Egovernment
elektronizace veřejné správy

Kybernetická bezpečnost

www.egovernment.cz

č. 2/2016

JISTOTA NEBEZPEČÍ

V dnešní době fungujeme díky IT. Ač se Vám to může zdát jako přehnané tvrzení, jsou informační technologie všudypřítomné. Jsou v našich počítačích, televizorech, mobilních telefonech, mixerech, troubách, lednicích, automobilech, ovládají naše domovy, naši bezpečnost, naši dopravu... ovládají náš život. Drobný problém nastává ve chvíli, kdy se začneme na informační technologie plně spoléhat. Mohou nám výrazně ulehčit náš život a vnést nám do něj vyšší komfort, mohou nám ale rovněž pěkně „zavařit". I když nikoli IT samo o sobě, jako spíše lidé kolem něj. V kyberprostoru, který se rozšiřuje skutečně dynamicky, už totiž nejde jen o spuštění nějakého viru. Už jde o uchvácení a ovládnutí toho kterého systému. A je jedno, jestli výsledkem je „vysání" citlivých dat, ovládnutí našich automobilů, nebo znehybnění armády. Informační technologie se tak stávají zároveň kanálem kterým skutečně pulzuje zločin. Upřímně ruku na srdce, i v případě, že jste natolik svědomití, že pravidelně aktualizujete veškeré své aplikace i antivirový systém, máte zapnutý firewall a do počítače nedáváte cizí paměťová média, kolik z Vás asi totéž činí se svým telefonem, neřku-li televizí?

Je důležité si uvědomit, že kyberzločin se neomezuje pouze na náhodné osoby, které se nestarají o svůj počítač. Je to dnes skutečně organizovaný zločin. A tak se objevují případy, kdy jsou atakovány a vydírány vládní instituce, čínský prezident navrhuje regulaci internetu a Evropa diskutuje o nutnosti sjednocení bezpečnostních politik. Měla by si pospíšit, podle odhadů totiž do roku 2020 škody vzniklé kyberzločinem údajně stoupnou na **2 000 000000 000 USD**.

A tak se zdá, že vedle zvyšujícího se pohodlí, které nám IT přináší, máme patrně jedinou jistou – jistotu nebezpečí, které se každým dnem zvyšuje.

I proto magazin Egovernment uspořádal další ze série seminářů na téma Kyberbezpečnost – víc než zákon. Hovořili jsme zde, s ročním odstupem od účinnosti zákona, o tom, co přinesl, jak vypadá bezpečnostní politika na některých úřadech, stejně tak jako v rámci kritické infrastruktury. Doufejme, že Vás toto čtení uklidní. Nebo zneklidní?

Ing. Michal Jirkovský
šéfredaktor

e-government 20:10

aneb žijem si jak na zámku, ať to trvá věčně

MIKULOV • 6. - 7. 9. 2016

ODBORNÝ PARTNER

Česká pošta, odštěpný závod ICT služby

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

SPCSS

PLATINOVÝ PARTNER

CISCO

GENERÁLNÍ PARTNER

Česká pošta

GORDIC®

NEWPS.CZ

ZLATÝ PARTNER

Atos

ČSOB

FORTINET

Hewlett Packard Enterprise

CERTIFICATION AUTHORITY

ICZ

Microsoft

ROWAN LEGAL

vmware

sefira SOLVE IT TOGETHER

STŘÍBRNÝ PARTNER

FUJITSU

TECHNOLOGICKÝ PARTNER

AV MEDIA komunikace obrazem

intel

PARTNER

COMSYS

ČÚZK

dns

ictunie

MARBES CONSULTING

OKI

SPRÁVA ZÁKLADNÍCH REGISTRŮ

scanservice END OF ENTROPY

AVERA

STÁTNÍ TISKÁRNA CENIN

OFICIÁLNÍ VŮZ

SEAT

... vše podstatné o eGovernmentu najdete v Mikulově.

Více naleznete na **www.egovernment.cz/mikulov**

Obsah

V rámci České a Slovenské republiky vydává:

info◆com s.r.o, Na Zatlance 10, 150 00 Praha 5
www.infocom.cz
IČO: 26426331
zapsána u Městského soudu v Praze pod č. C – 81357
tel.: 241 412 518
e-mail: egovernment@egovernment.cz
http: www.egovernment.cz
ISSN 1801-9420

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

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

Registrace:

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



I letos si Vás dovolujeme pozvat na konferenci **e-government 20:10, aneb žijem si jak na zámku, ať to trvá věčně.** Konference, kterou pořádá magazín Egovernment, proběhne tradičně na zámku Mikulov a to v termínu **6. - 7. 9. 2016**.

Opět pro Vás bude připraven bohatý dvoudenní program stejně jako společenský večer.

Součástí večera bude volba **Miss Egovernment**

- přihlašování soutěžících je již možné

(více na www.egovernment.cz/miss)

Vstupné na konferenci se mění v čase:

VEŘEJNÁ SPRÁVA (uvedené ceny jsou bez DPH):

registrace do 25. 5. 2016 ..... 600 Kč
registrace do 25. 6. 2016 ..... 700 Kč
registrace do 25. 7. 2016 ..... 1 000 Kč
registrace do 25. 8. 2016 ..... 1 200 Kč
registrace do 7. 9. 2016 ..... 1 500 Kč

KOMERČNÍ SFÉRA (uvedené ceny jsou bez DPH):

registrace do 25. 5. 2016 ..... 2 700 Kč
registrace do 25. 6. 2016 ..... 3 600 Kč
registrace do 25. 7. 2016 ..... 4 500 Kč
registrace do 25. 8. 2016 ..... 5 500 Kč
registrace do 7. 9. 2016 ..... 8 000 Kč

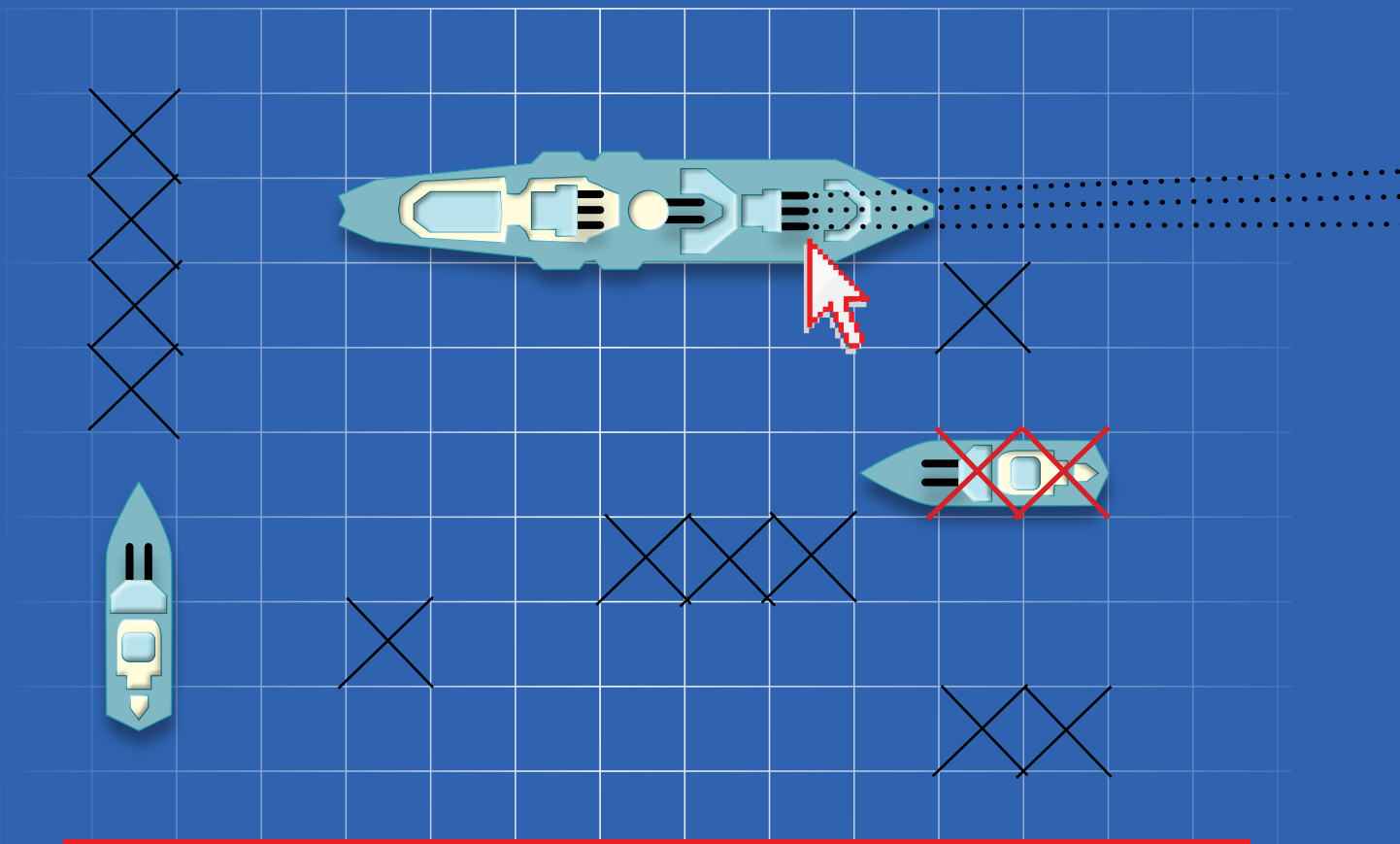






... vše podstatné o eGovernmentu najdete v Mikulově.

Přihlašování na konferenci je možné na **www.egovernment.cz/mikulov**

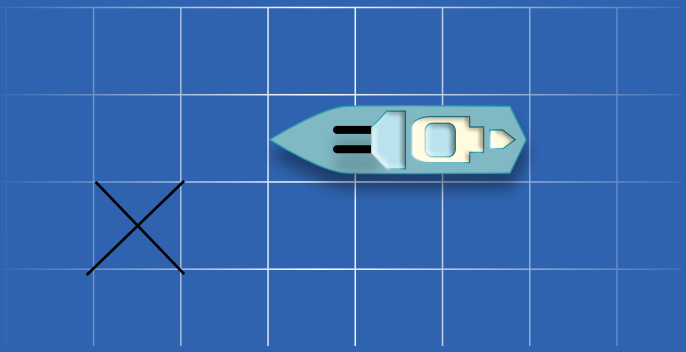


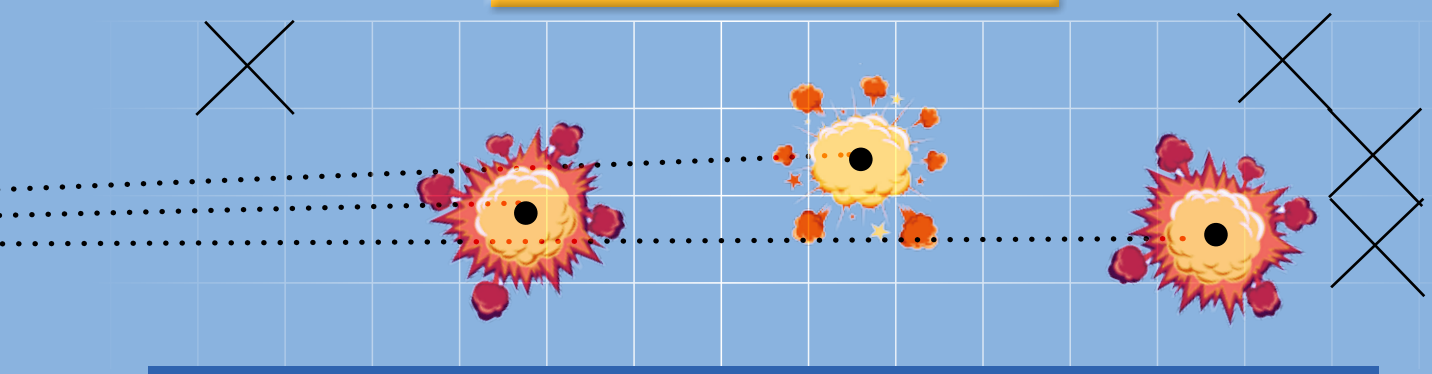
Bezpečí i zbraň zároveň

Místopředseda Poslanecké sněmovny Parlamentu ČR Jan Bartošek podpořil v pořadí již třetí setkání magazínu Egovernment na téma elektronické bezpečnosti. Jak sám uvedl, už samotná účast posluchačů ukazuje, že se jedná o zajímavé téma, a on jen doufá, že diskuze přinese očekávaný efekt.

