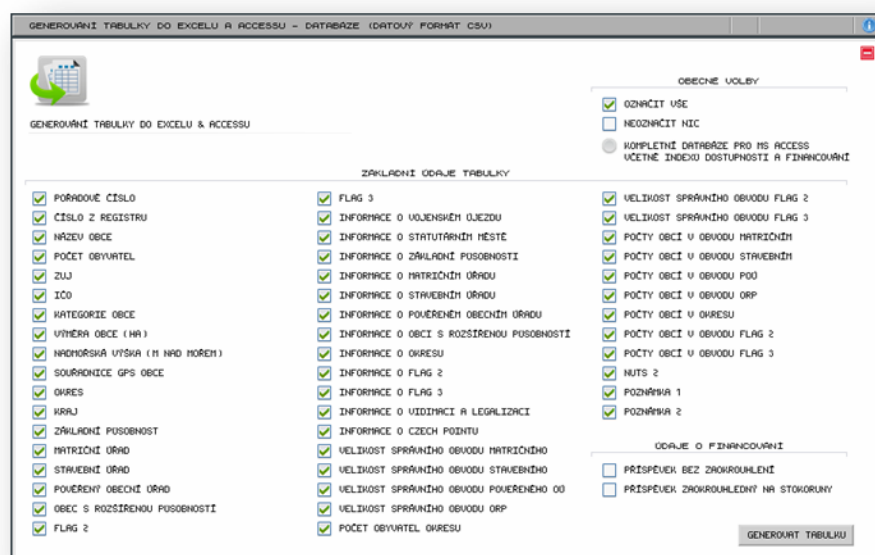
Datové registry z hlediska uživatele tvoří kompletní **kartotéku obcí**. Karta obce je formulářová digitální karta, ve které jsou zobrazovány primitivní datové prvky čitelné z registru obcí, ale také některé kompozitní prvky a další výstupy (např. z GPS souřadnic se již vypočítají dostupnosti v celé ČR nebo z rozlohy území a počtu obyvatel hustota zalidnění). Podoba karet je variabilní a je možno pracovat s nimi i v prostředí MS Accessu.

Obrázek 1: Ukázka podoby digitální karty obce v MS Accessu

⁸ Datové registry jsou interním pramenem Ministerstva vnitra.

Databáze

Snadná tvorba vlastních databází v libovolném rozsahu je jednou z nejsilnějších stránek DMVS. Datový fond v podobě registrů umí DMVS zpracovávat, třídit a vypočítávat na jeho základě libovolně zvolené informace. Databáze jsou poté připraveny pro export do známých tabulkových procesorů MS Excel, MS Access, OO Calc a OO Base. Databáze exportované z tohoto systému mají standardní formát *.CSV⁹, který lze načíst cestou importu dat prakticky kamkoliv.



Obrázek 2: Tvorba vlastní databáze v DMVS

Vysvětlivky Statistika Geoinformace Export O aplikaci							
Základní informace Informace o službách Správní obvody Dostupnost Optimalizace Financování Doplnující informace Třídění podle kategorií Souhrny							
Jihočeský kraj Kraj Vysočina Plzeňský kraj Královéhradecký kraj Liberecký kraj Moravskoslezský kraj Zlínský kraj Pardubický kraj Jihomoravský kraj							
Název obce	Počet obyvatel	ZUJ	IČO	Kategorie	Výměra (ha)	Nadmořská výška (m)	Kraj
Adamov	748	535826	00581160	obec	103	478	Jihočeský kraj
Albrechtice nad Vltavou	835	549258	00249521	obec	3672	428	Jihočeský kraj
Babice	104	537241	00582964	obec	580	447	Jihočeský kraj
Balkova Lhota	124	563251	00512516	obec	355	493	Jihočeský kraj
Báňovice	106	562726	00512915	obec	479	516	Jihočeský kraj
Bavorov	1578	550809	00250945	město	3539	446	Jihočeský kraj
Bečice	92	536156	00581178	obec	440	445	Jihočeský kraj
Bečice	73	563366	00512524	obec	324	432	Jihočeský kraj
Bednárec	109	562548	00512923	obec	781	530	Jihočeský kraj
Bednářeček	182	561053	00668874	obec	694	600	Jihočeský kraj
Bechyně	5226	552054	00252069	město	2122	406	Jihočeský kraj
Bělčice	1020	550817	00250953	obec	3432	526	Jihočeský kraj
Běleč	176	560448	00582506	obec	1223	457	Jihočeský kraj
Benešov nad Černou	1382	545406	00245780	obec	5706	661	Jihočeský kraj

Obrázek 3: Náhled do vygenerované databáze

⁹ Comma-separated values, hodnoty oddělené pouze čárkami, resp. středníky. Nezahrnují žádné formátování ani jiná specifika mezi sebou nekompatibilních programů (např. velikost písma, barvu buněk apod.).

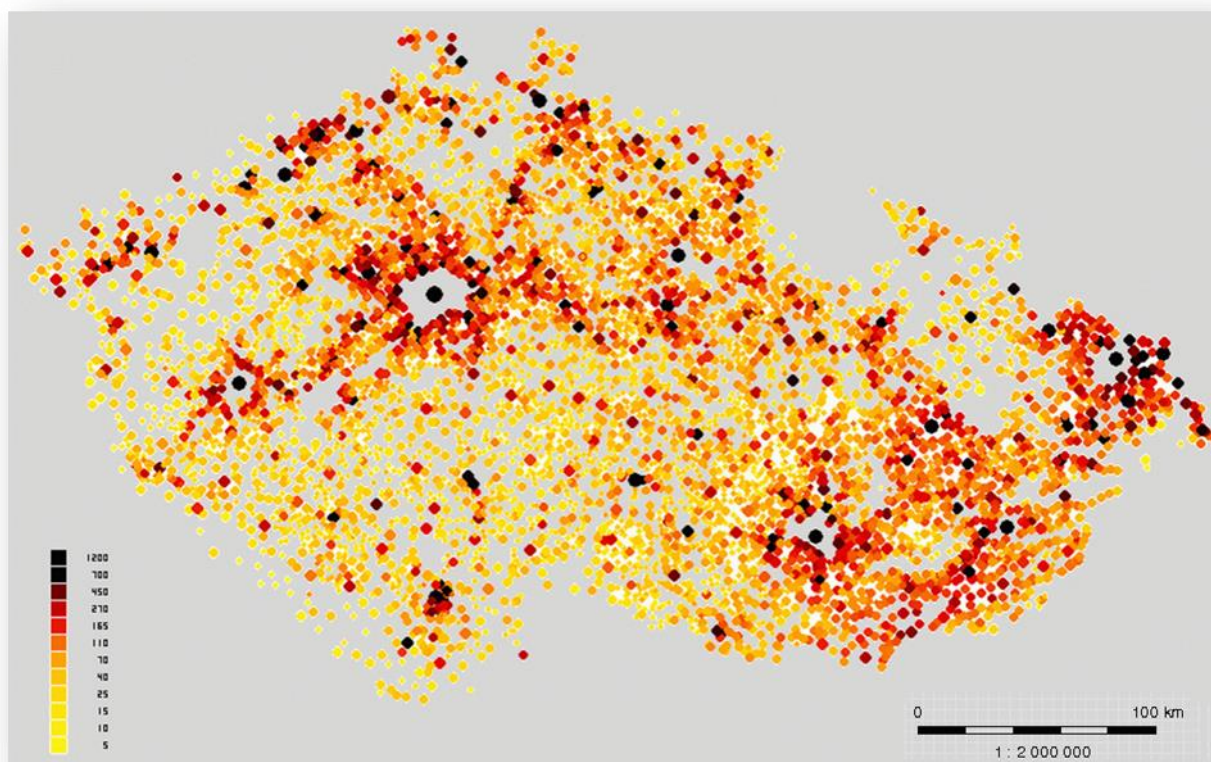
Grafické rozhraní

V grafickém rozhraní systému Digitálního modelu je k dispozici několik druhů zobrazení. Vzhledem k tomu, že je lze mezi sebou i kombinovat, není možné je zde všechny vypočítat.

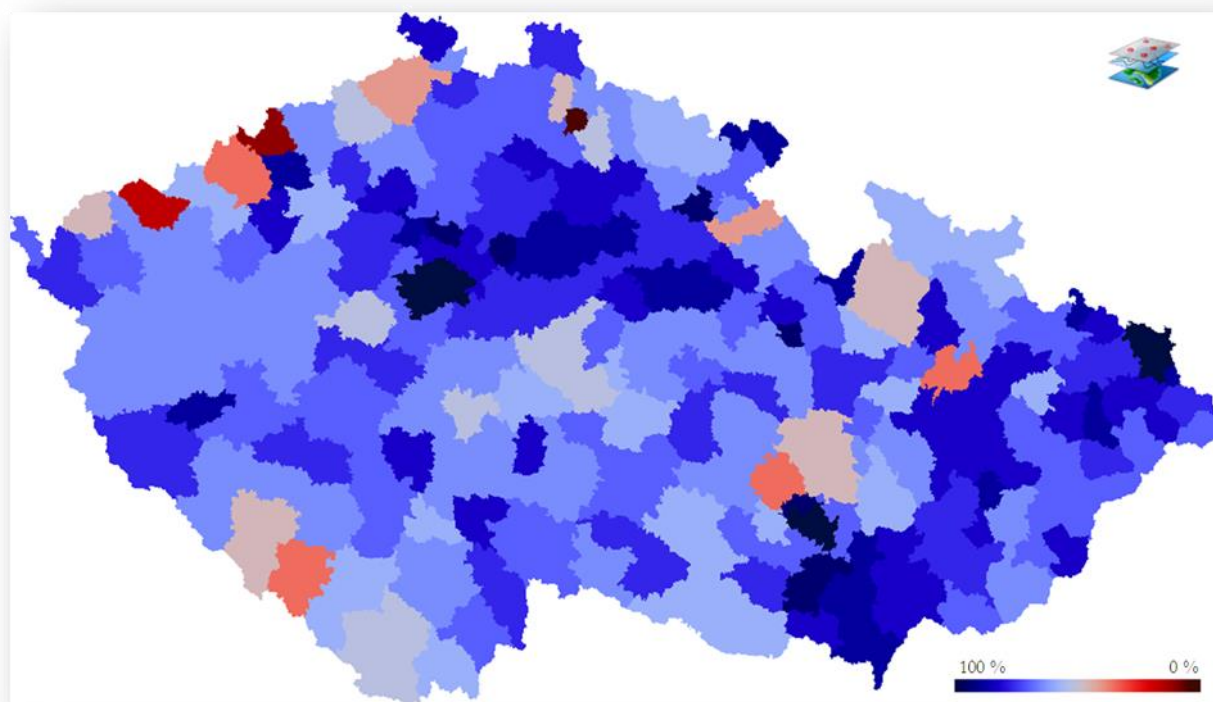
Mezi základní vizualizace patří:

1. Bodové mapy (obcí a center)
2. Katastrální hranice správních obvodů
3. Schematické mapy (logické propojování úřadů, operativní mapová vyjádření)
4. Rastrové mapy (rastr o velikosti několika kilometrů čtverečních dle volby)

Všechny uvedené vizualizace tvoří vždy jednu vrstvu map, kterou lze promítat na různé podklady, nejčastěji fyzické mapy.



Obrázek 4: Bodová mapa hustoty zalidnění v centrech obcí



Obrázek 5: Vizualizace jevu vážených indexů dostupnosti na všechny správní úřady

Simulování jevů ve veřejné správě

Simulovat lze na Digitálním modelu prakticky všechny hypotetické situace ve veřejné správě. Je možné posunout hranice správních obvodů, zvýšit či snížit počet konkrétních úřadů i jejich kategorií, počty obcí nebo kompletně přetvořit území. Simulované stavy jsou matematicky analyzovány a systém následně umožňuje nahlížet do důsledků, které jsou implikovány provedenými změnami. To znamená konkrétně nahlížet do důsledků finančních (přesné vyčíslení příspěvku na přenesenou působnost, finanční toky na určité agendy či územní celky), geografických (vizualizace území) či změn dostupnosti na jednotlivé úřady i v rámci obvodů obcí s rozšířenou působností nebo krajů.

Systém počítá i s dynamickými změnami. Lze simulovat stochastické jevy, migraci obyvatelstva, geografii rozvoje, ekologické dopady či predikovat vývoj. Na základě historicky známých faktů můžeme modelovat vývoj na mnoho let dopředu (s určitou pravděpodobností), nebo tyto fakty zohlednit pokud jde o potenciální zavádění koncepčních návrhů do praxe.

Finanční funkce, příspěvek na přenesenou působnost

Významným balíkem funkcí v DMVS jsou finanční funkce, zejména příspěvek na přenesenou působnost. Každá změna ve veřejné správě s sebou nese (kromě jiných důsledků) úspory nebo prodražení. Právě finanční stránka bývá v případě uvažovaných změn klíčová.

DMVS disponuje jednak funkcionalitami pro výpočet rozdělení příspěvku na přenesenou působnost (počítá samozřejmě s variabilní, nastavitelnou metodikou), funkcionalitami pro hledání specifických řešení (tj. např. provedení změn s ohledem na finanční objemy) nebo pro řešení s procentuální představou rozložení. Součástí balíku finančních funkcí jsou také rozsáhlé finanční analýzy.

Veškeré provedené změny tak může (uživatel)navrhovatel provádět experimentálně a kontrolovat finanční důsledky těchto změn¹⁰; nebo si vypočítat přesné náklady současného stavu. Konkrétní výstupy až po úrovni obcí a úřadů lze vždy exportovat do Excelu/Accessu.

Shrnutí

Digitální model nabývá tím větší významnosti, čím jsou potenciálně uvažované změny rozsáhlejší. Jeho úloha je nejpodstatnější při reformách veřejné správy.

Systém je navržen jako vysoce variabilní, aby bylo možné zpracovávat co nejširší spektrum změn a případů. Mezi jeho přednosti patří zejména **nízkonákladovost** a **uživatelská pružnost**. Datové registry může udržovat i aktualizovat běžný uživatel. Většinu změn lze provádět přímo na uživatelské úrovni.

K simulování situací, změn a koncepčních modelů je systém připraven prakticky okamžitě, uživatel nemusí složitě nastavovat nejjemnější parametry a odrazovat se množstvím technických detailů. Opačný stav vede uživatele často i u propracovaných a dobrých systémů k rezignaci.

Z dosavadní praxe je patrné, že existuje sílící tlak na to rozšířit jak funkcionality DMVS, tak přizpůsobit jej dalším oblastem. Na základě dnešních zkušeností se ukazuje nezastupitelnost tohoto systému v rovině analýz, expertních podkladů, statistických přehledů a optimalizačních hypotéz pro koncepční činnost v oblasti veřejné správy.

¹⁰ Např. hypoteticky by chtěl změnit hranice správních obvodů obcí s rozšířenou působností, může ihned prověřit, jaké finanční důsledky ve státním rozpočtu by daná změna znamenala.

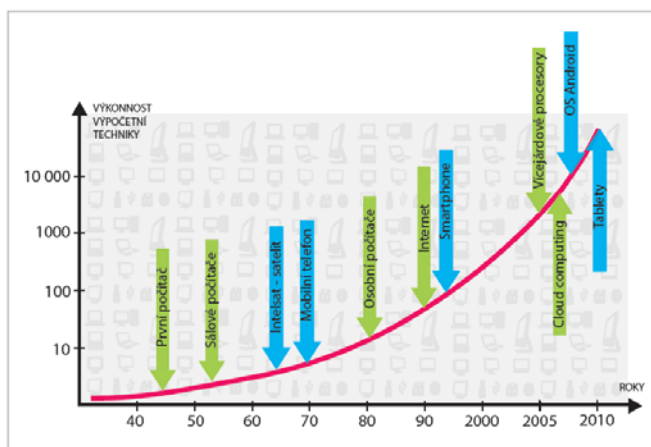
ZoKB – nutnost či zbytečný luxus? Bezpečnost?

Jitka Sládková, Jiří Sedláček, *Network Security Monitoring Cluster*

„To řeší IT...“ – nejčastější odpověď při setkání s technickým problémem v kanceláři. Stejně jako svým chováním můžeme předejít potenciálním problémům v běžném životě (např. jíst zdravě a sportovat abychom byli v dobré kondici), tak i svým přístupem k používání informačních a komunikačních technologií (ICT) můžeme mnohé ovlivnit. IT to sice „řeší“, viz. úvodní věta... **Byl ale opravdu nutný nežádoucí stav, kdy už je nutné „něco“ řešit? Proč máme Zákon o kybernetické bezpečnosti?** Co nám říká? Co z něj vyplývá? Máme se jím řídit, i když nemusíme? A skutečně nemusíme? Bude tomu tak i za rok? Dva? Pojďme se podívat na chápání ICT, Zákona o kybernetické bezpečnosti, povinností z něj vyplývajících a znalosti v oblasti ICT postupně.

Problematika ICT se dnes již netýká jen „ajtáků“. V minulém století zaznamenala lidská společnost obrovský technologický rozmach. S rozvojem vědy, techniky, technologií, s rostoucí lidskou populací, začaly vzrůstat nároky na zpracování dat. V 60. letech došlo k pokroku ve vývoji sálkových počítačů, které se používaly na řešení rozsáhlých statistických úloh, finanční transakce, řízení podniků. S rostoucí miniaturizací v elektronice měla výpočetní technika stále nižší prostorové nároky. V 70. letech se na trhu objevily první osobní počítače, které se díky klesající ceně pomalu ale jistě staly součástí našeho každodenního života. Zpočátku se jednalo o oddělené systémy, ale postupem času se začala řešit otázka jejich propojení z důvodu nutnosti sdílení informací. Začaly tak vznikat první počítačové sítě, zprvu lokálního charakteru. Tyto malé sítě byly postupně propojovány do rozsáhlejších struktur, až na začátku 80. let vznikla síť sítí – internet. To mělo obrovský dopad na kulturu, obchod, vznik elektronické pošty, sdílení informací.

Rozmach informačních a komunikačních technologií, především významné technologické milníky tohoto odvětví znázorňuje obrázek níže.



Zdroj: NSMC

Se stále rostoucím vlivem výpočetní techniky na náš každodenní život rovněž rostla potřeba **informace chránit**. A to nejen před jejich zneužitím či zcizením, ale i před jejich ztrátou. Pokud měl uživatel k dispozici jeden počítač, byl schopen více či méně úspěšně lokalizovat, chránit a uchovávat svá data. Stejně tak používal pouze aplikace instalované na tomto počítači a používal např. tiskárnu připojenou přímo k tomuto počítači. Časem vznikly lokální sítě, které se díky pokroku otevřely směrem ven do internetu. Od této doby se dostala potřeba ochrany dat a informačních systémů do zcela jiné roviny.

Přijdete ráno do práce, zapnete počítač, otevřete si poštu, spustíte web prohlížeč, spustíte program, se kterým každodenně pracujete, odkliknete tisk napsaného dokumentu, nebo tabulky... To jsou Vaše každodenní činnosti. **Jak ale zjistíte, proč Vám nebyl již dvě hodiny doručen žádný e-mail?**

Proč se dnes podniková aplikace tak loudá?

Jak to, že spuštění tisk dokumentu ještě nedorazil na tiskárnu?

Proč se Váš počítač chová dnes *divně*?

Jak to, že se ve Vašem webovém prohlížeči samovolně načítají stránky, které jste nevyvolali?

Jak je možné, že se kontakty Vašich zákazníků dostaly ke konkurenci a zrovna dnes Vám telefonovala úplně cizí paní, která tvrdila, že jí z Vaší mailové adresy chodí každý den desítky mailů, aniž jste jeden jediný poslali?

Je mnoho situací, které mohou nastat...

Jak lze chránit Vaše data před ztrátou či zneužitím?

Jak lze hlídat stav a kondici výpočetní techniky ve Vaší síti?

Jak lze zjistit, že došlo k průniku nebezpečného kódu, nebo hackera do Vaší sítě?

A jak se k této problematice staví náš stát?

Pochopitelně tak jak má – nastavením jasných pravidel – vydáním zákonné normy.

Zákon o kybernetické bezpečnosti je nový právní předpis, který vznikl za účelem zajištění bezpečnějšího kyberprostoru. Řeší prioritně ochranu státu, tedy aby fungovaly rozvodné sítě, aby nebyly ohroženy nemocnice výpadky energie, aby nedošlo k nečekanému vypouštění přehrad a jiným událostem, které mohou způsobit rozsáhlé majetkové škody či ztráty na životech. **Výpadek sítě státní správy může ovlivnit rychlost zpracování dávek sociální podpory. Několikadenní zpoždění může mít za následek vážné sociální dopady.** Kromě těchto závažných problémů přináší v dnešní době nefunkční ICT vždy minimálně finanční ztráty. **Dobře zabezpečené ICT jsou funkční a ekonomicky efektivní ICT. Jaké jsou tedy kroky k aplikaci ZoKB a reálnému zabezpečení sítě?**

Před nákupem různých zařízení je nutné *zrekapitulovat současný stav*, uvědomit si, co vlastně potřebuji a čeho chci dosáhnout, případně v jakém časovém horizontu toho chci dosáhnout. Z čeho se systém ICT v organizaci skládá. Na koho je napojen. S kým komunikuje a koho jeho nefunkčnost může ohrozit. Tedy jaká je architektura sítě – tj. kolik zařízení, jakého typu, jak a kam jsou napojena. Dalším krokem je *revize stávajících interních norem (politik)*, které standardizují nasazení a provoz ICT v organizaci, případně revize bezpečnostních předpisů vztahujících se k této oblasti. Klíčové je tedy provedení analýzy současného stavu a na základě zjištění definovat nutná opatření k nastolení požadovaného stavu. Až poté přichází na řadu *nákup zařízení, služeb*, atd. I zde však **koupit neznamená zabezpečit**. Každé zařízení musí být správně instalované, nakonfigurované, pravidelně aktualizované a udržované.

Shrňme si tedy shora naznačený postup:

- Analýza – popis současného stavu, revize politik, revize aktiv, monitoring sítě,
- definování požadovaného/cílového stavu,
- porovnání současného stavu s cílovým,
- vytvoření plánu, finančního a časového rámce k dosažení cílového stavu.

Tyto kroky je nutné v organizaci provést ať už interně nebo za pomoci specializovaných subjektů/firem, které také umí vyhodnotit postavení organizace z pohledu ZoKB a následně mohou doporučit nasazení potřebných technologií. Kdo je ale těmto subjektům partnerem? Je to pouze IT oddělení? Kdo rozhoduje o koupi doporučeného řešení či služeb? Je navržené řešení ekonomicky zdůvodnitelné?

Každý vedoucí či odpovědný pracovník by měl znát, jak a čím je zajištěn bezpečný chod ICT v organizaci a jaký to má pro fungování organizace význam. Víme, že to řeší pracovníci IT oddělení, nicméně vedení by mělo mít alespoň **základní přehled**. Jelikož technologie rostou jako houby po dešti, je relativně nesnadné se v nich zorientovat. Níže tedy uvádíme alespoň základní přehled pojmů, které je dobré znát.

Access control – jedná se o selektivní omezení přístupu do prostor, či k nějakým zdrojům. Z pohledu IT se může jednat např. o řízení přístupu k souborům (Access control list), IS, nebo do sítě.

Identity management – správa uživatelů. Aby měl identity management správná data a vedl uživatelské účty těch správných uživatelů, je třeba mít správný zdroj informací u uživatelích. Velmi často je tato podmínka opomíjena a uživatelé jsou ručně zakládáni administrátorem IT oddělení. Pokud je ale správa uživatelů „opřena“ o skutečně autoritativní zdroj dat – nejlépe personální systém (HR) dané organizace – je pak automaticky zajištěno přenesení všech potřebných změn, ke kterým dojde v personálním systému, také do identity managementu. Organizace pak má jistotu, že do IT systémů mají přístup jen relevantní uživatelé (kteří existují, jsou v zaměstnaneckém poměru), tzn. kteří jsou v aktuálním stavu v HR systému.

Log management – každé sofistikovanější zařízení, spadající do oblasti IT, vede vlastní provozní deník (tzv. log). Log management se zabývá sběrem a zpracováním těchto informací.

Asset management – jedná se o systémy pro řízení a správu provozních zdrojů (aktiv) organizace. Z pohledu IT se tedy převážně jedná o oblast softwarového a hardwarového managementu, který řeší dva důležité aspekty provozu IT oddělení – používání softwaru v souladu s licenční politikou a také nákladovou stránku.

Business continuity management – řízení kontinuity činnosti organizace. Jedná se o identifikaci potenciálních dopadů ztrát na činnost organizace. Cílem je vytvoření podmínek pro zajištění chodu organizace na předem stanovené minimální úrovni pro případ havárie.

Síťový a infrastrukturní monitoring – jedná se o sledování a vyhodnocování stavu zařízení, služeb v síti a dějů v síti. Dnes je běžné, že je prováděn v reálném čase, tzv. real time monitoring. Jeho výstupy jsou pak vyhodnoceny sofistikovaným softwarem. Tato technologie umožňuje mimo stavového monitoringu provádět i složitější analýzy síťového prostředí a může tak např. odhalit nežádoucí aktivity v síti (např. stahování dat). Analýza chování sítě se často provádí jako tzv. flow monitoring založený na paketové analýze.

Antivir a firewall – jedná se o nejběžnější způsob zabezpečení. Antivir chrání koncovou stanici – tedy počítač před virovou infekcí. Firewall zase určuje, jak a s kým počítač komunikuje. Problém může nastat v případě nesprávného nastavení, či když se neprovádí pravidelné kontroly a aktualizace.

DLP – Data Leak Prevention – jedná se o systémy, které zamezují úniku uživatelských dat a chrání tak před jejich zneužitím.

IDS/IPS systémy – Intruders Dection/Prevention System – jedná se o zařízení, která jsou schopna detekovat (případně zastavit) útoky v počítačové síti za použití tzv. signatur. Princip je podobný jako u antivirů. Pokud nemám aktuální databázi signatur, klesá účinnost tohoto nástroje. Oproti tomu metoda analýzy sítě za použití flow monitoringu je na signaturách zcela nezávislá.

SIEM – Security Information and Event Management – jedná se o správu bezpečnostních informací a událostí v reálném čase. Toto řešení umožňuje shromažďovat, analyzovat a prezentovat informace ze sítě a bezpečnostních zařízení, pomáhá spravovat identity a přístupy, analyzuje ohrožená místa, shody s bezpečnostními politikami atd. Základem tohoto řešení je zpracování logů (Log Management).