Téma kyberbezpečnosti podle vlastních slov podporuje především proto, že svět kolem nás se skutečně přesouvá do e-prostoru. A podstatné podle Jana Bartoška je to, že v tomto alternativním prostoru platí poněkud jiná pravidla a zvyklosti. A ke zlepšení dle jeho mínění jen tak nedojde. Samotná kyberbezpečnost má z jeho pohledu několik rovin. Je tu otázka národní bezpečnosti v případě války. Zbraní jakéhokoliv válečného konfliktu budoucnosti, jak upozornil, bude oblast IT. Prostřednictvím těchto technologií je možné převzít zbraňové systémy nepřítele, a tím jej bleskově a bez ztráty vlastních sil ovládnout. Podle Jana Bartoška je to realita, ve které žijeme, a některé nedávné dílčí konflikty to jen potvrdily.

Důvodem, proč opětovně podpořil seminář s tímto tématem, je rovněž skutečnost, že v Poslanecké sněmovně bude řešena velice důležitá otázka elektronické identity občana. Na jedné straně vynikající možnosti identity v elektronické jsou zároveň velice nebezpečné, protože přímo svádějí k pokusům o její zcizení. I proto je dle Jana Bartoška nutné věnovat zvýšenou pozornost samotnému zabezpečení. Jedná se o zcela zásadní otázku, a je proto rád, že ČR patří k zemím, které se o svoji kyberbezpečnost zodpovědně starají, protože například s realizací kyberzákona je oproti ostatním v určitém předstihu. Svoje vystoupení proto zakončil přáním: „Nechť kyberbezpečnost je naším bezpečím i naší zbraní zároveň."





Účinný pomocník

Úloha Národního kybernetického úřadu je v rámci kyberbezpečnosti ČR neodmyslitelná. I proto se po několikáté našeho semináře s tímto tématem účastnil ředitel NBÚ Dušan Navrátil.

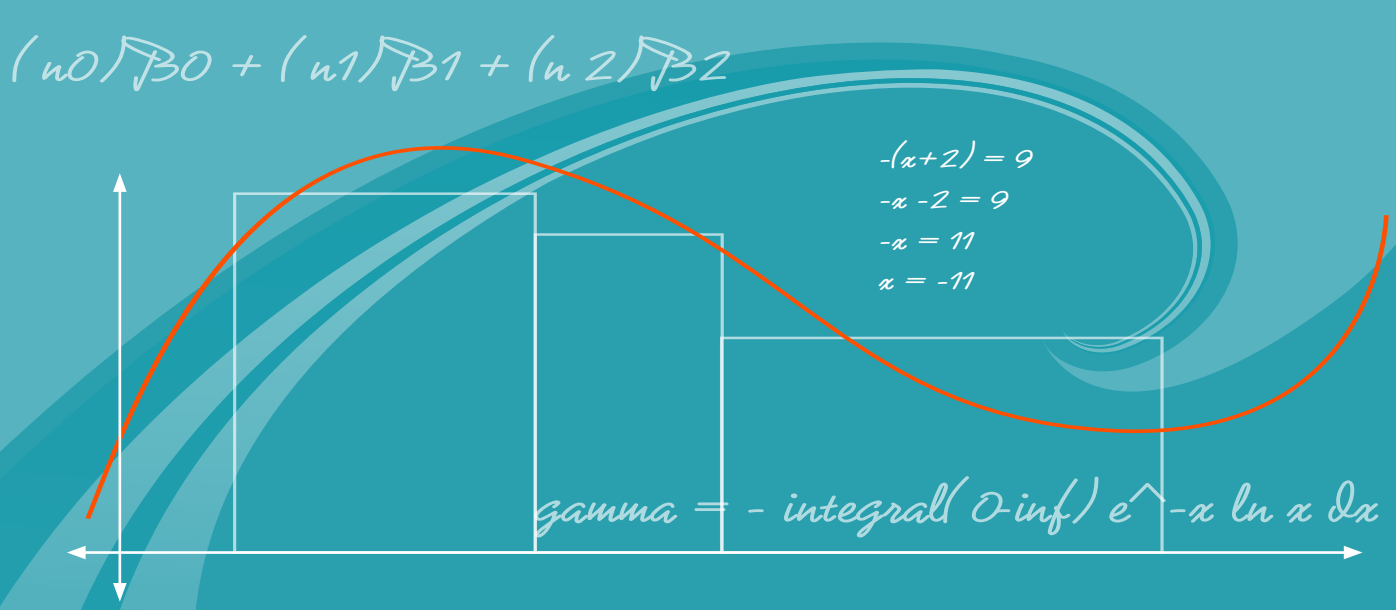
V úvodu svého vystoupení Dušan Navrátil připomněl, že s kybernetickou bezpečností se setkáváme skutečně každý den. Pouhý den před konáním semináře byl zajištěn malwer v německé jaderné elektrárně a v den, kdy jsme seminář organizovali, došlo k útoku na web sociální demokracie. Vedle těchto drobných incidentů upozornil rovněž na nebezpečnější útoky, například krádež dat státních úředníků ve Spojených státech amerických, či útok na ovládání energetické sítě v Izraeli. Zdůraznil, že i když u nás zatím takto závažné ataky neregistrujeme, není důvod si myslet, že se jim do budoucna vyhneme. Celková bezpečnostní situace v Evropě i ve světě se zhoršuje a v intencích současných trendů musíme předpokládat postupně se zvyšující výskyt podobných útoků a musíme na ně být připraveni.

Účinným pomocníkem na cestě k bezpečnějšímu kyberprostoru je, podle Dušana Navrátila, zákon o kybernetické bezpečnosti. Jak se nyní před publikováním směrnice NIS, tedy směrnice o vysoké bezpečnosti sítí ukazuje, máme v tomto směru vše podstatné již téměř z 80 % připraveno. V současné době probíhají práce na implementaci směrnice NIS do našeho zákona, což by neměl být zásadní problém. Ideálně bychom podle mínění Dušana Navrátila měli implementovat uvedenou směrnici ještě v současném volebním období. Přibližně v červenci by příslušná novela zákona č.181/2014 Sb., o kybernetické bezpečnosti měla putovat do meziresortního řízení. Definitivní znění směrnice bude publikováno v červnu a od tohoto okamžiku bude časový prostor 21 měsíců na její implementaci. Protože, jak bylo řečeno, máme v rámci Evropy určitý náskok, měli bychom si jej udržet. I z tohoto důvodu Dušan Navrátil uložil pracovníkům legislativního oddělení NBÚ úkoly, které směřují k tomu, aby se implementace i v takto „šibeničním" termínu podařila.

Jak Dušan Navrátil připomenul, zákon o kybernetické bezpečnosti platí od 1. ledna roku 2015. O zkušenostech za toto období bude následně hovořit náměstek Šmíd. Podle Dušana Navrátila je podstatné, že NBÚ již realizuje státní dozor. Proběhly tedy první kontroly ve významných informačních systémech a od května začínají kontroly v rámci kritické informační infrastruktury. První dávka kritické informační infrastruktury byla vládou schválena v květnu loňského roku a jednotlivé subjekty měly vždy rok na implementaci standardů, které jsou obsaženy ve vyhlášce, proto kontroly začínají právě v tomto období.

Samotný zákon o kybernetické bezpečnosti je podle Dušana Navrátila skutečně dosti ojedinělý i v rámci Evropy a odbornou veřejností je vítán pozitivně. Jak uvedl, nezaregistroval v poslední době žádné negativní ohlasy, spíše naopak. Zákon se vztahuje na kritickou informační infrastrukturu a na významné informační systémy, ale je možné jej chápat jako vzor i pro ostatní informační systémy. A jak Dušan Navrátil zdůraznil, je to rovněž velice vhodný podpůrný argument a návod pro ty, jejichž systémy sice zákonem nejsou pokryty, ale v rámci kyberbezpečnosti by bylo rozumné, aby uvedené požadavky splňovaly.

V závěru úvodního vystoupení semináře se Dušan Navrátil věnoval Národnímu centru kybernetické bezpečnosti v Brně a uvedl, že se stále rozvíjí. Nyní došlo k navýšení finančních prostředků ze 60 mil. na 100 mil. Kč ročně a tabulkové navýšení o 8 lidí v letošním i příštím roce. Tak bude podle jeho slov dosaženo stavu, který odpovídá kapacitě samotného centra v Brně. Protože však lze očekávat rozvoj v této oblasti, výhledově nebudou tyto kapacity stačit, a proto probíhají jednání o nových možnostech rozšiřování NCKB.



Nejen zákon, ale i vzdělání

Na ředitele NBÚ navazoval svým vystoupením jeho náměstek Jaroslav Šmíd. Protože tématem jeho vystoupení je zkušenost se zákonem o kyberbezpečnosti, řekl několik slov o tom, jaké zkušenosti NBÚ získává při kontrolách shody se zákonem u těch subjektů, které byly určeny jako kritické či významné informační systémy. Dále se rozhodl uvést několik čísel o tom, kolik systémů bylo určeno a v jakém jsou stavu, a krátce se vyjádřil rovněž ke stavu legislativy.

Od účinnosti zákona č. 181/2014 Sb., tedy od začátku ledna loňského roku, dostal NBÚ právo kontrolovat, jakým způsobem jsou naplňována kritéria zákona některými informačními systémy. Začalo tedy určování jednotlivých prvků kritické infrastruktury. Ve vyhlášce bylo definováno prvních 92 významných informačních systémů. Všechny organizace, kterých se kontroly týkají, dostaly roční přechodové období na to, aby naplnily uvedené požadavky zákona. Od začátku letošního roku může tedy NBÚ už dělat první kontroly u významných informačních systémů a od 25. května přijdou na řadu první kritické informační systémy. NBÚ vytvořil systém kontrol, které jsou v první fázi vedeny spíše jako určitá metodická pomoc.

Nyní byl ukončen první kvartál, v jehož rámci proběhlo pět kontrol. Výsledky jsou, podle Jaroslava Šmída, velice uspokojivé, i když v nich nějaké nedostatky byly. Jak uvedl, je samozřejmostí, že kontroly jsou oznamovány dopředu tak, aby bylo možné se na ně připravit. U jednodušších systémů kontrola zabere zhruba dva až tři dny. Složitější kontroly budou o něco delší, neměly by však překročit 8 dnů. Zdůraznil, že kontrola vychází z požadavků vyhlášky č. 316, tedy vyhlášky, která určuje standardy, které by měly jednotlivé systémy naplňovat. Kontrolní řád podléhá zákonu č. 255/2012 Sb., o kontrole. Celý proces kontroly je tedy v souladu s legislativou. Kontrolovaných oblastí je, v závislosti na složitosti systému, zhruba 100–150. Rozděleny jsou do tří základních oblastí:

- organizační opatření;
- technická opatření;
- způsob zvládání incidentů.

Nejčastější auditní zjištění

V rámci kontrol, jak Jaroslav Šmíd uvedl, nejčastěji dochází k poznatku, že sice existuje dokumentace, ale většinou z formálního důvodu není platná či úplná. Někdy nejsou dodržovány postupy, které si organizace sama nastavila. Často jsou rozpory v klasifikaci aktiv a v manipulaci s nimi. Podle Jaroslav Šmída jsou rovněž identifikovány nedostatky v řízení rizik. Ne všude, i když mají ISMS zavedeno, jsou schopni jej efektivně využívat, případně dochází k nepochopení smyslu některých dokumentů. Velké je množství formálních nedostatků, které NBÚ identifikuje a snaží se na ně upozornit.

Systémy podléhající zákonu o kyberbezpečnosti

První vlna určování proběhla od začátku loňského roku a první dávka 45 prvků kritické infrastruktury byla vládou schválena 25. května 2015. Od tohoto okamžiku musí

v letošním roce tyto systémy splňovat vyžadovaná kritéria. Druhá vlna byla realizována v druhé části roku 2015. Konkrétně v září byla předložena vládě a v listopadu byly tyto systémy určeny. Samozřejmě, jak se jednotlivé systémy i organizace vyvíjejí, určování dalších prvků a jejich identifikace probíhá neustále, a to nejen ve státní správě, ale i v soukromém sektoru. U těchto organizací vytipovalo NBÚ v loňském roce kolem 28 systémů, které byly určeny opatřením obecné povahy. V letošním roce probíhá další určování. Nyní je určeno dalších 22 prvků kritické infrastruktury v soukromém sektoru.

Znamená to, že od účinnosti zákona o kybernetické bezpečnosti máme přes 160 jednání s různými subjekty. Ve veřejném sektoru bylo určeno 48 prvků, které jsou spravovány 17 institucemi. V soukromém sektoru je nyní určeno 50 prvků u 19 správců. Pokud jde o předpokládaný vývoj, koncová čísla by podle Jaroslava Šmída měla být cca 150 v soukromém a 100 ve veřejném sektoru.

Významné informační systémy

Významné informační systémy jsou takové, které nepodléhají krizovému výkonu a jsou provozovány pouze veřejnou správou. První dávka těchto systémů byla již součástí vyhlášky. V první skupině se jednalo o 92 systémů, ale postupně 22 z nich bylo přesunuto mezi kritické systémy. I nadále identifikace probíhá, nicméně zde je mechanismus takový, že významné informační systémy si určují provozovatelé sami a NBÚ jsou pouze nahlašovány.

Nyní je aktuální novela vyhlášky, kde se aktualizuje příloha o významných informačních systémech. Nyní obsahuje 148 významných informačních systémů, ale objevují se další, a tak uvedené číslo ještě není konečné. NBÚ v této souvislosti předpokládá, že výsledné množství významných informačních systémů by mohlo být kolem 230 až 240.

Legislativa

Jak Jaroslav Šmíd upozornil, zákon o kyberbezpečnosti je v účinnosti od začátku loňského roku a definuje několik oblastí, které mu podléhají:

- poskytovatelé elektronických komunikací;
- orgány či osoby zajišťující významné sítě;
- správci informačních systémů kritické infrastruktury;
- správci komunikačních systémů kritické infrastruktury;
- správci významných informačních systémů.

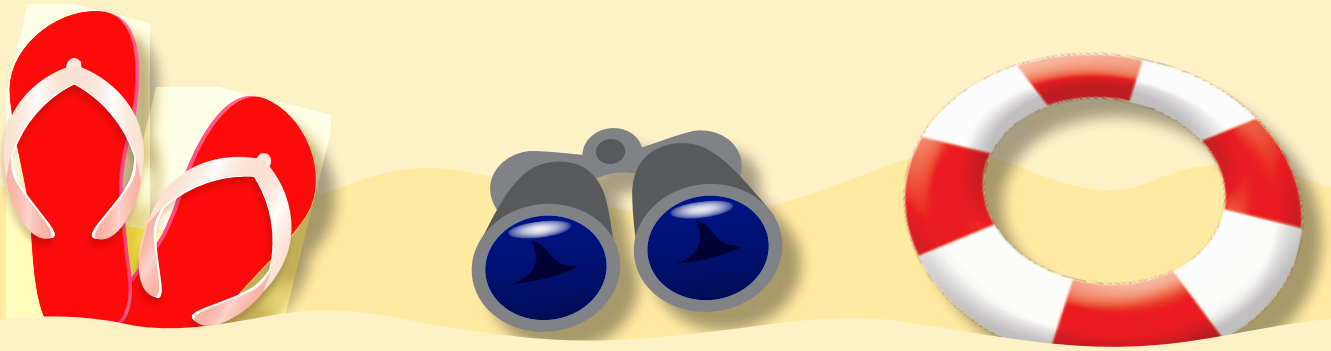
Největší požadavky jsou logicky kladeny na bezpečnost u kritických systémů. Nyní je připravována novelizace zákona, během června bude totiž zveřejněno znění evropské směrnice o bezpečnosti sítí a informací. Její transpozice je pro všechny státy povinná nejpozději do 20 měsíců od zveřejnění. Protože jsme se podíleli na tvorbě této směrnice, mohli jsme včas vytvořit pracovní skupinu (zástupci VS i soukromého sektoru, CZ NIC atp.). Podstatné je totiž, že novela by měla definovat dvě nové skupiny organizací podléhajících zákonu. Jednak jsou to poskytovatelé základních služeb (organizace, které se částečně kryjí s naším krizovým zákonem - podle Jaroslava Šmída je naší snahou dostat do systému touto cestou například nemocnice, které zatím kvůli špatně nastaveným kritériím nejsou takto podchyceny, podobně je to s plynem atp.).

Další skupinou jsou poskytovatelé služeb, jako jsou vyhledávače, cloudy a elektronická tržiště. Jak Jaroslav Šmíd upozornil, nebudeme se snažit tyto nové skupiny včleňovat do našeho krizového zákona. Bylo by to zdlouhavé a komplikované. Vytvoříme tedy další přístup k tomu, jak budeme definovat IS podléhající zákonu tak, že vzniknou tři skupiny - kritické informační systémy, významné informační systémy a skupina, která vznikne na základě uvedené směrnice EU.

Nedostatek personálu

Podle Jaroslava Šmída je největším problémem v oblasti kyberbezpečnosti nedostatek odborníků. S tím se setkávají všichni provozovatelé systémů, včetně NBÚ. Jak řekl, snažili se přispět ke zlepšení situace tím, že vytvořili návrh koncepce vzdělávání v oblasti kybernetické bezpečnosti. Návrh byl již projednán ve výboru pro školství PSP ČR. Nyní by měl být postupně implementován do praxe. NBÚ by tak rádo přispělo k tomu, aby se tato důležitá oblast dostala do škol a byla nějak smysluplně prezentována. Kromě tohoto návrhu NBÚ aktivně pracuje i na e-learningových kurzech a dalších systémech vzdělávání.

Samo NBÚ má smlouvu s osmi VŠ, vede diplomové práce a reealizuje další formy spolupráce. Velice dobrá spolupráce podle slov Jaroslava Šmída funguje v Brně s Masarykovou univerzitou. Byl zde vybudován již zmiňovaný kybernetického polygon. Na něm proběhla už dvě kybernetická cvičení, a to jak pro veřejnou správu, tak pro komerční sféru. Obě se setkala s velice kladným ohlasem. Právě takové aktivity považuje náměstek ředitele NBÚ Jaroslav Šmíd za velice důležité, protože uvedený nedostatek odborníků je možné považovat za největší bezpečnostní riziko.



Nejslabší místo kyberbezpečnosti = lidé

Prvním, kdo prezentoval názory a zkušenosti rezortů, byl Miroslav Tůma, ředitel odboru kybernetické bezpečnosti a koordinace informačních a komunikačních technologií MV ČR.

Pro přítomné si připravil stručný přehled, jak postupovalo MV ČR při implementaci zákona o kyberbezpečnosti a při zabezpečení jejich systémů. Celkově rozdělil svoji prezentaci do tří bloků:

1. implementace vlastního systému řízení bezpečnosti informací na základě zákona o kyberbezpečnosti;
2. zabezpečení jednotlivých systémů kritické informační infrastruktury a významných informačních systémů;
3. budování dohledového pracoviště (dohledového centra v SOCRU).

Pokud jde o samotné informační systémy kritické infrastruktury a významné informační systémy, pak, jak bylo již řečeno, v první vlně bylo schváleno 45 KII. Z těchto 45 spadá 17 pod MV ČR. Celkově MV ČR spravuje 27 systémů KII a VIS.

REALIZACE

Jak Miroslav Tůma přítomné informoval, na počátku realizace bylo vytvoření organizačních opatření. Konkrétně byl v rámci MV ČR zřízen **odbor kybernetické bezpečnosti**, ustaven **výbor pro řízení kybernetické bezpečnosti** (podle požadavků zákona), byl jmenován **manažer**, **auditor** a **architekt** kybernetické bezpečnosti a navíc byl vytvořen tzv. **tým kybernetické bezpečnosti**. Důvodem pro poslední krok je především šíře rezortu vnitra. Je zde sdruženo 53 organizací, s nimiž je nutno spolupracovat a které je nutno zabezpečit. Právě ze zástupců těchto organizací byl sestaven uvedený tým tak, aby bylo možné rychle implementovat dopady opatření, případně komunikovat a rozhodovat o aktuálních problémech. Zároveň byli určeni **garanti** pro jednotlivé informační a komunikační systémy kritické informační infrastruktury a významné informační systémy.

Po těchto organizačních opatření následovalo dle slov Miroslava Tůmy vytvoření organizačního zázemí. Jednotlivé uvedené složky byly propojeny základními řídícími procesy a zároveň byla vytvářena potřebná dokumentace. Bylo tedy nastaveno řízení kyberbezpečnosti a definovány základní akty. V této souvislosti upozornil Miroslav Tůma na kritický bod kyberbezpečnosti veřejné správy, kterým je legislativa. Například interní akt ministra vnitra o zřízení výboru kybernetické bezpečnosti byl připraven za dva týdny. Následně však trvalo tři měsíce, než prošel legislativním schvalováním a mohl být uveřejněn ve Věstníku. Je tedy podle něj otázkou, do jaké míry byrokratický proces brzdí samotnou kyberbezpečnost. Jak Výbor kybernetické bezpečnosti, tak tým začaly postupně pracovat. Výbor rozhoduje o strategických otázkách, tým se zabývá řešením jednotlivých opatření, jejich návrhy a vlastně zavádí a implementuje kybernetickou bezpečnost. Zároveň tým kybernetické bezpečnosti připravuje strategické podklady pro výbor a jeho rozhodování.

Jak již Miroslav Tůma uvedl, byla implementace kyberbezpečnosti pojata skutečně rezortně, protože pokrývá všech 53 organizací (Policii ČR, Hasičský záchranný sbor, ostatní OSS). Celkově tento rozsah zahrnuje podle jeho slov 70 tisíc lidí. Vedle organizační struktury bylo rovněž podstatné dodat potřebné podklady. Byl tedy vytvořen harmonogram postupu a struktura vlastní dokumentace, tedy především dokumentace ISMS (Systém řízení bezpečnosti informací dle zákona č. 181/2014 Sb.). Následovaly další dokumenty, především bezpečnostní politika. Právě na jejím základě mohlo MV ČR začít vymáhat jednotlivá opatření v rámci rezortu.

Miroslav Tůma upozornil, že i když vytvořit jednotlivé, především pak metodické dokumenty, není vůbec snadná záležitost (především ohlídat, aby nebyly duplicitní, ale vzájemně konzistentní), daleko těžší je pak jejich uvede-

ní do života. V rámci MV ČR byla v tomto směru připravena školení, zároveň však registrován určitý odpor zaměstnanců. Ti totiž mají často tendenci považovat základní principy kybernetické bezpečnosti za určité omezování (kontrola přenosných paměťových médií, zákaz používání soukromých e-mailových schránek k pracovním účelům atp.) Kromě základního školení širší veřejnosti bylo snahou MV ČR proškolit prezenčně zástupce jednotlivých odborů, útvarů a organizací. Podle Miroslava Tůmy byla představa taková, že tito proškolení „misionáři" budou povědomí o kyberbezpečnosti šířit dále do svých útvarů. To se bohužel nepotvrdilo. Bylo tedy nutné zvolit jinou metodu. Připravili webový portál s e-learningovým kurzem (s ohledem na množství lidí, které bylo nutno proškolit, nejúčinnější metoda). Ta školení, včetně příslušné dokumentace, jsou rozdělena na jakási základní a následně speciální podle rolí. Jak Miroslav Tůma uvedl, nejjednodušší je školení nových zaměstnanců, neboť ti nedostanou přístup do kyberprostoru dříve, než provedou základní seznámení s požadavky a zásadami kybernetické bezpečnosti a projdou příslušným školením. U stávajících zaměstnanců existuje vždy, sice minoritní, ne však nepodstatná skupina, která není ochotna pochopit nutnost takových kroků. Školení považuje za ztrátu času, zbytečné obtěžování a má dojem, že uvedenými pokyny se nemusí řídit. Potvrzuje to jeho přesvědčení, že v oblasti kyberbezpečnosti je nejtěžší právě práce s lidmi, samotnými uživateli.