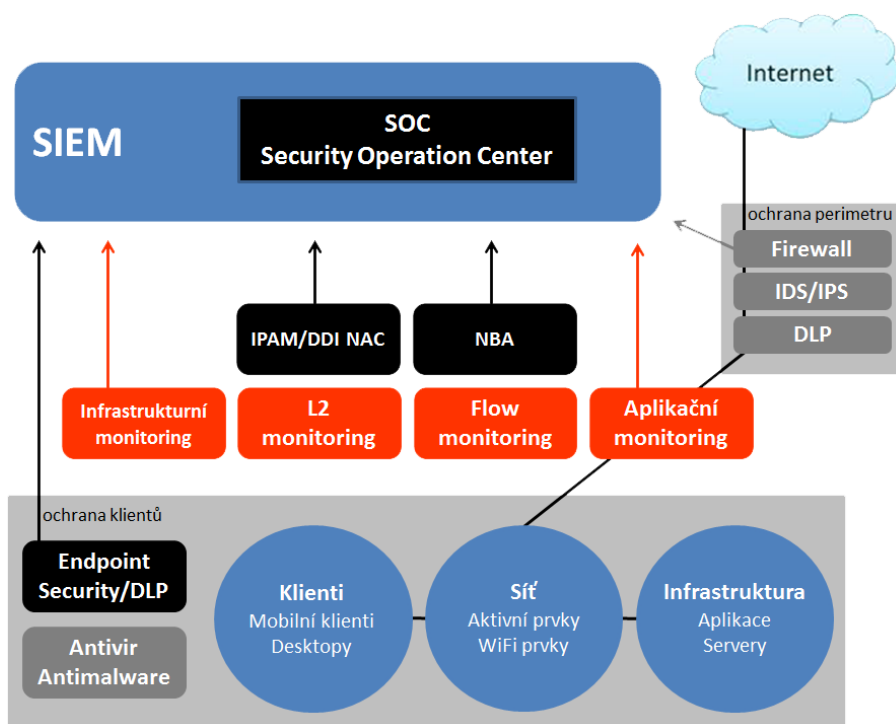
SOC – Security Operations Center – dohledové centrum zajišťující monitoring bezpečnostních událostí, reakci na tyto události, přijímání nápravných opatření a reporting. Jedná se o placenou službu se vzdáleným přístupem. Umožňuje monitoring bezpečnosti ICT v režimu 24/7/365. V současnosti se jedná o nejpokročilejší řešení bezpečnosti v ICT v souladu se ZoKB.

Vraťme se ale k původní otázce. Je nutné rozlišovat koho se ZoKB týká? Dle našeho názoru není. V dnešní době je zcela zjevné, že počítačová bezpečnost je nedílnou součástí ICT každé organizace. Nehledě na tuto skutečnost, již před přijetím ZoKB – zákona 181/2014 Sb., existovala zákonná norma vztahující se na informační systémy veřejné správy – zákon 365/2000 Sb. Co se tedy týká veřejné správy, zákonné normy existují, rámec je jasně vymezen.

Kybernetická bezpečnost má v podstatě dvě roviny. První je rovina evangelizační, druhou je rovina technická. Bez potřebných znalostí, orientace a povědomí o čem je bezpečnost v oblasti ICT, není možné prová-

dět nákup a následné nasazení potřebných služeb a technologií. Z tohoto důvodu začaly vznikat jak univerzitní kurzy, tak komerční vzdělávací programy.

Jak již bylo výše uvedeno, existuje mnoho subjektů, které se zabývají kybernetickou bezpečností. Jedním z nich je NSMC – Network Security Monitoring Cluster. Klastř spolupracuje s českými i zahraničními organizacemi, univerzitami a sdružuje 21 českých odborných firem zabývajících se počítačovou bezpečností. Portfolio NSMC dostatečně pokrývá celou oblast ICT. Jeho koncept aktivní bezpečnosti a spolehlivosti IT infrastruktury (viz obrázek níže) je unikátní a v souladu se ZoKB. Podstatou je pyramidové využití jednotlivých dostupných nástrojů k zabezpečení počítačové sítě. Do jaké míry je možno jej využít, tedy aplikovat, závisí na několika faktorech, např. velikosti dané sítě, napojení na kritickou infrastrukturu atd.



NSMC koncept aktivní bezpečnosti a spolehlivosti IT infrastruktury

V rovině evangelizační nabízí NSMC, jako nezávislý odborník na bezpečnost počítačových sítí, ve spolupráci s Masarykovou univerzitou, školení jak pro manažery, tak i pro IT specialisty, se zaměřením právě na vhodné zabezpečení ICT v organizaci. Školení je doplněno o možnost reálné simulace a návrhu zabezpečení ICT jednotlivých účastníků (tedy jejich organizací), v souladu se ZoKB.

V rovině technické nabízí NSMC komplexní služby od analýzy Vašeho prostředí až po návrh řešení a realizaci. Umožní Vám tedy nejen rozšířit obzory a usnadnit Vám tak orientaci v oblasti ICT a kybernetické bezpečnosti, ale také nasadit efektivní řešení v souladu s vašimi potřebami a ZoKB.

Více informací na www.nsmcluster.com, nebo pište na info@nsmcluster.com

Boj s korupcí zahrnuje i vzdělávání

Ondřej Štrba, Technology Unit Manager, Servodata a.s.

Jedním z primárních témat práce ve státní správě je v současné době boj s korupcí. Nyní je jeho nedílnou, povinně vyžadovanou součástí i protikorupční vzdělávání zaměstnanců ministerstev a úřadů.

Usnesením vlády ze dne 2. října 2013 č. 752 byl schválen Rámcový rezortní interní protikorupční program, který představuje závaznou osnovu pro vytvoření protikorupčních programů v jednotlivých rezortech ministerstev a ústředních správních úřadů. Kapitola 1.3 této osnovy stanovuje povinnost pravidelného školení zaměstnanců na všech referentských i vedoucích úrovních se zaměřením na protikorupční tematiku. Tuto povinnost lze nejlépe splnit prostřednictvím elektronického protikorupčního kurzu, poskytovaného společností Servodata.



Povinnost implementovat protikorupční program, jehož nedílnou součástí je i školení zaměstnanců, se vztahuje na všechna ministerstva a ústřední správní orgány. Termínem splnění je nejpozději konec roku 2015. „Rámcový rezortní interní protikorupční program stanovuje obsah protikorupčního vzdělávání, ovšem nikoli formu, jakou je třeba jej realizovat,“ říká Marcela Kuchelová, Business Unit Manager Microsoft ve společnosti Servodata. „Proto je možné, a po všech stránkách výhodné, využít elektronickou formu realizace vzdělávacího kurzu a ověření nabytých znalostí.“

Nezbytnou přípravu na boj proti korupci lze realizovat rychle a flexibilně, bez negativních dopadů na chod organizace. Servodata za tímto účelem nabízí kompletní platformu pro vzdělávání, materiály ke školení i testy pro ověření nabytých znalostí. Vzdělávací řešení Servodat lze provozovat přímo na serverech organizace, která potřebuje proškolit své zaměstnance, popřípadě ji využívat formou hostingu prostřednictvím portálu pro studium elektronických kurzů.

Píliře protikorupční politiky

Nástroje a procesy protikorupční politiky vycházejí z identifikace projevů a analýzy příčin korupčního jednání. Po volbě preventivních a represivních protikorupčních nástrojů a jejich zavedení do praxe následuje vyhodnocování účinnosti nastavené protikorupční strategie.

Realizace protikorupčního kurzu zahrnuje:

- **Vzdělávací platformu** integrovatelnou se stávajícími informačními systémy organizace.
- **Výukový obsah** splňující požadavky Vládní koncepce boje s korupcí.
- **Testy** prokazující znalosti proškolených zaměstnanců.

Obsah elektronického protikorupčního kurzu:

- Definice korupce a její typy.
- Negativní dopady na společnost.
- Právní úprava podle českého trestního zákona.
- Protikorupční politika ve veřejné správě.
- Identifikace projevů a analýza příčin korupčního jednání.
- Výskyt korupce v rámci jednotlivých správních činností a indikátory korupce.
- Identifikace účinných preventivních i represivních protikorupčních nástrojů a jejich zavádění do praxe.
- Kontrola ve veřejné správě.
- Protikorupční nástroje osobního (služebního) charakteru.
- Represivní nástroje.
- Zvláštní protikorupční nástroje ve vybraných činnostech veřejné správy.
- Protikorupční nástroje ve správním řízení.
- Přidělování dotací, přidělování prostředků z EU fondů.
- Nakládání s majetkem územních samosprávných celků (ÚSC).
- Veřejné zakázky (VZ).
- Vyhodnocování účinnosti strategie a zajištění její udržitelnosti.
- Pojmy z oblasti boje proti korupci.
- Whistleblowing.
- Protikorupční linka.
- Mezinárodní obchodní komora (International Chamber of Commerce – ICC).
- Zpráva o boji proti korupci v ČR.

„Zvláštní důraz je kladen na oblasti, ve kterých hrozí zvýšené riziko korupčního jednání, jako jsou správní řízení, přidělování dotací a rozdělování prostředků z fondů Evropské unie, zadávání veřejných zakázek či nakládání s majetkem územních samosprávných celků a zadávání veřejných zakázek,“ dodává Marcela Kucbelová.

Realizace protikorupčního vzdělávání

Hlavní výhoda elektronického vzdělávacího kurzu spočívá ve snadném a efektivním splnění povinností plynoucích z protikorupčního programu. Organizace mají protikorupční vzdělávání plně pod kontrolou a jejich zaměstnanci jej mohou absolvovat ve vhodné dobu, aniž by realizace školení znamenala dodatečné náklady na cestování nebo nepřítomnost zaměstnanců na pracovišti.

- **Školení na míru:** Protikorupční kurz vychází z podkladů definovaných Vládní koncepcí boje s korupcí. Může být ovšem upraven na míru dle Interních protikorupčních programů jednotlivých ministerstev či státních subjektů.
- **Nezávislé na místě a čase:** K elektronickému protikorupčnímu kurzu mají zaměstnanci přístup odkudkoli a kdykoli – stačí jen připojení k internetu.
- **Úspora nákladů:** Díky řešení společnosti Servodata lze splnit povinnosti protikorupčního vzdělávání při minimálních nákladech. Výukové materiály je možné snadno aktualizovat, pro realizaci školení není třeba platit lektora, pronajímat učebny ani nikam cestovat.
- **Interaktivní a atraktivní:** Interaktivní forma výuky s výkladem problematiky písmem, slovem, grafikou, animacemi a dalšími multimediálními prvky je lákavá pro všechny zaměstnance, které je nezbytné proškolit.
- **Ověření znalostí:** Nezbytnou součástí protikorupčního vzdělávání je ověření znalostí získaných absolvováním elektronického kurzu.

„Zájemcům z ministerstev a správních úřadů poskytujeme testovací verzi elektronického kurzu k vyzkoušení. Pro její získání se stačí obrátit na kontakty společnosti Servodata,“ uzavírá Marcela Kucbelová.

Profesionální partner pro protikorupční školení

Díky svým bohatým zkušenostem a vynikajícím odborným znalostem při realizaci významných vzdělávacích projektů financovaných z Evropského sociálního fondu (ESF) si společnost Servodata vybudovala pozici významného vzdělávacího centra. V současnosti se Servodata řadí mezi nejvýznamnější vzdělávací střediska v ČR.



Elektronické kurzy Servodat, určené pro státní správu a samosprávu:

- Microsoft Office 2013 (Word, Excel, PowerPoint)
- Windows 7
- Bezpečnost práce
- Požární ochrana
- Školení řidičů
- První pomoc
- Základní pojmy informačních technologií
- Práce s PC a správa souborů
- Textový editor
- Tabulkový procesor
- Účetní metodik
- Samostatný účetní

Další elektronické kurzy je možné připravit na míru, dle konkrétních potřeb dané organizace.

O společnosti Servodata

Servodata patří mezi nejvýznamnější platform providery v České republice a na Slovensku. Díky rozsáhlé transformaci a strategickému zaměření na komplexní ICT řešení vyhrála společnost Servodata prestižní ocenění IT projekt roku 2014 a potvrdila tak nejen svou vysokou technologickou úroveň, ale také schopnost realizace náročných řešení v praxi.

Kombinací dodávek technologií předních světových dodavatelů (Microsoft, Red Hat, EMC a další), služeb souvisejících s jejich implementací a provozem, odborných i uživatelských školení, a v neposlední řadě také inovativních řešení nad těmito technologiemi, pomáháme významným komerčním zákazníkům i státní a veřejné správě vytvářet a rozvíjet celopodnikové informační platformy a optimalizovat jejich využití.

Eskorty budou minulostí. Vyslýchané posadí před kameru

Květoslav Štrunc, Cisco Systems (Czech Republic) s.r.o.

Přesuny obviněných či odsouzených z jednoho konce republiky na druhý jen kvůli hodinovému či kratšímu výslechu budou zřejmě brzy minulostí. Místo drahého převozu s ozbrojenou eskortou bude stačit doprovod strážným do místnosti uvnitř věznice, kde bude nainstalováno videokonferenční zařízení. Výslech pak proběhne naprosto standardně, nicméně dlouhou cestu nahradí obrazovka a kamera.

Na první pohled by se mohlo zdát, že moderní technologie se v trestním či soudním řízení mohou uplatnit jen u forenzních techniků. Není to ale tak docela pravda, moderní technologie mohou výrazně proměnit stávající průběh řízení, přinést jeho zrychlení, ale zároveň i zlevnění. Ačkoli se někdy zdá, že snaha uspořit prostředky může vést ke komplikacím, nemusí to tak být vždycky. Příkladem může být nasazení videokonferenčních technologií pro komunikaci jak v trestním, tak soudním řízení.

Projekty se blíží do finále

Na zavedení videokonferenčních systémů získalo Ministerstvo spravedlnosti ve svém rezortu podporu v rámci programu Budování kapacit a spolupráce v rámci justice a nápravné služby včetně alternativních trestů (CZ 15) z tak zvaných Norských fondů. Projekt by měl skončit na konci dubna příštího roku, takže na jeho finální realizaci zbývají už jen poslední měsíce.

Projekt se týká jak samotného Ministerstva, jako ústředního orgánu státní správy, tak 86 okresních, osmi krajských, dvou vrchních a obou nejvyšších soudů v Česku, tedy Nejvyššího soudu ČR a Nejvyššího správního soudu. Do projektu jsou také zahrnuta obě nejvyšší státní zastupitelství a dvanáct vazebních věznic. Výše grantu činí 1 845 422 euro, což by mělo pokrýt přibližně 80 procent nákladů na celý projekt.

V červnu loňského roku se navíc podařilo získat dodatečné finanční prostředky ve výši 130 milionů korun z Norských fondů, které jsou určeny na zkvalitnění české justice, vězeňství a další odborný rozvoj Probační a mediační služby. Díky tomu mohl být připraven projekt pro vybudování nového komunikačního systému, který umožní plošné využívání videokonferencí.