Kromě školení dochází i k další distribuci informací, varování a doporučení. Na základě rozhodnutí kybertýmu jsou rozesílány informace například o hrozbě podvodného e-mailu a upozornění, jak s takovým nakládat. Tyto informace jsou distribuovány podle povahy buď všem, nebo jen určitým skupinám osob. Vedle toho existuje katalog hrozeb a opatření, tedy jakási databáze, co se může stát a jak se má postupovat. Zároveň je řada těchto dokumentů sdílena na intranetu se všemi organizacemi. Podstatné je, že od počátku se jedná o „bezpapírovou" dokumentaci, tedy vše je k dispozici pouze v elektronické podobě.

Miroslav Tůma ještě považuje za podstatné, že ve chvíli, kdy byl celý systém nastaven a implementován, nechalo jej MV ČR certifikovat podle ISO 27001 (od prosince 2015 je tedy certifikován systém implementace řízení bezpečnosti informací).

ZABEZPEČENÍ

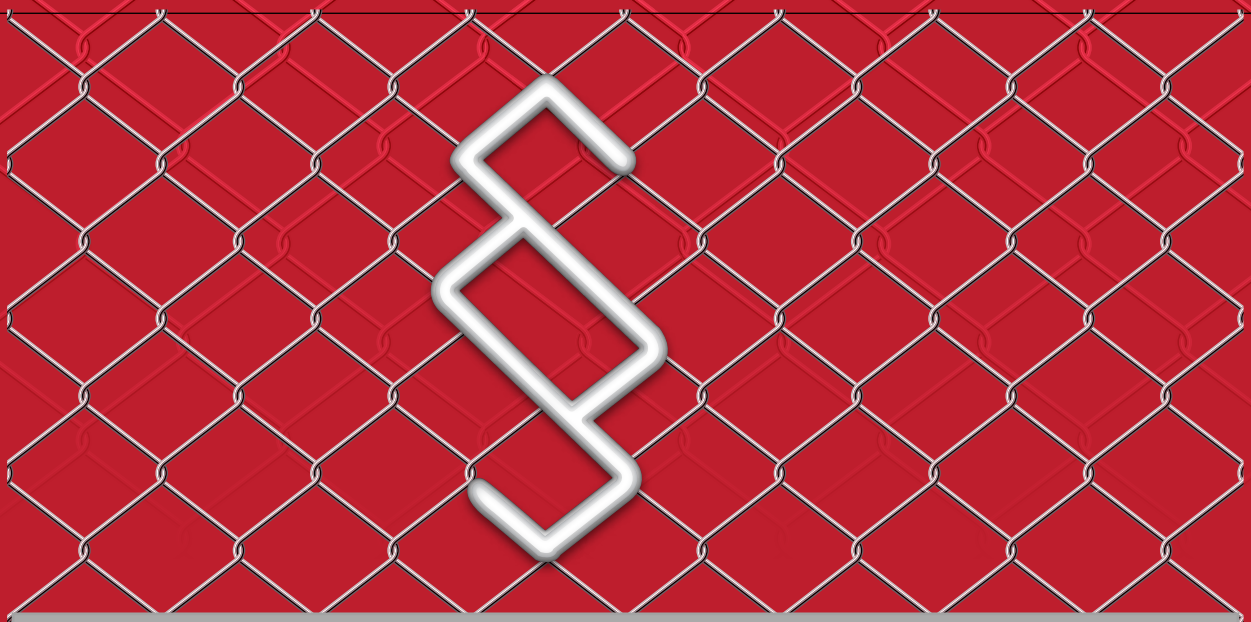
V rezortu MV ČR se jedná o 17 kritických informačních systémů a 10 významných informačních systémů, nicméně na ně navazuje a s nimi je provázáno dalších 120 systémů. Ty není možné oddělit, je tedy nutné je rovněž přiměřeně zabezpečovat. Při analýze rizik je nutné posuzovat každý tento systém samostatně a zároveň provázat a dívat se na ně jako na celek. Podle Miroslava Tůmy je to nikdy nekončící práce, neboť je třeba nastavení neustále analyzovat a stále zlepšovat. Základem příslušné dokumentace je v tomto směru analýza rizik, plán zvládání rizik a realizace odpovídajících opatření. Problémem je, že výstupem takové analýzy jsou finančně dosti náročná opatření. Je tedy nutné řešit jednotlivé kroky v pořadí určitých priorit. Je pravdou, že určitou pomůckou mohou být při jejich určování požadavky zákona, nicméně jak Miroslav Tůma upozornil, vlastní zabezpečení je podstatnější než litera zákona. Je to tedy velice složitý postup.

DOHLED

V praxi došlo postupně k napojování jednotlivých systémů na budované dohledové centrum, bylo řešeno nahlašování a následné řešení jednotlivých událostí a incidentů tak, aby byla zcela jasná vazba na vládní cert - NCKB (Národní centrum kyberbezpečnosti). Jak bylo již řečeno, každý systém má svého garanta, bezpečnostní dokumentaci a další provozní dokumentaci (především bezpečnostní politika, hodnocení rizik atd). Podle zkušeností Miroslava Tůmy se jeví jako nejsložitější ona riziková analýza. Pro její tvorbu se vychází z identifikace aktiv, která je nutné zatřídit a popsat. Následně jsou tato aktiva propojena v rámci modelu, abychom mohli identifikovat jednotlivé vazby. Hodnocení na základě zákona (dostupnost, důvěrnost, integrita) vede ke shrnutí hrozeb a jejich předpokládaných dopadů. Na základě toho pak dojde k výběru jednotlivých bezpečnostních opatření. Výsledkem je tedy konkrétní řešení popsané v příslušné dokumentaci. Tento proces se podle jeho slov neustále opakuje. Výstupy, tedy aktiva, hrozby a opatření jsou provázány databázově. V tom je ona složitost systému. Data jsou propojena tak, aby v případě, že učiním nějaké opatření, bylo ihned zřejmé, jaká další opatření to může ohrozit či posílit.

SOUHRN

Miroslav Tůma tedy zopakoval, že v rámci resortu MV ČR vytvořili bezpečnostní dokumentaci, zavedli organizační i technická opatření a celý systém napojili na dohledové centrum. To je základním centrem, které monitoruje jednotlivé systémy, infrastruktury i perimetry a které je neustále k dispozici rovněž pro nahlašování incidentů či pomoc.



Zákon o kybernetické bezpečnosti není kybernetická bezpečnost

Na vystoupení Miroslava Tůmy navazovala další rezortní prezentace, a to Miloslava Marčana za MPO. Ten připustil, že po prezentaci MV ČR dostal jistý pocit méněcennosti a zakomplexovanosti. MPO je totiž výrazně menší organizací, než je MV. V rezortu průmyslu a obchodu pracuje dohromady 2000 lidí, což je zhruba 35x méně než na MV. Proto si Miloslav Marčan myslí, že jejich zkušenosti ze zavádění zákona o kybernetické bezpečnosti budou zajímavé spíše pro menší organizace.

Jak Miloslav Marčan uvedl, MPO se otázkami kybernetické bezpečnosti zabývá už dlouho. V roce 2007 přijali jako jedni z prvních bezpečnostní politiku, včetně veřejné deklarace. Tu nejen publikovali na vlastním webu, ale v návaznosti na ni zpracovali řadu dokumentů, které vycházely z filozofie norem řady 27000. Před zákonem o kybernetické bezpečnosti se tedy MPO mohlo v oblasti kybernetické bezpečnosti opřít už o některá ustanovení zákona o informační sféře veřejné správy. Ta ve svých prováděcích vyhláškách ukládají provozovatelům i správcům informačních systémů určité povinnosti právě v oblasti kybernetické bezpečnosti. Určitá opora v zákoně zde tedy již existovala, i když Miloslav Marčan připouští, že nebyl tak důrazný jako zákon o kybernetické bezpečnosti.

Už v minulosti byla tedy v rámci MPO oblast kybernetické bezpečnosti součástí každého nového projektu. A navíc, jak Miloslav Marčan zdůraznil, mělo MPO i některé projekty přímo cílené do této oblasti (zpracování havarijních plánů, zavedení systému SIEM v rámci ministerstva, zavedení systému Varonis atp.).

CO PŘINESL ZÁKON?

Jak Miloslav Marčan připustil, zákon o kybernetické bezpečnosti donutil rezort průmyslu a obchodu udělat revizi a aktualizaci stávajících dokumentů, zahájit novou analýzu rizik a metodicky vést zhruba 10 rezortních organizací. V souladu s požadavky zákona určili významné informační systémy. V podmínkách MPO se zatím jedná o dva významné informační systémy. Je to registr živnostenského podnikání a ekonomický informační systém. Obdobně i v podřízených organizacích probíhá proces určování významných ekonomických systémů. Podle odhadu Miloslava Marčana budou nahlášeny v rezortních organizacích zhruba čtyři takové systémy.

ŘÍZENÍ KYBERNETICKÉ BEZPEČNOSTI

V rámci MPO byl zřízen výbor pro řízení kybernetické bezpečnosti s rozšířenou pravomocí, a to i se snahou metodicky řídit podřízené organizace. Členy výboru jsou zástupci jednotlivých rezortních organizací. Stejně jako na ostatních ministerstvech i MPO má svého architekta kybernetické bezpečnosti. Na doporučení NBÚ přidali do uvedeného výboru zástupce za legislativu a zástupce z odboru bezpečnosti a krizového řízení.

Samotný zákon naplňuje MPO tím, že zpracovalo akční plán, který identifikoval 14 základních oblastí. Jedná se například o aktualizaci bezpečnostní politiky, nastavení kontrolních mechanismů, či implementaci procesu zvládání kybernetických incidentů do provozu, včetně interakce s NBÚ nebo s Národním centrem pro kybernetickou bezpečnost. V rámci těchto 14 oblastí bylo identifikováno až 83 aktivit. Uvedený akční plán vychází rovněž z analýzy rizik. Výstupem je tabulka v Excelu, v níž jsou jednotlivá rizika pojmenována. Celkově jich bylo, podle slov Miloslava Marčana, identifikováno 537. Z vlastního hodnocení vyplývá, že většina z nich je nízkých, zhruba 10% je středních. I v jejich rámci jsou dopady spíš nižšího nebo středního rázu. Podle Miloslava Marčana je to možná důsledkem skutečnosti, že se MPO kybernetické bezpečnosti věnuje průběžně přes 10 let.

Jak bylo již řečeno, NBÚ nabízí určitou pomoc ve formě auditů. MPO si jeden takový přímo vyžádalo, a to před vlastním schválením uvedených dokumentů. K samotnému auditu došlo v březnu 2016 a byl zaměřen hlavně na registr živnostenského podnikání. Miloslav Marčan musí konstatovat, že auditoři z NBÚ jsou vysoce kvalifikovaní a profesionální odborníci, kteří věděli, co hledají, jak mají auditovat. Z jeho pohledu měl audit velice hladký průběh. Konkrétně v rámci 77 kontrolovaných položek bylo 72 shod. Dvě neshody byly organizačního a administrativního charakteru. Jeden z důvodů byl dán tím, že se kontrolovala dokumentace, která nebyla schválená. To byl ale z pohledu MPO záměr, nechtělo ji před metodickou podporou schvalovat, protože by pak muselo měnit schválenou dokumentaci a jednalo by se o složitější proces. Miloslav Marčan tedy v této souvislosti vyzval kolegy z ostatních rezortů, aby s vyžádáním metodické pomoci NBÚ neváhali, protože není nač čekat.

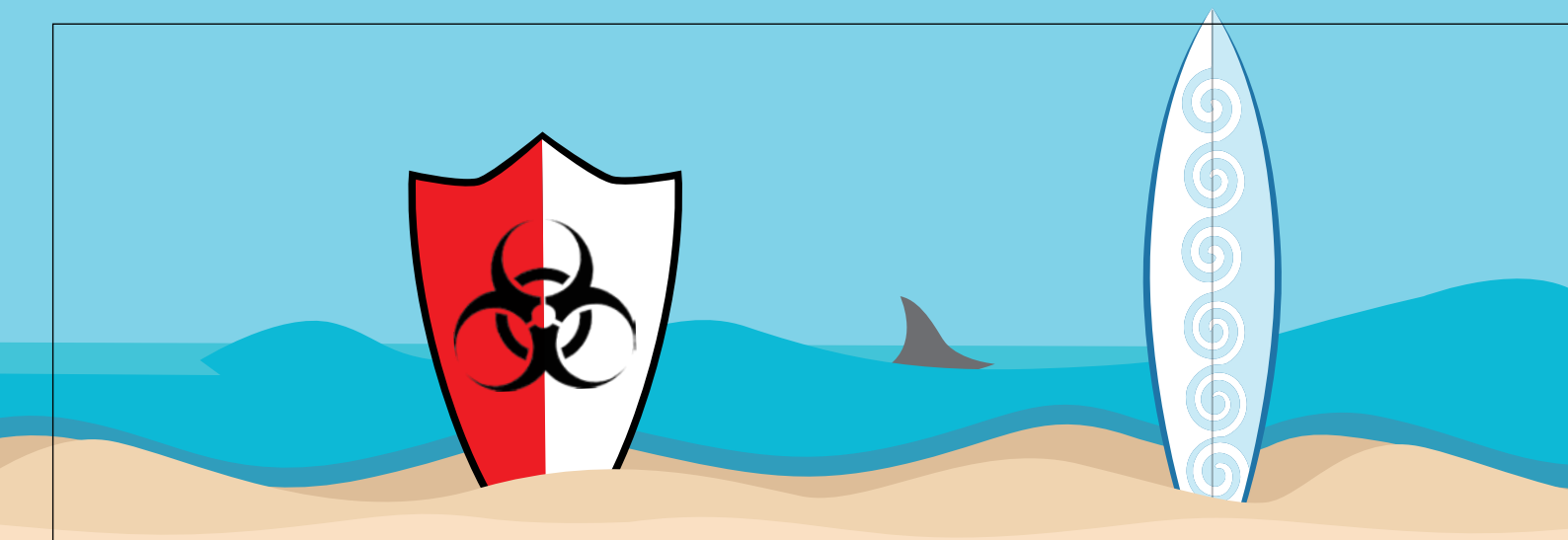
CO NÁM ZÁKON PŘINESL?

Miloslav Marčan upozornil, že je důležité si uvědomit, že zákon o kybernetické bezpečnosti není kybernetická bezpečnost. Zákon vytváří pouze bezpečnostní rámec. Je ale na nás, jak jej budeme implementovat do praxe nejen ve formální nebo formalizované podobě, ale hlavně v praktických činnostech. Miloslav Marčan sleduje, že existuje určitá obava z jeho naplňování, ale jak doufá, právě metodický audit, který na MPO proběhl, ji vyvrátil. Stejně tak apeluje na to, aby si budoucí auditoři dali pozor na zbytečně formalistický přístup. Tedy aby nesklouzli k praxi, kterou mají finanční úřady nebo NKÚ apod., ale aby se snažili být skutečně praktickým pomocníkem na cestě k zajištění bezpečnosti.

Klad v zákoně o kyberbezpečnosti vidí Miloslav Marčan v tom, že přinesl osobní zodpovědnost statutárních zástupců jednotlivých organizací. Pokud tedy právě oni budou bránit zavádění opatření ke zvýšení kybernetické bezpečnosti, tak sami sebe mohou nyní dostat do problémů, protože oni jsou ze zákona zodpovědni za tuto činnost.

Další klad zákona o kybernetické bezpečnosti spatřuje Miloslav Marčan v tom, že se podařilo vybudovat Národní centrum kybernetické bezpečnosti. To se stává významným pracovištěm v ochraně kybernetické bezpečnosti a současně, na základě metodické pomoci, umožňuje sjednotit postupy v řízení kybernetické bezpečnosti.

Miloslav Marčan neměl připravenu žádnou kybernetickou hrozbu, ale rozhodně musí podpořit již zmíněný názor, že jí je nedostatek odborníků. Jak řekl, personální situace ve veřejné správě je v této oblasti naprosto zoufalá, a pokud se v krátké době něco nezmění, jedná se skutečně o bezpečnostní riziko.



K ochraně proti kybernetickým hrozbám je třeba přistupovat systematicky

Masivní technologický rozvoj a nový přístup k IT sice organizacím přinesly nové výhody, jako je provozní pružnost a flexibilita, širší možnosti kontaktu se zákazníky a celkové zrychlení ve všech směrech, zároveň ale vytvořily prostředí pro nové hrozby. Pokud chtějí organizace udržet krok s neustále se vyvíjejícími kybernetickými hrozbami, musí k zabezpečení své infrastruktury přistupovat proaktivně, nikoli reaktivně. Společnost Fortinet nabízí komplexní bezpečnostní řešení, která vynikají nejen špičkovou funkcionalitou, ale i přehledností a jednoduchou správou.

Společnost Fortinet vyvíjí, vyrábí a prodává portfolio produktů a služeb, které tvoří nejmodernější a nejvýkonnější síťovou bezpečnostní platformu, s jejíž pomocí mohou zákazníci bezpečně budovat a rozvíjet své IT infrastruktury, a to jednodušeji a s nižšími náklady. Díky integraci širokého spektra bezpečnostních služeb v jednom zařízení pomáhá Fortinet zjednodušit celou síťovou infrastrukturu a zajistit pohodlnou centralizovanou správu, lepší kontrolu a ucelený pohled na bezpečnostní situaci v reálném čase.

Následky bezpečnostních incidentů jsou vážnější než pouhá ztráta dat

Přestože se kybernetická bezpečnost, i díky schválení kybernetického zákona, dostává do veřejné diskuze stále častěji, jedním z největších problémů současných firem je skutečnost, že mají tendenci kybernetické hrozby podceňovat. S tím, jak se změnily technologie, způsob práce s daty a posunulo se řízení systémů, které zasahují do reálného světa, je třeba adekvátně změnit i způsob ochrany.

Firmy a instituce si musí uvědomit, že žijeme ve světě, kde většina činností probíhá elektronicky nebo je určitým způsobem na elektronické systémy napojena. Ve světě, kde je většina informací uchovávána a zpracovávána prostřednictvím digitálních systémů, může ohrožení těchto dat způsobit nejen obrovské ekonomické škody, ale reálně i narušit bezpečnost jednotlivců i celých organizací. Ztráta a diskreditace dat je totiž v dnešní době závažným problémem, který může ohrozit konkurenceschopnost firmy, poškodit její jméno a zkompromitovat zákaznická data. Ještě závažnější jsou pak možnosti škod fyzických, způsobených potenciálním útokem na průmyslové a řídicí systémy. Rizika plynoucí z narušení kapacity a kvality výroby může potenciálně pocítit každý z nás.

Navíc je třeba si uvědomit, že cílem hackera se může stát i obyčejná domácnost. Dnes už i velmi malý procesor v pračce nebo v běžném routeru má nezanedbatelný výkon a v době, kdy lze připojit k internetu prakticky jakékoli zařízení, může hacker napadnout celý domácí systém a získat významnou výpočetní kapacitu. Elektřinu platí nic netušící oběť, navíc se vystavuje riziku, že útočník využije informace o jejím životním rytmu k tomu, aby mohl domácnost vykrást.

Zajistit dostatečné zabezpečení firemních sítí v době, kdy se o slovo hlásí nové trendy a technologie, jako je internet věcí, využívání soukromých mobilních zařízení, softwarově definované sítě či cloud, je pro IT oddělení obrov-

skou výzvou. Častým řešením řady firem je přidat další bezpečnostní řešení do infrastruktury již tak nepřehledné a přetížené. Složitost systému je přitom jednou z největších překážek bezpečnosti. Izolovaná bezpečnostní řešení s vlastní správou nemají šanci zajistit potřebnou komunikaci s ostatními systémy. Místo aby pomáhaly s ochranou infrastruktury, jejich obsluha a optimalizace pouze vytváří zbytečnou pracovní zátěž.

Jako řešení nabízí Fortinet novou bezpečnostní platformu „Cyber Security Fabric". Ta integruje kompletní bezpečnostní technologie pro koncové body, přístupovou vrstvu, sítě, aplikace, datová centra, obsah i cloud do jediného bezpečnostního řešení, které lze řídit prostřednictvím jednoho rozhraní. Zákazníci tak získají přehledné a vysoce škálovatelné bezpečnostní řešení s jednoduchou správou, které v sobě integruje špičkové bezpečnostní funkce a využívá pokročilé analytické nástroje pro ještě lepší ochranu proti kybernetickým hrozbám. Pro jednodušší integraci v rámci firemní infrastruktury a maximální využití stávajících zdrojů nabízí Fortinet otevřená rozhraní API umožňující technologickým partnerům a řešením třetích stran stát se součástí Fortinet Cyber Security Fabric.

Inovace na prvním místě

Od svého založení v roce 2000 společnost Fortinet vyvíjí technologie vlastními silami a má dokonalou kontrolu nad podobou svých produktů, bez kompromisů v kvalitě, výkonu a spolehlivosti. Za úspěchem Fortinetu stál právě jeho inovativní přístup. V době, kdy se všichni ostatní výrobci snažili na každou funkcionalitu využít speciální zařízení, Fortinet šel cestou all-in-one řešení, což se ukázalo jako správná strategie, která mu zajistila nezanedbatelný vývojový náskok. Ten se promítá nejen do kvality, ale i do cen. Díky vývoji vlastního HW se Fortinet nemusí spoléhat na řešení třetích stran a dosahuje velmi vysoké výkonnosti za zajímavou cenu.

Mimoto je společnost Fortinet jediným dodavatelem síťových bezpečnostních řešení, kterému dodává úplnou analýzu aktuálních hrozeb a veškeré bezpečnostní a aplikační signatury pro všechny produkty, vlastní globální tým, který neustále sleduje bezpečnostní scénu a poskytuje zákazníkům nepřetržitou ochranu před nejnovějšími internetovými hrozbami v reálném čase. Odborný tým v laboratořích FortiGuard čítá přes 200 výzkumných analytiků, techniků a forenzních specialistů rozmístěných po celém světě, kteří poskytují bezpečnostní aktualizace 24 hodin denně 7 dní v týdnu, a to s bezkonkurenční dobou reakce na nové a rozvíjející se hrozby, které ohrožují sítě, obsah a mobilní zařízení zákazníků.

Nadstandardní zákaznická podpora v českém jazyce

Na českém trhu působí společnost Fortinet již osm let a má zde velice silnou pozici. Technické a asistenční centrum v Praze zaměstnává více než 80 inženýrů v jednotlivých úrovních podpory, což umožňuje rychle a flexibilně řešit požadavky a dotazy bez ohledu na jejich náročnost. Obrovskou přidanou hodnotou technické podpory Fortinet oproti konkurenci je možnost komunikace v českém jazyce. Téměř polovinu inženýrů tvoří Češi, zákazníci se tak nemusí obávat zdlouhavé a složité komunikace s technickou podporou v jiných zemích, potažmo dokonce v jiných časových pásmech. Fortinet si zakládá na tom, že bezpečnost, kterou si firma koupí, není bezpečností jen k datu nákupu, ale po celou dobu životnosti zařízení.

Ing. Ondřej Šťáhlavský,
Regional Director CEE Fortinet

VMware NSX – revoluční řešení splňující nejvyšší standardy kyberbezpečnosti

Role IT v rámci organizací se výrazně mění. Stále více firem i organizací si začíná uvědomovat, že technologie mohou sehrávat klíčovou roli při zvyšování konkurenceschopnosti, zlepšování služeb interním i externím zákazníkům a bezpečném provozu. Spolu s tím ale vzniká i tlak na IT pracovníky, očekávají se od nich stále rychlejší a flexibilnější řešení, která jsou zároveň bezpečná a cenově dostupná.