Návratnost v řádu let

Jen náklady na střežení vězněných osob eskortovaných k orgánům činným v trestním řízení činily v první polovině letošního roku 39,4 milionu korun. Dalších 5,6 milionu Kč vydala Vězeňská služba ČR za dopravu těchto osob. To znamená celkem 45 milionů. Jejich značnou část by se mohlo podařit ušetřit s větším nasazením videokonferencí do soudního a trestního řízení.

Dokazují to zkušenosti z pilotního projektu, ve kterém je zapojena Policie ČR. Pilotní projekt, na kterém spolupracovala, jako dodavatel technologií také společnost Cisco ukázal, že právě v oblasti dopravy lze dosáhnout nezanedbatelných úspor, stejně jako v oblasti lidských zdrojů. V současnosti je potřeba například při eskortě zadržené osoby tři policistů. Podobná pravidla platí i v případě Vězeňské služby.

V tomto případě se navíc přidávají možné úspory v oblasti systému hromadných svozů k přemístění a umístění vězněných osob.

Ministerstvo spravedlnosti odhaduje, že rozšíření projektu videokonferencí by mohlo přinést celkové úspory až 25 milionů korun za pololetí. A to jistě není pro daňového poplatníka zanedbatelná částka. Další úspory lze očekávat v oblasti lidských zdrojů, logistiky i dalších běžných výdajů. V neposlední řadě by uvedení celého projektu v život mělo pomoci najít nový způsob komunikace také mezi orgány policie a justice, ale současně i k lepší komunikaci napříč resorty vnitra a spravedlnosti.

Velmi jednoduchým propočtem zjistíme, že investovaná částka (i bez započítání podpory) se vrátí České republice během pouhých pěti let pouze na přímých úsporách. Přínosy nasazení těchto technologií budou ale

mnohem širší a otevrou cestu ke zrychlení trestního řízení a tím i ke zvýšení vymahatelnosti práva v celé České republice.

Levněji neznamená hůře

Velmi častou příčinou průtahů v trestním i soudním řízení bývají omluvy obviněných, svědků a dalších zúčastněných osob. Vytěžení svědka tak pro příslušníky Policie ČR nebo soudy často znamená několik zbytečných cest nebo nařízených stání. Právě snaha o zkrácení času mezi jednotlivými úkony a snížení nákladů na dopravu vedlo Ministerstva vnitra i spravedlnosti ke spuštění tohoto projektu.

Možnost propojení orgánů Policie ČR i jednotlivých orgánů státní moci pomůže velmi výrazně eliminovat některé příčiny průtahů v trestním i soudním řízení. Eskorty obviněných či odsouzených k soudům bude možné v nemalém procentu případů nahradit výsledkem přes videokonferenci přímo ve věznici. Stejně tak nebude muset například soud odkládat líčení jen proto, že svědek či jiný účastník onemocněl. Videokonferenční zařízení lze nainstalovat v nemocnici a účastník řízení tak může vypovídat klidně ze svého nemocničního lůžka pod dozorem lékařů. To se může týkat zraněných či nemocných, ale například také osob hospitalizovaných v ústavech (například tělesně a duševně postižení, dlouhodobě nemocní atp.). Až dosud výslech takovýchto osob znamenal průtahy zejména v soudním líčení. Bylo nutné jednání soudu odročovat, či nařizovat zvláštní jednání například v prostoru nemocnice.

Nyní bude stačit například dopravit k nemocnému videokonferenční terminál, a může dojít k jeho výsledku za stejných podmínek, jako by se fyzicky účastnil jednání v budově soudu. Stejně tak lze například jednoduše vyslechnout obviněného, který byl již v jiném případě odsouzen a v současné době vykonává trest například ve věznici vzdálené několik stovek kilometrů.

Mezinárodní spolupráce

Videokonference jako nástroj pro výslech účastníků řízení navíc připouští i Evropská unie. Jde mimo jiné o směrnici Rady týkající se odškodňování obětí trestných činů, nařízení Evropského parlamentu a Rady (ES) č. 861/2007, kterým se zavádí evropské řízení o drobných nárocích, rámcové rozhodnutí Rady Evropské unie o postavení obětí v trestním řízení a celou řadu dalších předpisů.

Podobné projekty jako Ministerstvo spravedlnosti a Policie ČR připravují (nebo již realizovaly) i další evropské státy. To samozřejmě otevírá prostor pro mezinárodní spolupráci. České orgány tak budou moci jednoduše vyslechnout třeba belgického svědka dopravní nehody, aniž by mu museli platit cestu do České republiky a čekat, až dorazí k výsledku před českými soudy či orgány Policie. Jednoduše požádají partnerský orgán v dané zemi o spolupráci a vyslechnou ho, aniž by musel opustit své bydliště.

Technologie totiž dovolují používat nejen hardwarová zařízení, ale do videokonference lze připojit i účastníky z jejich vlastních počítačů pomocí softwarového klienta Cisco Jabber Guest. Díky tomu může soud velmi jednoduše přizvat k výsledku například tlumočníky, znalce nebo dokonce i některé svědky. I to může znamenat nejen další zrychlení jednání, ale také významné úspory za cestovní náklady.

Ochotnější svědci

Jak ukazují zkušenosti policie, zavedení videokonferencí do resortu Ministerstva spravedlnosti může mít ještě jeden podstatný rozměr z hlediska veřejnosti. Je jím mnohem větší komfort a ochrana, kterou tyto technologie přinesou obětem trestných činů a poškozeným. Pro velkou většinu z nich je přímé setkání s pachatelem během trestního či soudního řízení velmi frustrujícím zážitkem.

Velmi výrazně prožívají taková setkání zejména oběti znásilnění, ale ani pro ostatní postižené rozhodně nejde o příjemný zážitek. Při stávajícím způsobu vedení se navíc poškozený musí s pachatelem setkat hned několikrát. Policie během vyšetřování může k objasnění skutku potřebovat provedení konfrontace či reko-

gnice. A i když v druhém případě lze provést tento úkon v utajení (například za jednostranným zrcadlem), poškozený je fyzickému kontaktu s pachatelem či podezřelým subjektivně vystaven. Navíc, společnou přítomností pachatelů či obviněných a svědků v jednom místě může dojít nedopatřením nebo opomenutím k narušení anonymity. To mívá často neblahé důsledky pro další postup trestního či soudního řízení.

Videokonference tento problém zcela eliminují. Všichni účastníci mohou být na fyzicky zcela odlišných místech. Podezřelý například ve vazebních prostorech, svědci či poškozený na pro ně nejbližší služebně Policie ČR či na jiném vhodném místě. V případně rekognice je tak naprosto vyloučena jakákoli možnost náhodného prozrazení vytěžované osoby podezřelému. A také v případech konfrontace se poškození nebo svědci cítí obvykle jistěji v případech, kdy nedochází k přímému kontaktu. Větší bezpečnost, kterou subjektivně cítí poškození či svědci, se může příznivě odrazit v jejich větší ochotě spolupracovat s orgány činnými v trestním řízení i justice. Počet omluv plynoucích ze snahy oddálit či vyhnout se setkání s pachatelem, může díky tomu poklesnout.

Fyzické oddělení podezřelých (pachatelů) a poškozených navíc dává soudu prostor pro mnohem aktivnější a jednodušší využití institutu utajeného svědka. Podobně jako v případě přípravného řízení na policii, i při jednání soudu byla nutnost fyzické přítomnosti utajeného svědka ve stejné budově s obviněným potenciálně rizikovým faktorem. Nedopatřením či například zlým úmyslem mohlo dojít k prozrazení jeho totožnosti, a tím ke zmaření celého řízení.

Výslech utajeného svědka prostřednictvím videokonference tyto problémy téměř zcela eliminuje. Technologie modifikace obrazu a hlasu dokáže znemožnit odhalení totožnosti svědka obviněným, zároveň ale dávají tyto technologie soudu dostatečnou možnost tuto totožnost ověřit.

Bezpečnost i kvalita

Nepřekročitelnou podmínkou zavedení videokonferencí do trestního a soudního řízení je samozřejmě otázka bezpečnosti a informační integrity přenosu. Proto není v žádném případě možné využít řešení v podobě bezplatných komunikačních nástrojů, u nichž by mohlo snadno dojít k narušení spojení mezi koncovými body videokonference, což by mohlo vést ke zpochybnění výsledků. Systém musí být proto dostatečně robustní, aby byl schopen odolat kybernetickým útokům a nemohl zavdat jakoukoli pochybnost ohledně autentičnosti výpovědi.

Velmi důležitým aspektem, který možná v konečném důsledku rozhodne o nasazení videokonferenčních technologií do reálné praxe, je kvalita. Není samozřejmě přípustné, aby během jednání soudu či například výslechu svědka docházelo k výpadkům obrazu či zvuku. Tím by mohly vzniknout nesrovnalosti, nebo by docházelo k neúměrnému prodlužování jednání. Nejnovější generace videokonferenčních systémů společnosti Cisco, která je partnerem celého projektu, ale podobné nedostatky zcela eliminují.

I na méně kvalitních linkách dokážou algoritmy Cisco zajistit přenos obrazu i zvuku ve vysoké kvalitě HD. To zaručuje, že i na větší vzdálenost přenos všech nuancí v hlase či mimice vyslychaného. Pro soud je tak jen velmi malý rozdíl mezi skutečnou fyzickou přítomností dané osoby při jednání a vzdáleným výsledkem přes videokonferenci.

Samozřejmostí videokonferenčního řešení je propojení více účastníků do jedné konference. Každý z účastníků může přirozeně být na jiném místě. A tak se jednoduše k výslechu obviněného může soudce například přizvat právě znalce. Nejde ale jen o samotný přenos obrazu. Videokonference může být přímo připojena do informačního systému Evidence trestního řízení, takže vyslychaná osoba (a případně i její obhájce) může přímo sledovat protokolaci procesního úkonu.

Systém je navíc vybaven tak, aby bylo možné na dálku přenášet mezi všemi body také dokumenty. Je schopen přenášet, skenovat či prezentovat různé písemnosti, podklady, či poučení na jedné z obrazovek přímo při procesním úkonu.

Zákonná úprava

Současné znění trestního řádu na využití videokonferencí v trestním řízení pamatuje. Jedná se zejména o § 52a a 53 odst. 1 tr. ř., které stanovují, že využívat videokonferenční zařízení je možné, je-li to potřebné pro ochranu práv osob, zejména s ohledem na jejich věk nebo zdravotní stav, nebo vyžadují-li to bezpečnostní nebo jiné závažné důvody, a dále, že videokonferenční technikou lze nahradit i úkony dožádání, jejichž provedení vyžadují orgány činné v trestním řízení mimo svůj obvod.

V § 69 odst. 4 tr. ř. je dále stanoveno, že policejní orgán, který obviněného na základě příkazu zatkl, je povinen ho neodkladně, nejpozději do 24 hodin dodat k příslušnému soudu nebo na místo umožňující tomuto soudu provést výslech prostřednictvím videokonferenčního zařízení. A nakonec § 445 odst. 1 tr. ř. nelze-li předvolat k výslechu do České republiky podezřelého, obviněného, svědka nebo znalce, předseda senátu a v přípravném řízení státní zástupce může požádat příslušný orgán cizího státu o zajištění výslechu prostřednictvím videokonferenčního zařízení.

Kybernetická bezpečnost

Ing. Igor Štverka, MBA, Sales Manager GORDIC spol. s r. o.

Schválení zákona o kybernetické bezpečnosti je zásadním krokem pro řešení bezpečnosti informačních systémů, a to nejen v oblasti organizací veřejné správy. Produkty a služby dodávané společností GORDIC představují komplexní řešení kybernetické bezpečnosti s ohledem na právě přijatou legislativu.

- Komplexní řešení kybernetické bezpečnosti
- Analýza informačních aktiv, zranitelných míst a případných hrozeb
- Důkladná znalost IT prostředí veřejné správy
- Špičkové, odzkoušené a cenově dostupné komponenty

Cyber Security GINIS

Jádrem řešení kybernetické bezpečnosti v pojetí GORDIC je tzv. bezpečný produkt GINIS. Pro uživatele systému byla připravena sada komponent pro podporu a vylepšení těchto instalací tak, aby zvedla hladinu tzv. aplikační bezpečnosti na nově požadovanou úroveň. Tyto komponenty se označují jako moduly CSG: Cyber Security GINIS. Umožňují bezpečnou správu identit, zabezpečenou komunikaci se systémy třetích stran, monitoring chybových hlášení a upozorňování na ně, bezpečnou správu a ukládání elektronických dokumentů, atd.

Základní registry jedou naplno!

Návod pro občana: Co mám dělat, když si měním adresu trvalého pobytu?

Zpracoval: Správa základních registrů a Ministerstvo vnitra ČR



Co mám dělat, když si měním adresu trvalého pobytu?

Už od poloviny roku 2012 se můžete spolehnout na tzv. základní registry, které zajišťují, že už nemusíte obíhat všechny úřady a hlásit změnu na každém úřadě zvlášť. Většina úřadů si data, která potřebuje, předává díky registrům mezi sebou automaticky.

Následujícím textem nás provede Jan Novák.

První krok - místně příslušný obecní úřad.



Jan Novák se přestěhoval. Jeho první zastávkou je obecní úřad v místě nového trvalého pobytu. Vyplní tam a podepíše přihlašovací lístek k trvalému pobytu. Předloží platný občanský průkaz a doklad, který ho opravňuje užívat byt nebo dům (např. výpis z katastru nemovitostí, kupní smlouvu, nájemní smlouvu) anebo úředně ověřené písemné potvrzení oprávněné osoby (např. majitele nemovitosti) o souhlasu s ohlášením změny místa trvalého pobytu a opět doklad, který to dokazuje (např. výpis z katastru nemovitostí). Úředně ověřené potvrzení se nevyžaduje v případě, že oprávněná osoba potvrdí svůj souhlas na přihlašovacím tiskopisu přímo na úřadu a předloží i doklad o oprávněnosti užívání bytu či domu. Dále je povinností Jana Nováka požádat o nový občanský průkaz na obecním úřadě s rozšířenou působností podle místa nového trvalého pobytu.