VMware, který před lety způsobil revoluci v IT díky virtualizaci serverů, přenáší tento koncept na celé datové centrum. Rozšířením principů virtualizace, jako je abstrakce, sloučení a automatizace, na všechny zdroje a služby datového centra, vzniká architektura softwarově definovaného datového centra (SDDC). SDDC je odpovědí na požadavky moderního IT, protože zajišťuje výrazně vyšší výkon s nižšími kapitálovými výdaji, dramaticky zrychluje nasazení a poskytování aplikací a zjednodušuje správu a provoz s nejvyššími bezpečnostními standardy.

Virtualizace sítí s VMware NSX

Problémem běžných síťových a bezpečnostních řešení je jejich nedostatečná přizpůsobivost, složitost a nekompatibilita s řešením jiných výrobců. To vše dohromady brání podnikům naplno využívat výhody modelu softwarově definovaného datového centra, především co se týče pružnosti, efektivity a optimalizace nákladů.

VMware NSX tento problém řeší, protože díky virtualizaci sítí umožňuje provozovatelům datových center zacházet s fyzickými sítěmi jako se zdrojem transportní kapacity, který lze využívat a měnit podle požadavků. Protože VMware NSX zajišťuje celý OSI model sítí a zabezpečení (Layer 2 – Layer 7) v podobě softwaru, mohou zákazníci rozšířit svou infrastrukturu pouhým přidáním serverových uzlů.

Díky NSX poskytuje VMware zákazníkům tzv. Zero-Trust bezpečnou infrastrukturu za třetinové náklady oproti tradičním přístupům. Dokáže zákazníkům pomáhat při automatizaci, která umožňuje jejich IT reagovat na vývoj potřeb bez zpoždění, a to díky urychlení poskytování infrastruktury z měsíců na minuty. NSX také pomůže zlepšit dostupnost aplikací a zkrátit cílovou dobu obnovy až o 80%.

Řešení vyvinuté na základě požadavků organizací

Síťová virtualizační platforma VMware NSX byla na trh uvedena v roce 2013. Od té doby získala celou řadu vylepšení a nových funkcionalit vycházejících z reálných poznatků a připomínek zákazníků, distribučních partnerů a profesionálních poskytovatelů služeb. Aktuální verze VMware NSX 6.2 je významným milníkem hned z několi-

ka důvodů – obsahuje přes 20 nových funkcí reagujících na potřeby organizací, a co je důležitější, prošla testováním podle více než 1000 různých scénářů a díky tomu je připravena na reálný provoz lépe než kdy dříve.

Novinky v NSX spadají do tří samostatných kategorií:

- **Lepší možnosti řízení toku dat v datovém centru a mezi datovými centry** – VMware NSX 6.2 zlepšuje nepřetržitý provoz aplikací a usnadňuje obnovu po výpadku prostřednictvím podpory dynamického směrování a zabezpečení s vCenter vMotion přes VXLAN. Správci mohou hladce migrovat mezi serverovými systémy vCenter bez ztráty historických dat o virtuálním stroji. VMware NSX 6.2 zákazníkům umožňuje podle potřeby rozšiřovat prostředí vSphere v rámci jednoho i více datových center přenášením celého síťového a bezpečnostního modelu spolu s virtuálním strojem, aniž by bylo nutné jakkoli upravovat příslušnou fyzickou infrastrukturu.
- **Hlubší integrace do fyzické infrastruktury** – VMware NSX 6.2 zavádí podporu Open vSwitch Database (OVSDB) do sítí NSX v prostředí vSphere, což umožňuje jednodušší a konzistentnější provoz celé sítě datového centra a rozšíření mikrosegmentace na fyzické servery. Podpora OVSDB umožňuje integraci s partnerským hardwarovým přepínáním a pokročilými řešeními pro vyvažování zátěže pomocí mechanismů založených na obecně přijímaných standardech, což dále zjednodušuje zavádění síťové virtualizace v datových centrech.
- **Pokrok v oblasti provozu a řešení problémů** – funkce Traceflow umožňuje uměle vytvořit paket, který vypadá, jako by přesně pocházel od hostujícího virtuálního stroje, a lze jej vložit do datového toku. Centrální rozhraní NSX s příkazovou řádkou (CLI) umožňuje zachytávat sdílené provozní informace ze všech distribuovaných komponent v systému a zobrazuje je v jediném rozhraní.

Nové hrozby si žádají nové řešení

Společným a stále více skloňovaným jmenovatelem pro organizace je bezpečnost IT ekosystému a kyberbezpečnost.

„Bezpečnostní hrozby jsou jedinou oblastí, která roste rychleji než výdaje na zabezpečení infrastruktury," trefně komentoval Pat Gelsinger, CEO společnosti VMware, aktuální situaci na poli informačních technologií. Kybernetické útoky se dynamicky vyvíjejí a hledání účinných způsobů obrany patří k největším globálním a politickým výzvám dneška.

Odpovědí je jednoznačně mikrosegmentace procesů v rámci SDDC architektury, která zabraňuje šíření útoků a nebezpečného kódu uvnitř datového centra. Řada firem sice využívá pokročilý firewall, pokud však hrozba pronikne za něj, nemají firmy většinou metody, jak útok zastavit. Mikrosegmentace vytvoří interní systém firewallů, které mají strukturu podobnou včelí plástvi, a umožňuje okamžitě aplikovat nová pravidla pro různé firewally v rámci datového centra. Díky tomu mohou organizace efektivně zachytit a izolovat hrozby dříve, než napadnou další stroje.

Jak může NSX pomoci při naplnění požadavků zákona o kyberbezpečnosti?

- **Vestavěná bezpečnost v designu řešení:** NSX a jeho Zero-Trust bezpečnostní model uvnitř datacenter a cloudů.
- **Minimalizace rizik:** bezpečnostní skupiny povolují sestavit adaptivní, aplikačně-centrickou bezpečnostní politiku pro virtuální stroje v momentě provisioningu a aplikuji zadaná firewallová pravidla v souladu s požadavky aplikací.
- **Kontrola bezpečnostní úrovně v reálném čase:** síťová a Guest introspekce umožní kontrolovat bezpečnost virtuálních strojů a dynamicky je odsunout do tzv. „Quarantine Security-group" v případě napadení.
- **Posouzení vlivu na osobní data:** řešení NSX a vRealize Operations umožní organizacím vytvořit vlastní šablony pro posouzení vlivu na osobní data a tím získat realistický pohled na bezpečnost celého datacentra.
- **Šifrování dat v pohybu:** NSX Edge vykonává IPSec a SSL VPN tunelování pro uživatele a partnery vně datacenter.

Více informací o VMware NSX je k dispozici zde:
www.vmware.com/cz/products/nsx/

vmware®

Kyberbezpečnost – víc než jen informatika

O závěrečné vystoupení semináře, ve kterém několikrát zaznělo, že přenosovou soustavu je potřeba chránit i z pohledu kybernetické bezpečnosti, se postaral Ing. Jan Šmolík, vedoucí oddělení strategie a bezpečnost ICT, ČEPS, a.s.

V úvodu přítomné blíže seznámil se společností ČEPS, která je provozovatelem přenosové soustavy. 100% akcií společnosti je drženo státem a jako jediná v České republice vlastní licenci na přenos elektřiny. Společnost poskytuje přenosové a systémové služby - prostřednictvím přenosových služeb je elektrická energie přenesena z místa výroby do místa spotřeby a systémové služby zajišťují prostřednictvím dispečerského řízení rovnováhu mezi výrobou a spotřebou elektřiny v každém okamžiku. Společnost ČEPS je rovněž součástí významných mezinárodních energetických organizací a sdružení.

Z pohledu bezpečnosti informací je podstatné, že společnost byla certifikována podle normy ISO/IEC 27001 v rozsahu předmětu jejího podnikání. Certifikační autoritou je společnost DNV-GL, která je akreditovaná u britské agentury UKAS. Iniciační audit proběhl v prosinci roku 2014 následovaný o rok později periodickým auditem. Rozsah ISMS je vymezen přes všechny procesy společnosti včetně procesů dceřiné společnosti ČEPS Invest. Představenstvo obou společností je informováno dvakrát ročně o stavu ISMS formou Management review. V polovině roku o průběžném plnění cílů ISMS a v listopadu o celém ISMS, včetně návrhů na jeho zlepšení.

BEZPEČNOSTNÍ DOKUMENTACE

Jan Šmolík se dále věnoval organizaci bezpečnostní dokumentace ve společnosti. Základním dokumentem je bezpečností řád, který definuje celkovou bezpečnostní politiku. Na tento řád navazuje směrnice Bezpečnost informací, která má 11 příloh. Jan Šmolík zdůraznil první tři, což jsou Klasifikace a ochrana informací, Pravidla bezpečnosti informací pro uživatele informačního systému a Pravidla pro provozovatele informačního systému. Tyto tři přílohy směrnice jsou také součástí smluv uzavíraných s dodavateli vybraných ICT služeb.

Detailní revizi analýzy rizik provádí společnost ČEPS každé tři roky dle metodiky RAMSES (jejím základem je metodiky CRAMM). Analýza trvá řádově 5 – 6 měsíců a je do ní zainteresováno cca 16 manažerů společnosti a cca 30 vlastníků aktiv.

Revize analýzy rizik je prováděna 1x ročně. Výstupem revize je plán zvládání rizik, který je součástí cílů ISMS. Interní audit ISMS je prováděn 1x ročně ve spolupráci s externisty. Rovněž prohlášení o aplikovatelnosti je revidováno jednou ročně. Jako součást řízení dodavatelů jsou prováděny zákaznické audity u poskytovatelů služeb kritické informační infrastruktury.

TĚŽKO NA CVIČIŠTI...

Společnost ČEPS také, podle slov Jana Šmolíka, absolvovala v minulých dvou letech některá kybernetická cvičení. Všechna cvičení byla jednotlivými účastníky velmi pozitivně hodnocena.

- **CyberCzech II** organizované NBÚ se zaměřením na ochranu infrastruktury společnosti.
- **Cyber Defense Exercise** – jehož cílem bylo seznámit jednotlivé správce infrastruktury s tím, jak uvažují útočníci, jaké používají techniky, jak skrývají svoji činnost v infrastruktuře, jakým způsobem lze jejich činnost detekovat, popřípadě jak zjistit jejich cíl a motiv.
- **Red Team Blue Team Training** připravené European Network For Cyber Security se zaměřením na obranu průmyslových řídicích systémů a Smart Grid systémů. Po teoretické části následovalo praktické cvičení, ve kterém bylo demonstrováno, že uvedené systémy je možné prolomit a získat nad nimi plnou kontrolu.
- **Strategic Decision Making Course** organizované za českou stranu NBÚ. Cvičení bylo zaměřeno především na procvičení komunikačních kanálů a spolupráci při řešení kybernetických incidentů mezi čtyřmi skupinami – vládními složkami, armádou a zpravodajskými službami, policejními složkami a státním zastupitelstvím a soukromým sektorem. Přínos společnost ČEPS shledává v řešení jednotlivých scénářů z pohledu kdo a na jaké úrovni činí rozhodnutí, zda je potřeba spolupráce zúčastněných složek a proč, kolik je třeba času

k rozhodnutí a jak by měla být informace o rozhodnutí chráněna.

- **NATO CMX 2015.** Součástí cvičení bylo ověřit reakční a komunikační scénáře po napadení přenosových soustav Polska a České republiky prostřednictvím zavlečeného škodlivého kódu zhrzeným zaměstnancem.

CO NÁM DAL CERTIFIKAČNÍ AUDIT

Jan Šmolík shrnul přínosy auditu pro společnost takového rozsahu a důležitosti, jakou ČEPS je. Podle jeho vlastních slov se poznatky dají vyjádřit jako dostavení se určitého „Aha efektu". Jak řekl, některé útvary ve společnosti se domnívaly, že ISMS a bezpečnost informací se týká pouze informatiky a fyzická bezpečnost s personální bezpečností do rozsahu nepatří. Nikdo zpočátku nechápal, proč se auditor ptá na revizní zprávy elektrospotřebičů, proč se ptá na to, jak a podle čeho jsou řízeni dodavatelé na stavbách (vždyť to přece nesouvisí s informatikou) apod.