Katastrální úřad.



Na katastrální úřad nemusí Jan Novák nic oznamovat. Data si tento úřad aktualizuje automaticky. Správnost nové adresy je možné ověřit na veřejném portále Českého úřadu zeměměřického a katastrálního v sekci „Nahlížení do katastru nemovitostí“ <http://nahlizeniidokn.cuzk.cz/>.

Zdravotní pojišťovna.



I když jsou k základním registrům připojeny všechny tuzemské zdravotní pojišťovny, stále však platí pro Jana Nováka oznamovací povinnost dle zákona o veřejném zdravotním pojištění. Musí tedy do 30 dnů od přestěhování tuto změnu své pojišťovně oznámit bez ohledu na to, zda pojišťovna provede změnu sama. Pokud je situace, že se Jan

Novák v místě trvalého pobytu nezdržuje, je povinen příslušné zdravotní pojišťovně oznámit také adresu místa pobytu na území ČR, kde se převážně zdržuje.

Finanční úřad.



Všechny finanční úřady jsou k základním registrům napojeny. Dejte ale pozor na to, že finanční úřady rozlišují, zda v daňovém řízení je daňový subjekt (v našem případě Jan Novák) u finančního úřadu registrován či nikoliv. Též je nutné rozlišovat, zda se daňový subjekt přestěhuje v rámci územní působnosti finančního úřadu (tj. v rámci kraje, resp. v rámci Prahy) či mimo tuto územní působnost (např. z Prahy do Brna).

Pokud se Jan Novák přestěhuje mimo územní působnost finančního úřadu a u finančního úřadu není registrován, zašle původně místně příslušný finanční úřad Janu Novákovi oznámení o změně místní příslušnosti (ve kterém mimo jiné uvede, u kterého územního pracoviště příslušného finančního úřadu bude uložen jeho daňový spis). Pokud se však jedná o registrovaný daňový subjekt, který se přestěhuje mimo územní působnost finančního úřadu, vydá finanční úřad rozhodnutí o stanovení data konce místní příslušnosti a teprve tímto datem, tedy dnem výslovně uvedeným v tomto rozhodnutí, přechází místní příslušnost na finanční úřad podle nové adresy trvalého pobytu Jana Nováka. Pokud se Jan Novák přestěhuje v rámci územní působnosti finančního úřadu (např. z Děčína do Litoměřic), bude jeho daň spravovat totožný finanční úřad, avšak jeho spis bude ve většině případů přesunut na jiné územní pracoviště tohoto finančního úřadu.

Speciální kategorií jsou daňové subjekty, jejichž místní příslušnost byla před přestěhováním delegována. Po přestěhování Jana Nováka v takovémto případě tak nedojde automaticky ke změně finančního úřadu, ale musí být rozhodnuto o zrušení, změně nebo potvrzení delegace.

Řidičský průkaz a registr vozidel.



Řidičský průkaz:

Pokud Jan Novák mění adresu trvalého pobytu v rámci jedné obce, nemá povinnost tuto změnu oznamovat. Jestli se však Jan Novák stěhuje z jedné obce do druhé (v praxi častější případ), musí tuto změnu nahlásit do pěti pracovních dnů na příslušném obecním úřadu obce s rozšířenou působností tam, kam se přestěhoval. Za změnu údajů v řidičském průkaze zaplatí správní poplatek ve výši padesáti korun.

Co s sebou?

Starý řidičský průkaz
Občanský průkaz
Pasovou fotografii

Registr vozidel:

Jestli Jan Novák vlastní automobil, bude ho čekat také cesta na registr vozidel, kde bude muset změnu adresy trvalého pobytu nahlásit z důvodů doplnění údajů do velkého technického průkazu a výměny malého technického průkazu. Změnu je třeba nahlásit do 10 pracovních dnů. Za změnu tohoto údaje je stanoven správní poplatek ve výši 50 Kč.

Co s sebou?

Velký i malý technický průkaz
Průkaz totožnosti

Od 1. 1. 2015 však nastala změna oproti minulému roku týkající se výměny registrační značky v případě stěhování do jiného kraje. V tomto případě již zůstane Janu Novákovi původní registrační značka. To ovšem neplatí v případě, pokud je třeba registrační značku vyměnit z důvodu ztráty, poškození, zničení či odcizení. V tomto případě je zde stanoven správní poplatek ve výši 50 Kč za přidělení nové registrační značky a poplatek 400 Kč za vydání 2 ks tabulek s přidělenou registrační značkou.

Úřad práce.



I když jsou k základním registrům úřady práce v některých agendách připojeny, stále však platí pro Jana Nováka dle platných zákonných ustanovení v oblasti státní sociální podpory, péče o děti, dávek pro osoby zdravotně postižené, příspěvku na péči, hmotné nouze i podpory v nezaměstnanosti 8 denní oznamovací povinnost. Musí tedy do 8 dnů od změny adresy trvalého pobytu tuto změnu příslušnému oddělení úřadu práce nahlásit.

Živnostenský úřad.



Živnostenskému úřadu nemusí Jan Novák, pokud podniká, změnu adresy trvalého pobytu hlásit. Adresu trvalého pobytu změní živnostenské úřady v rejstříku živnostenského podnikání samy. Mějte však na paměti, že adresa sídla podnikatele zůstává na původní adrese a v případě změny adresy sídla je nutné novou adresu sídla do 15 dnů nahlásit (na jakémkoli živnostenském úřadě, bez ohledu na místní příslušnost). Pouze pokud Jan Novák již dříve oznámil živnostenskému úřadu, že při změně adresy trvalého pobytu požaduje změnit sídlo na stejnou adresu, jako je adresa trvalého pobytu, není povinen při změně adresy trvalého pobytu změnu sídla živnostenskému úřadu oznamovat.

Česká správa sociálního zabezpečení.

V případě, že Jan Novák pobírá důchod, musí změnu nahlásit sám. Způsob hlášení změny u příjemců důchodu závisí na způsobu výplaty důchodu, tj. zda v hotovosti na pobočce pošty nebo na účet u peněžního ústavu.



5. Jan Novák pobírá důchod na poště

Pokud Janu Novákovi ČSSZ vyplácí důchod prostřednictvím pošty, změnu nahlásí na kterékoli poště, která převede výplatu důchodu na poštu v novém místě trvalého pobytu a následně změnu adresy ohlásí ČSSZ.

6. Jan Novák pobírá důchod na účet u banky

Změnu musí Jan Novák nahlásit sám – třeba formou vlastnoručně podepsaného dopisu, v němž uvede svoje rodné číslo a novou adresu trvalého pobytu. Ten musí poslat na adresu ČSSZ, Křížová 25, Praha 5, 225 08. Je možné však také použít formulář, který je k dispozici na webových stránkách ČSSZ a také na okresních správách sociálního zabezpečení.

Oznámení o změně je možné poslat též v elektronické podobě podepsaným uznávaným elektronickým podpisem na adresu e-podatelny: posta@cssz.cz nebo datovou zprávou přes informační systém datových schránek do datové schránky ČSSZ: ID 49kaiq3.

Jestli Jan Novák pobírá důchod a bydlí v cizině, musí oznámit změnu adresy buďto písemnou formou vlastnoručně podepsaného dopisu, který zašle na výše uvedenou adresu ČSSZ (s tím, že do adresy připiše Oddělení výplat důchodů v oblasti mezinárodních důchodových agend), nebo na výše uvedený e-mail či datovou schránku.

Další instituce, kam Jan Novák musí zatím změnu trvalého pobytu hlásit.

Jan Novák musí změnu i nadále ohlašovat především nestátním (komerčním) subjektům.

Jde především o:

- banky (či jiné finanční společnosti, kde má Jan Novák např. úvěr),
- dodavatele elektrické energie,
- plynárny,
- komerční pojišťovny, u kterých má pojistku,
- ošetřujícího lékaře, zubaře,
- zaměstnavatele či školu,
- poštu (v případě SIPO, placení televizních a rozhlasových poplatků),
- telefonního operátora, atd.

Připravujeme možnost, že i komerční subjekty budou napojeny na základní registry a občanům se tak v případě změny adresy trvalého pobytu zase o něco zjednoduší komunikace nejenom s orgány státní správy, ale rovněž i s komerčními subjekty.

Straší vás, že bezplatný příjem televize skončí kvůli rychlému mobilnímu internetu?

Nebojte se!

Dohlédneme, aby se moderní technologie navzájem **nerušily**.

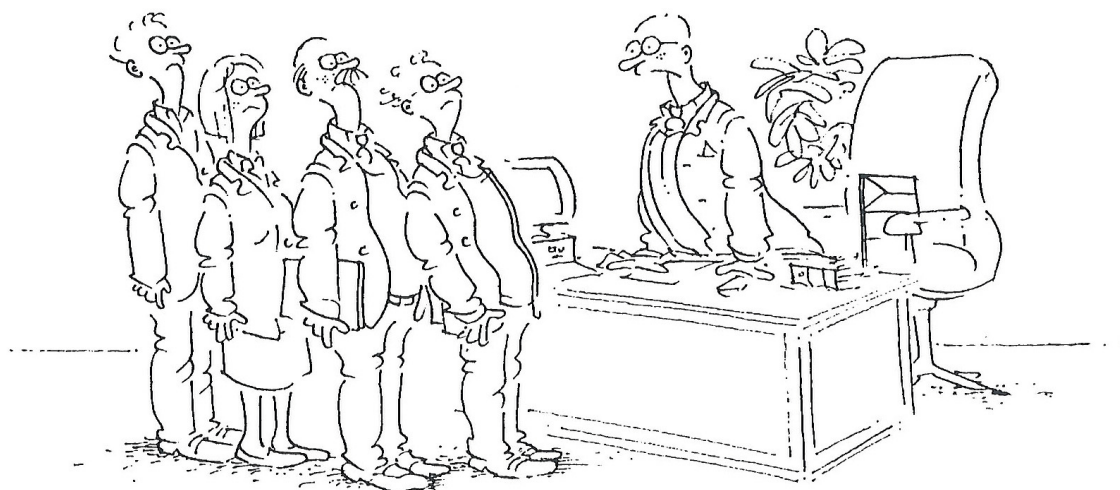


Český telekomunikační úřad

**Regulátor telekomunikačních
a poštovních služeb**

www.ctu.cz

KATALOG



MÁM. ALE NEPŘÍDÁM VÁM NA PLATU. Z ČEHO BY SE POTOM KRADLO?!

Generální partner konference

Česká spořitelna, a. s.

Centrála České spořitelny
Olbrachtova 1929/62, 140 00 Praha 4
Info linka: 800 207 207
E-mail: csas@csas.cz
www.csas.cz



Česká spořitelna je moderní banka orientovaná na drobné klienty, malé a střední firmy a na města a obce. Nezastupitelnou roli hraje také ve financování velkých korporací a v poskytování služeb v oblasti finančních trhů.

Hlavní partner konference

Atos IT Solutions and Services, s. r. o.

Dudlebská 1699/5, 140 00 Praha 4
tel.: +420 233 034 211
fax: +420 233 034 299
www.cz.atos.net



Atos je světový poskytovatel IT služeb s ročními tržbami 2013 ve výši 10 miliard eur a 86 000 zaměstnanci v 66 zemích. Celosvětově základně klientů nabízí vysoce technicky vyspělé transakční služby, poradenství, systémovou integraci a manage services.

Společnost Atos se soustředí na technologie v podnikání (business technology), které jsou motorem pokroku a pomáhají organizacím vytvářet firmu budoucnosti. Atos je celosvětovým IT partnerem Olympijských her. Akcie společnosti jsou obchodovány na pařížské burze Eurolist. Atos působí pod obchodními jmény Atos, Atos Consulting & Technology Services, Worldline a Atos Worldgrid.

Cisco Systems (Czech Republic) s.r.o.

V Celnici 10, 117 21 Praha 1
tel.: +420 221 435 111
www.cisco.com



Cisco je vedoucí firmou v oblasti síťových služeb. Mění způsob, jakým se lidé propojují, komunikují mezi sebou a spolupracují. Pro společnost Cisco jsou na prvním místě její zákazníci. Usiluje o dlouhotrvající partnerství, hledá řešení jejich potřeb a cesty ke společnému úspěchu.

Řešení a technologie od společnosti Cisco lze najít po celém světě, na jeho hranicích i na oběžné dráze. Patří mezi ně klasické síťové produkty, jako jsou routery, switche nebo servery, přes které protéká více než 90 % celosvětového internetového provozu. Nabízí i řadu jedinečných zařízení a „inteligentních“ systémů, které pomáhají zajišťovat bezpečnost, komunikaci mezi lidmi i organizacemi nebo budovat internet všeho. Díky technologiím Cisco může budoucnost začít již dnes.

Česká pošta, s. p.

Politických vězňů 909/4, 110 00 Praha 1
tel.: +420 221 131 111 (ústředna)
zákaznická linka: 840 111 244
www.ceskaposta.cz



Listovní a balíkové služby jsou pro Českou poštu tak samozřejmé, jako je dnes pro každého občana samozřejmé auto či televize. Avšak pokud chce udržet krok s dobou, už dávno nestačí dobře a včasné doručovat zásilky. Je třeba přinášet pravidelné inovace a uspokojit tak dostatečně nároky zákazníka.

Proto Česká pošta nabízí mimo jiné i služby eGovernmentu, které umožňují rychlou, důvěryhodnou a efektivní komunikaci občanů, živnostníků i velkých korporací se státní správou, úřady, soudy, policií atp. Stěžejními produkty eGovernmentu jsou Czech POINT, Datové schránky, Elektronické podpisy, Časová razítka, ale i další užitečné služby typu Datový trezor či Poštovní datová zpráva.

ICZ a.s.

Na hřebenech II 1718/10, 140 00 Praha 4
tel.: +420 222 271 111
fax: +420 222 271 600
e-mail: marketing@iczgroup.com
www.i.cz



ICZ a.s. – dodavatel IT a systémový integrátor pro veřejnou správu, zdravotnictví, obranu, dopravu, výrobu, logistiku, finance a další. Působí v ČR i zahraničí.

VITA software, s.r.o

Na Beránce 57/2, 160 00 Praha 6
tel.: +420 212 241 549
email: vita@vitasw.cz
www.vitasw.cz



VITA vytváří software pro správní orgány, zejména pro městské a krajské úřady a ministerstva. VITA je dominantním dodavatelem softwaru pro stavební úřady, úřady územního plánování, silniční správní úřady, vodoprávní úřady, vyvlastňovací úřady, orgány na úseku ochrany památek a velmi významným dodavatelem pro správní orgány řešící přestupky a jiné správní delikty, životní prostředí, dopravní agendy, koordinované stanovisko a poskytování informací. Dodávaný software je integrován se spisovou službou, ekonomickým systémem, geografickým informačním systémem, identity managementem, portálem občana i portálem úředníka. Samozřejmě je integrován s celostátními informačními systémy ISZR, ISDS, ISKN, ČSÚ atd. Dodávaný software je v souladu s legislativou, vyniká vysokou kvalitou a je významným pomocníkem úředníků.

Hlavní odborný partner konference

Microsoft s.r.o.

BB Centrum, budova Alfa
Vyskočilova 1461/2a, 140 00 Praha 4
www.microsoft.cz



Společnost Microsoft byla založena v roce 1975 a je světovým lídrem v poskytování softwaru, služeb a řešení, které pomáhají lidem a firmám po celém světě plně realizovat jejich potenciál. Česká pobočka společnosti Microsoft Corporation zahájila svoji činnost v roce 1992 a jejím generálním ředitelem je od července 2013 Biljana Weber. V České republice Microsoft významně podporuje charitativní projekty. Již roce 1996 vznikl z iniciativy firmy a Nadace Charty 77 projekt Počítače proti bariérám (»), jehož podpora trvá dodnes. Cílem projektu je pomoci postiženým občanům uplatnit se jak v běžném životě, tak i na trhu práce. Charitativní činnost společnosti Microsoft zastřešuje celosvětová iniciativa s názvem Potenciál bez hranic. Tento program je celosvětově zaměřen na partnerství s veřejnými školícími středisky, která pro potřebné spoluobčany organizují školení, zaměřená na výpočetní techniku a technologická řešení. Dotace v rámci programu slouží k zajištění vzdělávacích školení v komunitních centrech či speciálních vzdělávacích střediscích, kde se lidé mohou učit pracovat s počítačem. www.microsoft.com/cze

Partneři konference

Asseco Central Europe, a. s.

Budějovická 778/3a, 140 00 Praha 4
tel.: +420-234 292 500
fax: +420-234 292 502
email: sales@asseco-ce.com
www.asseco.com/ce



Asseco Central Europe (Asseco CE) je jedním z nejsilnějších softwarových domů ve střední a východní Evropě. Působí v České republice, Slovensku, Maďarsku, Německu, Rakousku a Švýcarsku. Patří mezi nejvýznamnější poskytovatele komplexních řešení a služeb v oblasti informačních technologií. Realizuje náročné projekty jak pro komerční sféru, tak pro státní správu a samosprávu. Asseco CE má dlouholeté zkušenosti s rozsáhlými projekty, u kterých klade silný důraz na podporu strategických záměrů svých klientů. Asseco Central Europe je součástí mezinárodní skupiny Asseco, která působí ve více než 30 zemích světa a zaměstnává přes 18 000 lidí.

AV MEDIA, a. s.

Pražská 63, 102 00 Praha 10
tel.: +420 261 260 218
fax: +420 261 227 648
e-mail: praha@avmedia.cz
www.avmedia.cz



Společnost AV MEDIA je leaderem na poli prezentační, projekční a audiovizuální techniky v České republice. Prostřednictvím návrhů a realizací řešení pro sdílení obrazu a zvuku přinášíme svým zákazníkům inspiraci, užitek i radost. Poskytujeme profesionální služby od projektového návrhu řešení až po zaškolení a následný servis a vždy sledujeme nejnovější trendy, které pak přinášíme do ČR jako první. AV technika a další produkty společnosti jsou využívány v konferenčních a zasedacích místnostech, na dispečerských pracovištích s nepřetržitým provozem, v učebnách a školicích místnostech, u speciálních simulačních a 3D aplikací, v kinosálech, v muzejních expozicích, na veletrzích a na mnoha dalších místech. Našimi zákazníky jsou školy, vysoké školy, kulturní instituce, firmy, veřejná správa, hotely i domácnosti. Vedle realizací řešení zajišťujeme i pronájem a obsluhu špičkové audiovizuální techniky pro širokou škálu různorodých akcí, od firemních školení přes korporátní kongresy, společenské akce a veletržní expozice až po venkovní projekci na budovy.

Citrix Systems Czech Republic s.r.o.

Na Pankráci 129/1724, 140 00 Praha 4
tel.: +420 739 545 287
e-mail: citrix@arrowecs.cz, roman.kapitan@citrix.com
www.citrix.cz



Citrix Systems je přední světový výrobce řešení, která umožňují uživatelům přístup k jejich datům a aplikacím kdykoliv, kdekoliv a z jakéhokoli zařízení. Technologie Citrix využívá denně přes 75 % uživatelů internetu na světě.

DATASYS s.r.o.

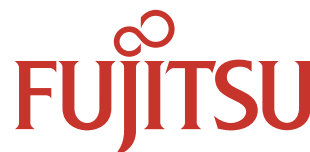
Jeseniova 2829/20, Praha 3
tel.: +420 225 308 111
fax: +420 225 308 111
e-mail: marketing@datasys.cz
www.datasys.cz



Datasys je významný český poskytovatel služeb a řešení v oblasti informačních technologií. Společnost vznikla v roce 1994 a svým současným obchodním obratem a šíří záběru patří mezi přední IT společnosti v České republice. Jejimi zákazníky jsou významné české společnosti z oblasti utilit, financí, telekomunikací, zdravotnictví či obchodu a služeb a instituce státní správy a samosprávy. Sídlo společnosti Datasys je v Praze a pobočky v Hradci Králové a Plzni.

FUJITSU

Fujitsu Technology Solutions s.r.o.
V Parku 2336/22, 148 00 Praha 4
tel.: +420 233 034 007
fax: +420 233 034 099
e-mail: recepce.cz@ts.fujitsu.com
www.fujitsu.cz



Fujitsu patří mezi největší japonské společnosti z oblasti informačních a komunikačních technologií (ICT) a nabízí kompletní portfolio IT produktů, řešení a služeb. Přibližně 160 000 zaměstnanců Fujitsu obsluhuje zákazníky ve více než 100 zemích. Fujitsu společně se svými zákazníky využívá své dlouholeté zkušenosti a sílu ICT k vytváření budoucnosti naší společnosti.

Fujitsu využívá koncepci dynamických infrastruktur a nabízí kompletní portfolio IT produktů, řešení a služeb – od klientů až po řešení datových center, spravovanou infrastrukturu a infrastrukturu poskytovanou jako služba (IaaS). Zákazníkům poskytuje služby od poradenství a návrh systému, dodávky systému a jeho implementaci až po následný provoz, údržbu a servis.

GORDIC spol. s r. o.

Erbenova 4, 586 01 Jihlava
tel.: +420 567 309 136
fax: +420 537 307 343
e-mail: gordic@gordic.cz
www.gordic.cz



Společnost GORDIC je dlouhodobým lídrem na trhu informačních systémů a specializovaných softwarových aplikací pro oblast státní správy a samosprávy. Její nosný produkt, komplexní IS GINIS, je již řadu let nejpožívanějším informačním systémem v oblasti veřejné správy České republiky. Za více než dvacet let existence na trhu si společnost vybudovala široké portfolio klientů od velkých ministerstev až po nejmenší příspěvkové organizace. Počet jejích zákazníků dnes přesahuje číslo 6 000. Své metodické znalosti i zkušenosti z praxe úřadů firma využívá také v roli akreditované vzdělávací instituce podle zákona č. 312/2002 Sb., o úřednících územních samosprávných celků, a pořádá školicí kurzy pro prohlubování kvalifikace úředníků.

NEWPS.CZ s.r.o.

Na Žertvách 29, 180 00 Praha 8
e-mail: info@newps.cz
datová schránka: 3y2qms4
www.newps.cz

NEWPS.CZ

Jsme jedničkou na českém trhu v oblasti řešení správy uživatelských účtů a kontroly přístupu uživatelů. Specializujeme se na správu uživatelů – Identity Management, kontrolu přístupu uživatelů – Access Management a na správu dat. Zaměřujeme se i na integraci a konsolidaci autentizačních systémů.

Postavili jsme např. systém správy uživatelů Informačního systému datových schránek, Jednotný identitní prostor systému Czech POINT a budujeme další.

Technologičtí konzultanti naší firmy jsou držiteli odborných certifikátů na produkty Novell, NetIQ, SUSE, Cisco, Software602 a další. Jsou rovněž držiteli certifikátů ITIL. Firma jako celek je držitelem mnoha uznávaných certifikací.

O2 Czech Republic a.s.

Za Brumlovkou 266/2, Praha 4
www.o2.cz



Jsme největším integrovaným operátorem v České republice. Naše produkty a služby nabízíme pod komerční značkou O2. V současnosti provozujeme téměř osm milionů mobilních a pevných linek, což z nás činí jednoho z vedoucích poskytovatelů plně konvergentních služeb v Evropě. Máme nejucelenější nabídku hlasových a datových služeb v České republice. Mimořádnou pozornost věnujeme využití růstového potenciálu především v oblasti mobilních datových přenosů a internetu. Obhospodařujeme nejrozsáhlejší pevnou a mobilní síť pro přenos dat, hlasu, obrazu i videa, včetně sítí 3. generace – UMTS a 4. generace (4G/LTE). Jsme také předním poskytovatelem ICT služeb a cloud.

Patříme do skupiny PPF Group, jejíž investice směřují do různých odvětví, jako jsou bankovní a finanční služby, pojišťovnictví, nemovitosti, energetika, těžba kovů, zemědělství, maloobchod a biotechnologie. Působnost skupiny PPF sahá ze střední a východní Evropy přes Rusko až do Asie. Skupina PPF má svou korporátní vlastnickou a řídicí strukturu v Nizozemsku: společnost PPF Group N.V. se sídlem v Amsterdamu je klíčovou holdingovou společností skupiny PPF, kde jsou přijímána strategická rozhodnutí, kterými se řídí činnost celé Skupiny.

Partneři odborných bloků

Český institut manažerů informační bezpečnosti o.s.

Rybná 716/24, 110 00 Praha 1
e-mail: tomas.hebelka@cimib.cz
www.cimib.cz



Český institut manažerů informační bezpečnosti (zkráceně ČIMIB – www.cimib.cz) byl založen v roce 2007 jako profesní sdružení manažerů informační bezpečnosti.

Více jak čtyři roky se zaměřujeme na připravovaný Zákon o kybernetické bezpečnosti. Nezabýváme se pouze samotnou legislativou, ale koncentrujeme se především na aplikaci zákona do praxe.

Členskou základnu tvoří přes 100 odborníků z více jak 80 institucí. Jedná se převážně o subjekty státní správy, utility, finanční instituce, komerční subjekty a technologické dodavatele.

Český telekomunikační úřad

Sokolovská 219, 190 03 Praha 9
adresa pro doručování: P.O. BOX 02, 225 02 Praha 025
tel.: +420 224 004 111, fax: +420 224 004 830
e-mail: podatelna@ctu.cz
www.ctu.cz



Český telekomunikační úřad je ústředním orgánem státní správy. Vykonává působnost státu ve věcech stanovených zákonem, včetně regulace trhu a stanovování podmínek pro podnikání v oblasti elektronických komunikací a poštovních služeb.

Český úřad zeměměřický a katastrální

Pod sídlištěm 1800/9, 182 11 Praha 8
tel.: +420 284 041 111, fax: +420 284 041 416
e-mail: cuzk@cuzk.cz
www.cuzk.cz



Network Security Monitoring Cluster

Botanická 68a, CERIT Science Park, 602 00 Brno
tel.: +420 733 713 702
e-mail: info@nsmcluster.com
www.nsmcluster.com



Network Security Monitoring Cluster je zájmové sdružení zabývající se ICT bezpečností. Věnuje se vzdělávání, evangelizaci a VaV v oblasti kyberbezpečnosti.

T-Mobile Czech Republic a.s.

Tomíčková 2144/1, 148 00 Praha 4
tel.: +420 603 604 605
e-mail: info@t-mobile.cz
www.t-mobile.cz



T-Mobile Czech Republic je součástí skupiny Deutsche Telekom a v České republice předním integrovaným poskytovatelem ICT služeb a řešení. Portfolio zahrnuje kompletní nabídku služeb od telekomunikačních včetně mobilních, IT až po systémovou integraci pro veřejnou správu a firemní zákazníky ve všech oborech – od průmyslových podniků přes telekomunikace, finančníctví, obchod, služby až po energetiku.

Spolupracující instituce a sdružení

Asociace krajů ČR

Zborovská 11, 150 21 Praha 5
tel.: +420 236 003 481
fax: +420 236 007 103
www.asociacekrajů.cz



ICT UNIE z.s.

K Červenému dvoru 25a/3269, 130 00 Praha 3
tel.: +420 222 582 880
e-mail: ictu@ictu.cz
www.ictu.cz



IDC CEMA s.r.o.