Došlo tedy k určitému vzdělávacímu efektu v tom smyslu, že rámec auditu je vymezen pro společnost tím, jaké jsou její zákonné povinnosti, jaké jsou její cíle, jaké má v uzavřených smlouvách závazky a co vyžaduje norma ISO/IEC 27001. Bezpečnost informací je postavena na základě řízení rizik a je třeba věnovat odpovídající pozornost všem procesům.

Za pozornost stojí například objekty v rekonstrukci. Stává se, že na jednom objektu pracuje současně více dodavatelů. Někteří vykonávají stavební činnost, jiní dodávají infrastrukturu. Cílem je provést rekonstrukci za předem daných podmínek, při zachování kritických procesů společnosti. S tím souvisí nastavené podmínky v uzavřených smlouvách, jak jsou zajištěny a prováděny stavební dozory, jak je řízen přístup do objektu, jak je řízen pohyb osob a pořádek na staveništi, jak jsou prováděny kontroly a jak jsou účinné (např. zda pustit auto s mixem do objektu, když řidič není registrován pro vstup apod.). To je řada výzev a otázek "všedního" dne, s kterými je třeba se vypořádat. Výsledek auditu podle Jana Šmolíka vedl mimo jiné i k tomu, že byla revidována pravidla pro přístup do objektu a pro řízení dodavatelů na stavbách tak, aby bylo dosaženo cíle a nastavená pravidla nevedla k zablokování činností během rekonstrukce.

Další zajímavý nález z auditu je podle Jana Šmolíka například otázka nesdílených kompetencí. Jde o situaci, kdy sice každý útvar dělá sám za sebe vše na jedničku, ale ve chvíli, kdy se na to podíváme jako na výsledek celku, dochází k překryvům, anebo zůstávají „bílá" místa. Je tedy nutné "vyladit" spolupráci jednotlivých útvarů, aby se skutečně doplňovala a navazovala na sebe.

U zákaznických auditů vidí velký přínos v sladění požadavků na činnosti vykonávané vlastními zaměstnanci a třetími stranami. Rovněž je třeba společně vnímat rizika spojená s vykonávanou činností třetích stran pro naše systémy, zejména prvky kritické informační infrastruktury.

A CO ZÁKON

Jan Šmolík uvedl, že velmi často dostával otázku, zda zavedení zákona o kybernetické bezpečnosti znamenalo pro společnost ČEPS nějaké zvýšení nákladů, lidských zdrojů či provozní investice. V této souvislosti prohlásil, že s ohledem na charakter firmy bezpečnost a spolehlivost provozu vždy byla a je její nedílnou součástí. To znamená, že uplatnění zákona žádné další náklady nepřineslo. Zákon o kybernetické bezpečnosti pomohl k urychlení certifikace podle standardu. Stejně tak pro diskuse a rozhodování některých útvarů je důležitou argumentací skutečnost, že k 9. říjnu letošního roku by mělo být vše v souladu se zákonem a připraveno na případnou kontrolu.

SPOLUPRÁCE S NBÚ

Spolupráce probíhala především v oblasti definování prvků kritické informační infrastruktury, konzultací o výkladu kybernetického zákona a analýzy rizik, případně byla diskutována i kritéria pro určování prvků kritické informační infrastruktury. Jak Jan Šmolík upozornil, NBÚ rovněž poskytuje společnosti ČEPS zpětnou vazbu o jejím internetovém perimetru. Naopak NBÚ vyžaduje zpětnou vazbu, zda jsou nálezy relevantní, případně jak s nimi bylo naloženo. Jan Šmolík v tomto směru nazval spolupráci s NBÚ jako příkladnou a prospěšnou pro obě strany.

SOULAD SE ZÁKONEM

Společnost ČEPS je připravena doložit soulad buď dle § 23 Kontrola, zákona 181/2014 Sb. nebo dle § 29 Prokázání certifikace, vyhlášky 316/214 Sb.

Pan náměstek Šmíd dnes prezentoval, že kontroly NBÚ budou probíhat auditorským způsobem podle ISMS a Správního řádu. Dle vyjádření Jan Šmolíka má společnost ČEPS zkušenost s auditem ISMS a proto neočekává v tomto způsobu doložení souladu problém.

Půjde NBÚ do cloudu?

Aplikace kybernetického zákona znamenala pro řadu organizací a jejich systémů zásadní změny. Tvoří se nová dokumentace, zavádějí nové procesy, a pokud je opravdu velká vůle, dojde i na implementaci nových bezpečnostních technologií. Jedno však zůstalo stále stejné a za to patří tvůrcům zákona a vyhlášek obrovský dík: všechna opatření musí odpovídat vyhodnoceným rizikům. Od začátku jsme se všichni učili, že analýza rizik je základ všeho, a kybernetický zákon toto svaté dogma nemění.

Při tvorbě legislativy se stanovují pravidla a od nich je jen malý krůček k regulaci. Při psaní zákona však jeho tvůrci pracovali přesně podle nejlepších praktik, a proto v žádné související vyhlášce nenajdeme povinnost používat u kritických systémů dvoufaktorovou autentizaci nebo zákaz vyžívání cloudu.

Vydávat regulace je jednoduché a zároveň nebezpečné. Regulace v IT může velmi rychle sklouznout k preferenci určitého řešení, technologie či produktu. Pokud by toto nastalo, tak nepotřebujeme kybernetický zákon. Stačí dát dohromady soupis technologií, které musí osoby povinné implementovat, a svět bude hned bezpečnější. Nicméně by to byla špatná cesta, kterou snad tvůrci zákona neplánovali. Obor kybernetické bezpečnosti je velmi rozmanitý a nabízí na různá rizika celou škálu řešení. Někdo preferuje striktní technologická omezení, jiný se soustředí na procesní a organizační opatření. Obojí je správně, pokud implementovaná úroveň bezpečnosti správně reaguje na zjištěná rizika.

Cloudová řešení jsou dnes velmi diskutovaná, a to nejen v souvislosti s kybernetickým zákonem. Padají otázky, která data mohou být v cloudu a která musí být jenom v nějaké lokální serverovně. Každý, kdo měl tu možnost se detailně seznámit s úrovní bezpečnosti profesionálních cloudových řešení, musí souhlasit, že datová centra předních poskytovatelů nabízí mnohem vyšší procesní, technologickou i fyzickou bezpečnost než drtivá většina státních serveroven českých úřadů.

Která organizace může prohlásit, že má kompletní přehled o umístění svých dat? Skutečně mají všechny státní úřady data jen ve svých „bezpečných" serverovnách? Opravdu se nevyskytují žádná interní data úřadu na noteboocích dodavatelů, v jejich serverovnách, v jejich cloudech? Oponovat, že s dodavatelem má úřad NDA, je zbytečné, protože totéž může mít s poskytovatelem cloudu, a to obvykle s mnohem přísnějšími podmínkami.

Interní data úřadu se také mohou vyskytovat na soukromých noteboocích a tabletech pracovníků zaměstnaných například na DPČ. Ti běžně používají vlastní zařízení, která nejsou téměř pod kontrolou a přitom obsahují různá citlivá data úřadu. Tito lidé mají mnohem více možností a zároveň důvodů tato data dále sdílet než nějaký bezejmenný administrátor komerčního poskytovatele cloudu. Dovolím si s úspěchem pochybovat, že by jakýko-

li kvalitní cloudový poskytovatel dovoloval svým zaměstnancům, aby přistupovali do ostrého prostředí ze soukromých nekontrolovatelných notebooků.

NBÚ nevydal žádné schválení ani neschválení využívání cloudu a doufejme, že se tak nikdy nestane. Kybernetický zákon je dobrý hlavně proto, že nedefinuje bezpečnostní opatření dopředu a nediktuje osobám povinným, jak mají své systémy zabezpečit. Přesně v souladu s nejlepšími praktikami zákon předepisuje, aby si osoba povinná analyzovala všechna relevantní rizika pro své systémy a zvolila optimální opatření na jejich pokrytí. V tomto smyslu se také NBÚ vyjadřuje k otázkám ohledně cloudu. Nemůže se totiž vyjádřit jinak, protože by zpochybnil svůj vlastní zákon.

Jan Mikulecký

Česká pošta
odštěpný závod ICT služby

Jan Mikulecký pracuje jako ředitel odboru bezpečnosti a podpory v odštěpném závodě České pošty. Do jeho odpovědnosti spadá zajištění kompletní bezpečnosti podniku, provoz dohledového centra e-governmentu, interní IT a rozvojové bezpečnostní projekty pro veřejnou správu. Je expertem na řízení informační bezpečnosti, zavádění ISMS a BCMS a provozování bezpečnostních technologií. Má rozsáhlé zkušenosti s definováním bezpečnostních požadavků při zadávání veřejných zakázek a uzavírání smluv. Před nástupem do ČPOZ pracoval 2 roky ve společnosti Deloitte a 12 let v Risk Analysis Consultants jako konzultant pro oblast informační bezpečnosti. Získal doktorský titul Ph.D. ze systémového inženýrství na ČVÚT. Je držitelem certifikací CISM, CRISC a CGEIT. 3 roky byl v Chicagu členem mezinárodní komise pro tvorbu testů CISM – ISACA CISM Test Enhancement Committee. Několik let působil v redakční radě DSM a programovém výboru Information Security Summit. Od roku 2010 je zastupitelem MČ Praha 18 Letňany. Ve volném čase se věnuje primárně rodině a sportu.

IROP se zaměřuje na rozvoj informačních systémů pro veřejnou správu

Jedním z cílů Integrovaného regionálního operačního programu (IROP) za přispění Evropských a strukturálních investičních fondů (ESIF) je dosáhnout vysoké kvality služeb veřejné správy a samosprávy prostřednictvím propojení a sdílení informací a dat, dokončit proces elektronizace agend veřejné správy a zavést úplné elektronické podání pomocí rozvoje služeb nad základními registry. Mezi další klíčové oblasti patří zajištění specifických informačních a komunikačních systémů, včetně zajištění funkční infrastruktury a datových center pro potřeby veřejné správy. V této souvislosti Řídicí orgán IROP vyhlásil již několik průběžných výzev, ve kterých je možné předkládat žádosti o podporu.

Vedle výzev č. 4 Aktivity vedoucí k úplnému elektronickému podání a č. 17 e-Legislativa a e-Sbírka, Národní digitální archiv je možné aktuálně předkládat žádost o podporu ve výzvách:

Výzva č. 10 – Kybernetická bezpečnost

Ve výzvě zaměřené na kybernetickou bezpečnost jsou podporovány projekty zaměřené na zvýšení odolnosti tzv. významných informačních systémů a kritické informační infrastruktury veřejné správy proti kybernetickým hrozbám. V těchto projektech budou podporovány například tyto aktivity: fyzická bezpečnost, nástroje pro ochranu integrity komunikačních sítí, nástroje pro ověřování identity uživatelů, nástroje pro řízení přístupových oprávnění, nástroje pro ochranu před škodlivým kódem, nástroje pro detekci, sběr a vyhodnocení kybernetických bezpečnostních událostí, bezpečnost průmyslových a řídicích systémů apod. Oprávněnými žadateli jsou v tomto případě organizační složky státu a jejich příspěvkové organizace, státní organizace a státní podniky. Dále také kraje a obce (kromě Prahy a jejích částí) a organizace zřizované nebo zakládané kraji nebo obcemi. Žádosti o podporu je možné předkládat do 30. 5. 2017.

Výzva č. 23 a č. 28 – Specifické informační a komunikační systémy a infrastruktura I. a II.

V obou výzvách je možné získat finanční prostředky na rozvoj, modernizaci a zvýšení dostupnosti komunikačních a informačních systémů a infrastruktury, na budování, rozvoj a modernizaci národních datových center a komunikační infrastruktury pro nově pořízené nebo modernizované informační systémy, na vytváření nových informačních systémů v souvislosti s centry sdílených služeb a na vytváření nových a modernizaci stávajících podpůrných informačních systémů. Oprávněnými žadateli jsou u výzvy č. 23 organizační složky státu a jejich příspěvkové organizace, státní organizace, státní podniky a u výzvy č. 28 kraje a obce (kromě Prahy a jejích částí) a organizace zřizované nebo zakládané kraji nebo obcemi. Žádosti o podporu bude možné předkládat do 31. 12. 2017 (výzva č. 23) a 27. 12. 2017 (výzva č. 28).