Malé náměstí 13, 110 00 Praha 1
tel.: +420 221 423 140
fax: +420 221 423 150
www.idc-czech.cz



International Visegrad Fund

Kráľovské údolie 8, 811 02 Bratislava, Slovak Republic
tel.: +421 259 203 811, –802
fax: +421 259 203 805
e-mail: visegradfund@visegradfund.org
www.visegradfund.org



Komora administrátorů veřejných zakázek

Na Ořešovicce 580/4, 162 00 Praha 6-Střešovice
tel.: +420 224 232 611
fax: +420 233 313 067
e-mail: kavz@kavz.cz
www.kavz.cz



Komora
administrátorů
veřejných zakázek

Svaz měst a obcí ČR

5. května 1640/65, 140 21 Praha 4
tel.: +420 234 709 711
fax: +420 234 709 786
e-mail: smocr@smocr.cz
www.smocr.cz



Sdružení tajemníků městských a obecních úřadů, o. s.

Dlážděná 1004/6, 110 00 Praha 1-Nové Město
tel.: +420 481 312 276
mobil: +420 606 882 187
fax: +420 481 312 276
e-mail: stmou@mmdecin.cz
www.tajemnici.cz



Zeměměřický úřad

Pod sídlištěm 1800/9, 182 11 Praha 8
tel.: +420 284 041 111
fax: +420 284 041 416
e-mail: zu.praha@cuzk.cz
www.cuzk.cz



Kraje a města

Kraj Vysočina

Žižkova 57, 587 33 Jihlava
tel.: +420 564 602 111, 564 602 100
fax: +420 564 602 420
e-mail: posta@kr-vysocina.cz
www.kr-vysocina.cz



Královéhradecký kraj

Krajský úřad Královéhradeckého kraje
Regiocentrum Nový pivovar
Pivovarské náměstí 1245, 500 03 Hradec Králové
tel.: +420 495 817 111
fax: +420 495 817 336
e-mail: posta@kr-kralovehradecky.cz
www.kr-kralovehradecky.cz



Statutární město Hradec Králové

Magistrát města Hradec Králové
Československé armády 408, 502 00 Hradec Králové
tel.: +420 495 707 111
fax: +420 495 707 100
e-mail: posta@mmhk.cz
www.hradeckralove.org



Hlavní město Praha

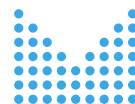
Magistrát hlavního města Prahy
Mariánské nám. 2, 110 01 Praha 1
tel.: +420 12 144
e-mail: info@praha.eu
www.praha.eu



Ministerstva

Ministerstvo vnitra ČR

Nad Štolou 3, poštovní schránka 21, 170 34 Praha 7
tel.: +420 974 811 111
e-mail: posta@mvcz.cz
www.mvcz.cz



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Ministerstvo pro místní rozvoj ČR

Staroměstské náměstí 6, 110 15 Praha 1
tel.: +420 224 861 282, 224 861 138
e-mail: info@mmer.cz
www.mmer.cz



MINISTERSTVO
PRO MÍSTNÍ
ROZVOJ ČR

Ministerstvo zemědělství ČR

Těšnov 65/17, 110 00 Praha 1
tel.: +420 221 811 111
e-mail: info@mze.cz, posta@mze.cz
www.eagri.cz

Ministerstvo financí ČR

Letenská 15, 118 10 Praha
tel.: +420 257 041 111
e-mail: podatelna@mfer.cz
www.mfer.cz

Ministerstvo práce a sociálních věcí ČR

Na Poříčním právu 1/376, 128 01 Praha 2
tel.: +420 221 921 111
e-mail: posta@mpsv.cz
www.mpsv.cz

Ministerstvo školství, mládeže a tělovýchovy ČR

Karmelitská 7, 118 12 Praha 1
tel.: +420 234 811 111
e-mail: posta@msmt.cz
www.msmt.cz

Ministerstvo zdravotnictví ČR

Palackého nám. 4, 128 01 Praha 2
tel.: +420 2 2497 1111
e-mail: mzcr@mzcr.cz
www.mzcr.cz

Prezentace firem

ANECT a.s.

Vídeňská 204/125, Přízřenice, 619 00 Brno
tel. Praha: +420 271 100 100, tel. Brno: +420 547 100 100
e-mail: anect@anect.com
www.anect.com



ANECT a.s. je předním dodavatelem profesionálních řešení z oblasti informačních a komunikačních technologií. Od svého vzniku se společnost orientuje na komplexní dodávky v oblasti komunikačních systémů, výstavby počítačových sítí pro středně velké a velké zákazníky. Nabízíme zkušený tým profesionálů, který zhodnotí Vaše investice v ICT, a to formou identifikace a optimalizace té části komunikačních a informačních technologií, která významně podporuje Vaši podnikatelskou činnost či vizi strategického rozvoje.

ARCDATA PRAHA, s.r.o.

Hybernská 24, 110 00 Praha 1
tel.: +420 224 190 511
fax: +420 224 190 567
e-mail: office@arcdata.cz
www.arcdata.cz

ARCDATA PRAHA



Distributor geografických informačních systémů Esri a dodavatel komplexních GIS řešení s řadou referencí ve veřejném i privátním sektoru.

ATLAS consulting spol. s r.o. – CODEXIS

Výstavní 292/13, 709 16 Ostrava
tel.: +420 596 613 333
e-mail: klientske.centrum@atlasconsulting.cz
www.atlasconsulting.cz



CODEXIS – komplexní právní informační systém, který je určen nejen odborníkům z oblasti práva, ale všem, kteří při výkonu své profese přicházejí do styku s právní problematikou.

AXENTA a.s.

Mlýnská 326/13, 602 00 Brno
tel.: +420 725 516 401
e-mail: info@axenta.cz
www.axenta.cz



AXENTA a. s. je integrátor bezpečnosti ICT = bezpečnosti IT, ochrany informací a fyzické bezpečnosti. Je zkušeným dodavatelem Log Managementu, SIEM a Security Operation Center řešení v ČR, SR.

BiZZdesign Česká republika, s.r.o.

V dolině 1533/1d, Michle, 101 00 Praha 10
tel.: +420 602 259 855
e-mail: info@bizzdesign.cz
www.bizzdesign.cz



BiZZdesign nabízí kompletní a integrovaná řešení pro podnikovou architekturu (EA) a procesní řízení (BPM). Naše ucelená řešení se skládají z uživatelsky přátelských nástrojů, manažerského poradenství a efektivních školení. Spravujeme architekturu veřejné správy v Holandsku, Slovensku a nyní i v České republice.

CGI IT Czech Republic s.r.o.

Na Okraji 335/42, Praha 6
tel.: +420 284 020 111
fax: +420 284 020 112
e-mail: libor.benak@cgi.com
www.cz.cgi.com



Společnost CGI založená v roce 1976 poskytuje globální služby v oboru informačních technologií a obchodních procesů. Prostřednictvím 68 000 odborníků dodává vysoce kvalitní služby v oblasti firemního poradenství, systémové integrace a outsourcingu.

Corpus Solutions a.s.

Na Vítězné pláni 1719/4, 140 00 Praha 4
tel.: +420 241 020 333
e-mail: info@corpus.cz
www.corpus.cz



Společnost Corpus Solutions a.s. se zaměřuje na řešení potřeb zákazníků zejména v oblasti IT bezpečnosti (Security Intelligence), podpory business rozhodování (Data Intelligence) a řízení ICT služeb.

CZ.NIC, z. s. p. o.

Milešovská 5, 130 00 Praha 3
tel.: +420 222 745 111
e-mail: podpora@nic.cz, podpora@mojeid.cz
www.nic.cz, www.mojeid.cz



Službu mojeID vyvíjí a provozuje sdružení CZ.NIC, jehož hlavní činností je provoz registru doménových jmen .CZ, zabezpečení provozu domény nejvyšší úrovně .CZ a osvěta v oblasti doménových jmen.

ČD - Telematika a.s.

Pernerova 2819/2a, 130 00 Praha 3



ČD - Telematika a.s. – telekomunikační služby, služby výstavby a servisu infrastruktury, druhá největší optická síť v ČR a vysoce zabezpečená datacentra.

DIGIS, spol. s r. o.

Výstavní 292/13, 702 00 Ostrava
tel.: +420 602 725 374
e-mail: marketing@digis.cz
www.digis.cz



Dodáváme ucelená řešení v oblasti geografických informačních systémů (GIS). Prodej a autorizovaný servis velkoformátových skenerů CONTEX, distribuce stolních a knižních skenerů SMA.

ESET software spol. s r.o.

Classic 7 Business Park, Jankovcova 1037/49, Praha 7, 170 00
tel.: +420 233 090 233
e-mail: info@eset.cz
www.eset.cz



Společnost ESET již od roku 1987 vyvíjí bezpečnostní software, který drží rekordní počet ocenění a díky němuž může přes 100 milionů uživatelů bezpečně objevovat možnosti internetu. Široké portfolio produktů ESET nabízí firmám i spotřebitelům maximální proaktivní ochranu při minimálních nárocích. Jedno z výzkumných center ESET pro detekci malware je v Praze.

GEOVAP, spol. s r.o.

Čechovo nábřeží 1790, 530 03 Pardubice
tel.: +420 466 024 111
fax: +420 466 657 314
e-mail: info@geovap.cz
www.geovap.cz



Informační systémy pro města a obce, ekonomický informační systém, spisová služba a systémy pro správu dokumentů, mapové servery a systémy GIS.

GEPRO spol. s r.o.

Štefánikova 52, 150 00 Praha
tel.: +420 257 089 811
fax: +420 257 089 838
e-mail: gepro@gepro.cz
www.gepro.cz



Geoportál GEPRO i GIS systém MISYS používají zaměstnanci více než 1800 úřadů měst i obcí a občané celé ČR. VYZKOUŠEJTE: http://geoportal.gepro.cz/obce/nazev_obce

HC Logic, s. r. o.

Sokola Tůmy 16, Ostrava, 709 00
tel.: +420 731 648 404
mail: info@hc-logic.cz
www.hc-logic.cz



Strategický partner nemocnic v oblasti logistiky, strukturálních plánů a rozvoje. Inovativní řešení zvyšující kvalitu, bezpečnost a efektivitu zdravotní péče.

Intergraph CS s.r.o.

Prosecká 851/64, 190 00 Praha 9
tel.: +420 234 707 820
fax: +420 234 707 821
e-mail: info-cz@intergraph.com
www.intergraph.cz



Intergraph CS poskytuje svým zákazníkům jedinečná a spolehlivá geoprostorová řešení v oblastech správy a komprimace dat, mapových portálů, mobilních a smart technologiích.

INVEA-TECH

U Vodárny 2965/2, 616 00 Brno
tel.: +420 511 205 250
e-mail: dolnicek@invea.com
www.invea.com



Výrobce řešení pro monitorování a bezpečnost počítačových sítí se specializací na analýzu IP toků uváděný v průzkumech Gartner a patřící do Deloitte CE Fast 50.

IterSoft s.r.o. Choceň

Husova 86, 565 01 Choceň
tel.: +420 608 077 142
e-mail: info@itersoft.cz
www.itersoft.cz



Vyvíjíme aplikace pro správce městských lesů. Dále nabízíme univerzální offline mobilní aplikaci pro prohlížení vašich dat v terénu, tvorbu pasportů atd.

IZIP, a.s.

Hvězdova 1073/33, 140 21 Praha 4
tel.: +420 221 458 117
e-mail: zdena.vankova@izip.cz
www.izip.cz



PALANTE je projekt Evropské komise podporující vývoj elektronických systémů, které pomohou pacientům řídit lépe svoji zdravotní péči.

K-net Technical International Group s.r.o.

Olomoucká 170, 627 00 Brno
tel.: +420 548 220 150
fax: +420 548 220 151
e-mail: info@k-net.cz
www.k-net.cz



Jsme IT partner řady úřadů. Pomáháme uspořádat počítačové systémy v rámci IT projektů, podobně jako zajišťujeme provoz IT poskytováním profesionálních služeb.

MARBES CONSULTING s.r.o.

Brojova 16, 326 00 Plzeň
tel.: +420 378 121 500
fax: +420 378 121 501
e-mail: marbes@marbes.cz; obchod@marbes.cz
www.marbes.cz



Konzultační, vývojová a vzdělávací společnost působící v oblasti informačních technologií jako systémový integrátor a dodavatel ucelených SW řešení zejména pro státní správu a samosprávu.

NESS Czech s.r.o.

V Parku 2335/20, 148 00 Praha 4-Chodov
tel.: +420 244 026 400
e-mail: nesscz@ness.com
www.ness.cz



Svět nemusí být složitý

Ness Technologies je globálním partnerem v oblasti business procesů a technologií. Specializuje se na vývoj sw produktů a aplikací, systémovou integraci a konzultace.

NEWTON Media, a.s.

Na Pankráci 1683/127, 140 00 Praha 4
tel.: +420 225 540 111
e-mail: obchodni@newtonmedia.cz
www.newtonmedia.cz



newton media

NEWTON Media je největší středoevropský poskytovatel služeb mediálního monitoringu a analýz s tradicí sahající do roku 1995. Působí v ČR, na Slovensku, v Polsku, Chorvatsku, Slovinsku, Srbsku, Bosně a Hercegovině a Makedonii. Monitoring a analýzy NEWTON Media pokrývají oblast „tradičních“ médií, internetu a sociálních sítí. Společnost disponuje největším mediálním archivem ve střední Evropě, sahajícím do roku 1996. Klienti rovněž využívají služby včasného varování při krizové komunikaci, monitoring reklamy i trénink v oblasti sociálních sítí. Portfolio služeb s přidanou hodnotou zahrnuje strategické poradenství a návrhy a realizaci doporučení s cílem napomoci klientům posílit jejich konkurenceschopnost. NEWTON Media poskytuje služby s přeshraničním a vícejazyčným přesahem. Je členem mezinárodních odborných sdružení FIBEP a AMEC a sdílí mediální obsah s dalšími agenturami z celého světa.

Novell-Praha, s.r.o.

Novodvorská 1062/12, 142 00 Praha 4
tel.: +420 220 410 540
fax: +420 220 410 549
e-mail: nccc@novell.cz
web: www.novell.cz

Novell®

Společnost Novell věří, že zákazníci by měli mít možnost výběru a plnou kontrolu nad svými IT systémy. Jako celosvětový lídr v oblasti podnikových aplikací přináší Novell řešení, díky kterým jsou pracovní prostředí produktivnější, bezpečnější a snadno spravovatelná. Podporuje tisíce organizací po celém světě prostřednictvím technologií pro spolupráci, mobilitu, zabezpečení koncových zařízení a souborové a síťové služby. Díky produktům jako Novell GroupWise, Novell ZENworks, Novell Open Enterprise Server, Novell Filr, NetIQ Sentinel a NetIQ Identity Management mohou zákazníci dosáhnout vyšší úrovně produktivity a zároveň minimalizovat náklady, složitost a rizika spojená s jejich IT infrastrukturou. Více informací naleznete na webu www.novell.cz.

Novicom s.r.o.

Koněvova 67a, 130 00 Praha 3
tel.: +420 271 777 231–2
e-mail: sales@novicom.cz
www.novicom.cz



novicom

Výrobce síťových a bezpečnostních řešení integrované správy IP adresního prostoru, základních síťových služeb, řízení sítí, přístupů a monitoringu infrastruktury.

Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví

Roškotova 1225/1, 140 21 Praha 4
tel.: +420 261 105 555
fax: +420 261 105 300
e-mail: ozp@ozp.cz
www.ozp.cz



OZP je první zdravotní pojišťovna v ČR nabízející plně funkční a bezpečné online komunikační nástroje nejen pro web, ale rovněž pro mobilní telefony a tablety.

OKI Systems (Czech and Slovak) s.r.o.

Sokolovská 651/136a, 186 00 Praha
tel.: +420 224 890 157
fax: +420 222 326 621
e-mail: info@oki.cz
www.oki.cz



Výrobce působící na trhu v oblasti dokumentových technologií a služeb. Poskytujeme vlastní technologický a inovativní vývoj a komplexní služby v oblasti tiskových a multifunkčních zařízení.

OKsystem a.s.

Na Pankráci 125, 140 21 Praha 4
tel.: +420 236 072 111
e-mail: info@oksystem.cz
www.oksystem.cz



OKsystem je česká společnost působící na trhu informačních technologií již od roku 1990. Specializuje se na vývoj rozsáhlých programových systémů na zakázku, na řešení personální a mzdové agendy, včetně zpracování manažerských informací. Dále vyvíjí mobilní aplikace, pomáhá zvyšovat bezpečnost dat a řeší systémy pro správu dokumentů. Své programové systémy dodává do soukromého sektoru i do státní správy a přizpůsobuje je pro různá odvětví podnikání. Každodenně s nimi pracuje více než 200 000 spokojených uživatelů.

QCM, s.r.o.

Bellova 370/40, 623 00 Brno
tel.: +420 538 702 702
e-mail: info@qcm.cz
www.qcm.cz



QCM je leader v elektronizaci veřejných zakázek. Spolehlivě dodává pro zadavatele z řad státní správy a samosprávy individuální elektronický nástroj E-ZAK, e-tržistiště Gemin, systém centralizovaného zadávání RS CZ, e-aukční portál eAUKCE, poskytuje profil zadavatele na Portálu pro vhodné uveřejnění a nabízí právní služby a administraci veřejných zakázek.

SEFIRA spol. s r.o.

Antala Staška 2027/77, 140 00 Praha
tel.: +420 222 558 111
e-mail: sales@sefira.cz
www.sefira.cz



SEFIRA je stabilním dodavatelem IT řešení a služeb. Zaměřuje se na dodávky podnikových řešení, zakázkový vývoj IS, bezpečnost enterprise aplikací (centralizace PKI služeb, autentizace, mobilní a databázová bezpečnost) a systémovou integraci. SEFIRA je dodavatelem řešení pro archivaci elektronických dokumentů OBELISK Archive a poskytovatelem služby pro ověřování platnosti digitálních certifikátů CertReview. SEFIRA má zákazníky z oblasti energetiky, finančnictví, pojišťovnictví, průmyslu a veřejné správy.

Servodata a.s.

Dolnoměcholupská 12, 102 00 Praha 10
tel.: +420 296 813 111
e-mail: info@servodata.net
www.servodata.net



Servodata se dlouhodobě specializují na návrh a realizaci komplexních řešení podnikové infrastruktury v oblasti informačních a komunikačních technologií.

Software602 a.s.

Hornokřeská 15, 140 00 Praha 4
tel.: +420 222 011 602
e-mail: info@602.cz
www.602.cz



Software602 je český dodavatel programového vybavení s více než 20letou historií. Podporujeme všechny platformy, procesy i celý životní cyklus práce s dokumentem od vzniku až po dlouhodobou archivaci.

Státní pokladna Centrum sdílených služeb, s. p.

Na Vápence 915/4, 130 00 Praha 3-Žižkov
tel.: +420 225 515 111
e-mail: info@spcss.cz
www.spcss.cz



Státní pokladna Centrum sdílených služeb, s. p. provozuje datové centrum, které poskytuje ICT služby s nadstandardní bezpečnostní úrovní a maximální odbornou podporou. Provozujeme jedno z nejlépe zabezpečených datových center v Praze s vysokou dostupností služeb v oblasti ICT odpovídající parametrům TIER III dle hodnocení Uptime Institute.

STÁTNÍ TISKÁRNA CENIN, státní podnik

Růžová 6, č. p. 943, 110 00 Praha 1
tel.: +420 236 031 111
fax: +420 236 031 400
e-mail: stc@stc.cz
www.stc.cz



Od roku 1928 jsme dodavatelem komplexního technologického know-how v oblasti tisku produktů ceninového charakteru, vyžadujících vysoký stupeň zabezpečení výroby.

STYRAX, a.s.

Zelený pruh 95/97, 140 00 Praha 4
tel.: +420 227 027 324
fax: +420 227 027 320
e-mail: info@styrax.cz
www.styrax.cz



STYRAX, a.s. se orientuje především na vývoj a implementaci proprietálních informačních systémů a na poskytování konzultačních a analytických služeb. STYRAX úspěšně realizoval rozsáhlé projekty, zejména v oblasti finančního a kapitálového trhu a také v oblasti zdravotnictví.

Tender systems s.r.o.

nám. Před bateriemi 18, 162 00 Praha
tel.: +420 212 241 545
e-mail: info@tendersystems.cz
www.tendersystems.cz



Společnost Tender systems s.r.o. se zabývá výrobou a provozováním informačních systémů pro elektronické zadávání veřejných zakázek. Nabízíme celou řadu doplňkových produktů a služeb, včetně vzdělávání a odborného poradenství v oblasti elektronizace veřejného investování.

TRIADA, spol. s r. o.

U Svobodárny 1110/12, 190 00 Praha 9
tel.: +420 284 001 284
fax: +420 284 818 027
e-mail: info@triada.cz
www.triada.cz



Společnost TRIADA patří k předním dodavatelům software (IS MUNIS) a služeb pro sféru veřejné správy ČR. Kromě této činnosti pořádá například významnou konferenci ISSS, organizuje setkání starostů Den malých obcí a vydává odborný časopis Obec a finance.

Turistické informační centrum Hradec Králové

Gočárova 1225, 500 02 Hradec Králové
tel.: +420 495 534 482
fax: +420 495 534 485
e-mail: icko@ic-hk.cz
www.ic-hk.cz



Turistické informační centrum v Hradci Králové má 3 provozovny – Gočárova 1225, Velké nám.165 a hala hlavního nádraží ČD, které poskytují veškerý servis pro turisty a prodej vstupenek na kulturní akce přes rezervační systémy.

TyfloCentrum Brno, o. p. s.

Chaloupkova 3, 612 00 Brno
tel.: +420 515 919 770
e-mail: info@centrumpronevidome.cz
www.centrumpronevidome.cz



Poradna pro bezbariérový web – www.blindfriedly.cz

T-MAPY spol. s r.o.

Špitálská 150, 500 03 Hradec Králové
tel.: +420 498 511 111
e-mail: info@tmapy.cz
www.tmapy.cz



Nabízíme webové technologie pro geografické i základní informační systémy, softwarové prostředky pro desktopový GIS a geografická data pro všestranné využití.

VEEAM SOFTWARE

tel.: +420 228 882 884
www.veeam.com/cz/



Společnost Veeam je průkopníkem nového trhu dostupnosti moderních datacenter (Availability for the Modern Data Center™) tím, že pomáhá organizacím dosáhnout hodnot RTPO™ nižších než 15 minut pro všechny aplikace a data. Veeam řešení umožňuje vysokorychlostní obnovení dat, zamezuje ztrátu dat, poskytuje ověřitelnou ochranu, zmírnění rizik a kompletní transparentnost.

Vema, a. s.

Okružní 871/3a, 638 00 Brno
tel.: +420 530 500 000
e-mail: vema@vema.cz
www.vema.cz



Přední český dodavatel informačních systémů pro řízení lidských zdrojů. Vyvíjí a implementuje vlastní softwarové řešení v oblastech zpracování mezd, evidence personálních údajů, docházky, hodnocení, systemizace, vzdělávání, výběrových řízení, plánování dovolené, pracovních cest atd. Lídr na poli cloudových řešení HR systémů.

VERA, spol. s r.o.

Sídlo: Lužná 2, 160 00 Praha 6
Kontaktní adresa: Klicperovo nám. 39/I, 503 51 Chlumeck nad Cidlinou
tel.: +420 495 703 211
e-mail: obchod@vera.cz, info@vera.cz
www.vera.cz



VERA Radnice, VERA Dimenze – Kompletní řešení IS pro veřejnou správu.

Komplexní systémy zahrnují mj. ekonomiku, majetek, agendy, podporu interních procesů, vč. mobilních řešení, manažerských nadstavb, portálových řešení pro občany a možnosti integrace na okolí.

ERP systém pro organizace s vlastnickým podílem obcí, krajů a států.

VÍTKOVICE IT SOLUTIONS a.s.

Cihelní 1575/14, 702 00 Ostrava, Moravská Ostrava
tel.: +420 596 663 111
fax: +420 596 663 112
e-mail: itsolutions@vitkovice.com
www.vitkovice.cz



VÍTKOVICE IT SOLUTIONS a.s., člen holdingu VÍTKOVICE Machinery Group, poskytuje komplexní řešení v podobě produktů a služeb na základě požadavků zákazníka v mnoha IT oblastech. Společnost se zaměřuje na oblasti řídicích systémů, integrovaných bezpečnostních systémů a systémů pro podporu krizového řízení a plánování.

**vysoká škola
CEVRO Institut, o.p.s.**

Jungmannova 17, 110 00 Praha 1-Nové Město
tel.: +420 221 506 700
fax: +420 221 506 709
e-mail: info@vsci.cz
web: www.cevroinstitut.cz

CEVRO Institut je dynamicky se rozvíjející soukromou vysokou školou práva, politologie, mezinárodních vztahů, ekonomie a bezpečnostních studií. CEVRO Institut nabízí elitní vzdělání, individuální přístup a rodinnou atmosféru umocněnou místy výuky – historickou budovou Měšťanské besedy v srdci Prahy a pobočkou v Českém Krumlově.



WEBHOUSE, s. r. o.

Masarykovo nám. 47, 586 01 Jihlava
tel.: +420 561 207 247
e-mail: obchod@webhouse.cz
www.webhouse.cz

Tvoříme weby nejen pro veřejnou správu. Naše stránky jsou bezbariérově přístupné a splňují zákonné požadavky kladené na města a obce. Vyvíjíme redakční systém vismo Online s unikátním principem „Edituj, co vidíš“.



Wolters Kluwer, a.s.

U Nákladového nádraží 6, 130 00 Praha 3
tel.: +420 246 040 444
fax: +420 246 040 401
e-mail: obchod@wolterskluwer.cz
www.wolterskluwer.cz



Wolters Kluwer – Když si musíte být jistí!

Wolters Kluwer patří k předním světovým vydavatelům a poskytovatelům informačních produktů a služeb. Jedním z nejznámějších produktů je systém ASPI.

YOUR SYSTEM, spol. s r.o.

Türkova 2319/5b (Prague Gate), 149 00 Praha 4-Chodov
tel.: +420 277 775 500
e-mail: info@ys.cz

Společnost YOUR SYSTEM, spol. s r.o. je ryze česká IT firma působící na českém trhu již 25 let.



Zeměměřický úřad

Pod sídlištěm 1800/9, 182 11 Praha 8
tel.: +420 284 041 111
fax: +420 284 041 416
e-mail: zu.praha@cuzk.cz
www.cuzk.cz



Pořadatelé

TRIADA, spol. s r. o.

U Svobodárny 1110/12, 190 00 Praha 9-Libeň
tel.: +420 284 001 284
fax: +420 284 818 027
e-mail: info@triada.cz
www.triada.cz



Pobočka Brno:
Cejl 72, 602 00 Brno
tel.: +420 545 210 549, fax: +420 545 210 549



Vzdělávací instituce akreditovaná MV ČR; www.triada.cz



Munis – informační systémy pro města a obce; www.munis.cz
iMunis SMiS – portál obce pro komunikaci s občany; www.imunis.cz



Obec & finance – odborné periodikum pro ekonomické otázky měst a obcí
Veřejná správa online – příloha zaměřená na ICT technologie ve veřejné správě
www.obecafinance.cz



Den malých obcí – pravidelné setkání starostů malých obcí s představiteli
státní správy a dalšími odborníky nad aktuálními problémy
www.denmalychobci.cz



Deník veřejné správy – konference, semináře a školení pro pracovníky ve veřejné správě
www.dvs.cz



Solon – legislativní a metodická podpora pracovníků veřejné správy
www.solon.cz

Sdružení Český zavináč

U Svobodárny 1110/12, 190 00 Praha 9
tel.: +420 284 001 284
fax: +420 284 818 027
www.ceskyzavinac.cz



PONCA spol. s r. o.

Drahobejlova 1142/34, 190 00 Praha 9
www.ponca.eu