Výzva č. 26 e-Government I.

Podporované aktivity musí vycházet z jednoho z následujících projektových okruhů implementačního plánu č. 3 Strategického rámce rozvoje veřejné správy: eCulture, eEducation, eHealth, eJustice, sociální služby, pojištění, dávky, výběr daní a pojištění, Elektronická identita nebo Elektronické doručování a ekvivalence dokumentů (eIDAS). Oprávněnými žadateli jsou stejné typy institucí jako u výzvy č. 10.

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

EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

Česká pošta
odštěpný závod ICT služby

PŘEHLED VYBRANÝCH PROJEKTŮ

CMS

vybudování a provoz centrálního místa služeb veřejné správy

ITS

vybudování a provoz integrované telekomunikační sítě resortu MV ČR a složek IZS

KSP

vybudování jednotné úrovně IS, modernizace technologií operačního řízení IZS

NIS IZS

zvýšení úrovně operačního řízení, sjednocení platformy informací OS IZS

ISoSS

informační systém o státní službě

EKIS

nástroj MV při výkonu funkce správce rozpočtových pravidel a účetnictví

DCeGov

vybudování a provoz centrálního provozního a bezpečnostního dohledového centra MV

Česká pošta
odštěpný závod ICT služby

Česká pošta, s. p., Odštěpný závod ICT služby, Olšanská 1951/4, 130 00 Praha 3, tel.: +420 974 841 656, e-mail: spokojenost@cpost.cz, www.CPOZ.cz

Mohou obce pomoci s naplněním vize 202020?

Na začátek připomenu, co vlastně vize 202020 znamená. Zdeněk Zajíček, nový prezident ICT Unie, představil tuto vizi na konferenci ISSS 2016 v Hradci Králové. Byla to reakce nového prezidenta Unie na současnou situaci českého e-governmentu a na jeho vnímání ze strany hodnotitelů, ať už z EU nebo třeba z OSN. Cílem vize je do roku 2020 dostat Českou republiku do první dvacítky zemí z pohledu elektronizace služeb veřejné správy a jejich zpřístupnění občanům.

Aktuální stav e-governmentu

Jak si tedy stojíme? Jak se to vezme. Na centrální úrovni máme funkční a provozem ověřené 3 základní pilíře – základní registry, Informační systém datových schránek a Czech POINT. Dokonce jsme postoupili tak daleko, že některé služby již označujeme „sdílené služby eGov". To znamená, máme hotový backend a k dispozici jsou referenční údaje základních registrů. Rovněž máme systém splňující požadavky eIDAS na garantované elektronické doručování.

K fungujícím částem patří dále subsystém Czech POINTu, známý jako JIP/KAAS. Jedná se o autentizační a autorizační systém pro úředníky orgánů veřejné moci a jimi zřízených organizací. Jeho služby kromě uživatelů Czech POINTu využívá dnes několik desítek agendových informačních systémů a další postupně přibývají. To je jeden z praktických příkladů využití sdílených centrálních služeb. Proč stavět nový autentizační a autorizační systém, když už jeden takový zde je, spolehlivě slouží a prakticky jediným nákladem provozovatele připojeného v AISu je systémový certifikát, pod kterým se k JIP/KAAS daný AIS hlásí (registruje)?.

Jak mohou s naplněním Vize pomoci obce?

Odpověď je prostá. Větším využitím centrálních – sdílených zdrojů a sjednocením nabídky poskytovaných služeb tak, aby se občan snadno orientoval, ať už je na portále v Aši nebo u Jablunkova.

Využití sdílených služeb

Jeden příklad na využití sdílených zdrojů můžete najít např. v Moravskoslezském kraji. V rámci vnitřní integrace úřadu zde byl vybudován lokální jednotný identitní prostor (LJIP), ve kterém jsou spravovány uživatelské účty jak zaměstnanců krajského úřadu, tak externích uživatelů. Přitom je jedno, zda tím externím uživatelem je zaměstnanec některé z obcí kraje, nebo krajem zřizované organizace. Je zde i možnost, aby v LJIP kraje byl účet uživatele například dodavatelské firmy, nebo spolupracujícího subjektu. Lokální JIP totiž zavádí do systému správy uživatelů v rámci kraje koncepci jednotného identitního prostoru Czech POINT. Pro kmenové zaměstnance je autoritativním zdrojem dat personální systém krajského úřadu, pro externí uživatele je využit koncept lokálních administrátorů. Ano, těch lokálních administrátorů, kteří už spravují účty v JIP Czech POINT.

Možná si řeknete: ale takový lokální administrátor pak musí spravovat uživatelské účty v JIP Czech POINT a stejné účty v LJIP kraje. I na tohle koncept lokálního JIP pamatuje, a to synchronizací uživatelských účtů LJIP s JIP Czech POINT. Všechny změny provedené u uživatele na jedné straně jsou automaticky propagovány na druhou stranu. Odpadá tak riziko opomenutí zneplatnění účtu nebo změny přístupových oprávnění apod. Uživatel LJIP tak používá pro přístup do lokálních aplikací stejný uživatelský účet jako pro přístup do centrálních ISVS, ke kterým přistupuje přes JIP/KAAS.

Usnadnit práci uživatelům samosprávních úřadů tím, že jim poskytnete pohodlí jednoho unikátního uživatelského účtu, rozhodně pomůže cílům vize 202020. Uživatel nebude vystaven dále stresu, že si nevzpomene na heslo do x-té aplikace, protože bude používat pouze jedny přístupové údaje. Pro dosažení nepopiratelné odpovědnosti uživatele za provedený úkon v kyberprostoru je pro unikátní uživatelský účet používán v rámci procesu autentizace a autorizace certifikát. Tato podmínka kromě výše uvedeného ukazuje svoji výhodu i době před nástupem eID.

Pokud chtějí obce pomoci s rozvojem e-governmentu v Čechách, mají zde konkrétní vzor. Pouštět se do jakéhokoliv jiného řešení totiž vede zákonitě k izolaci od okolního prostředí a zbytečným výdajům. Řešení správy uživatelů s využitím konceptu LJIP navíc odpovídá referenčním modelům Národního architektonického plánu, který není sice pro samosprávu povinný, ale může být v mnohém užitečný.

Sjednocení nabídky

Každá obec má svůj portál. To je dnes samozřejmost. Samozřejmostí pak také je, že co portál, to originál. Jak se v tom občan má ale vyznat? Neexistuje totiž jednotná forma, jíž obce publikují na svých portálech informace o agendách v přenesené působnosti, které vykonávají za stát a o svých samosprávních agendách. Schválně, podívejte se na dvě libovolná města, Vámi zvolenou agendu nenajdete na stejných místech těchto portálů. Mnohé portály dokonce nemají ani samostatně rozdělené sekce pro občany, podnikatele apod. Chudák občan, který pak hledá a hledá.

Tím, co mě ale trápí více (protože se zabývám uživateli a jejich uživatelskými účty) je nešvar vytváření dalších uživatelských účtů na těchto portálech. V praxi to vypadá třeba takhle: „...je nutno získat přístupové jméno a heslo, které se vydává po vyplnění a ověření žádosti...“

Pokud chce občan služby portálu využívat, nezbývá mu nic jiného, než si takový účet založit – zaregistrovat se. Přitom už několik let je k dispozici možnost využít pro autentizaci občana přihlašovací údaje z ISDS.

Tam, kde dosud státní správa neměla dostatečnou nabídku služeb, aby motivovala občany ke zřízení datových schránek fyzických osob, mohou pomoci obce. A to i v situaci, kdy se blížíme ke stavu, kdy budeme mít k dispozici eID podle eIDAS.

Představte si ten rozdíl. Občan, který komunikuje například se třemi obcemi (protože v jedné bydlí, v druhé má chatu a ve třetí bydlí rodiče), musí mít registrovány hned 3 uživatelské účty! Ale při využití autentizace prostřednictvím přístupových údajů ISDS bude mít pouze jeden. A to ho bude navíc používat pro svůj standardní přístup ke své datové schránce, službám CzechPOINT@home a třeba taky k ePortálu ČSSZ.

Ing. Martin Řehořek vystudoval FSI ČVUT a postgraduální studium v oboru aplikace mikropočítačů v průmyslu.

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

Mohou obce pomoci s naplněním vize 202020?

Odpověď je tedy zřejmá – ano. A dokonce zásadně. Jak jsem uvedl výše, prvním krokem je využití sdílených služeb e-governmentu. Jsou to např. centrální správa uživatelů s využitím konceptu lokální JIP a synchronizací účtů s JIP/KAAS a využití přístupových údajů z ISDS pro autentizaci občanů přistupujících k elektronickým službám obce.

Tím druhým pak sjednocení nabídky elektronických služeb na portálech obcí tak, aby občan našel službu vždy na stejném místě portálu, nezávisle na tom, na portálu které obce právě hledá. Hezkým příkladem sjednocení služeb je portál Podejto.cz. Proč to tedy nezkusit, když pro realizaci lze využít stávající výzvy?

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

NEWPS.CZ

Deklarace eGovernment 202020 pro občany a firmy

V kuloárech elektronizace veřejné správy se již nějakou dobu hovoří o nové iniciativě s názvem 202020. Dohledat podrobnosti o této aktivitě je však stále poněkud nesnadné. Iniciativ 202020 je ve světě několik, například na adrese: 202020vision.com.au/ jsou informace o australské aktivitě, která si klade za cíl do roku 2020 vytvořit obydlené oblasti o 20 % zelenější, než je tomu nyní. Na adrese: 20x20x20.org/ naopak najdeme podrobnosti k charitativní aktivitě na podporu 20 miliónu slepých lidí a za strohým 20-20-20 se skrývá aktivita Evropské unie směřující ke snížení emisí CO_2 do roku 2020 o 20 %. Existuje, respektive je registrována doména 202020.cz, ale zatím bez obsahu. Zajímali jsme se tedy o podrobnosti.

V současné době je téměř ve finální podobě deklarace inicitativy 202020 (celým názvem eGovernment 202020 pro občany a firmy), která upozorňuje na skutečnost, že se ČR nachází na nelichotivých umístěních hodnocení rozvoje e-governmentu (53. místo na žebříčku OSN a 27. na žebříčku EU). Uvedená deklarace v návaznosti na tyto pozice zavazuje její signatáře vyvinout úsilí k tomu, abychom se do roku 2020 posunuli na 20. místo žebříčku OSN. V textu se dále píše, že je za tímto účelem „nezbytné efektivně spolupracovat se soukromým sektorem", veřejná správa musí „transparentně komunikovat s ICT sektorem", je nezbytné zajistit „shodu politické reprezentace napříč politickým spektrem" a na všech úrovních veřejné správy a „důsledně dodržovat ochranu osobních údajů". To jsou ovšem proklamace, pod které by se bezpochyby podepsala řada dosavadních politických elit, přičemž řada z nich je i otevřeně hlásala. Co tedy iniciativa 202020 přináší nového a jaký má potenciál, aby uvedeného stavu (20. místo v žebříčku OSN) pomohla dosáhnout? O tom jsme diskutovali s hlavními protagonisty výzvy, konkrétně Zdeňkem Zajíčkem, prezidentem ICT Unie, Jiřím Běhounkem, hejtmanem Kraje Vysočina a místopředsedou Asociace krajů ČR a Tomášem Prouzou, státním tajemníkem pro evropské záležitosti a koordinátorem digitální agendy.

JAKÉ MÁ INICIATIVA 202020 KONKRÉTNÍ CÍLE?

Hejtman Kraje Vysočina Jiří Běhounek upřesňuje, že tato aktivita není účelově zaměřena na splnění cíle, kterým by měl být posun na ono 20. místo. Jde spíše o podnícení realizace konkrétních kroků a posun na tuto příčku bude pak jejich důsledkem.

Podle prezidenta ICT Unie Zdeňka Zajíčka jsme ve fázi, kdy v rámci veřejné správy máme již silnou infrastrukturu a nyní jsme začali sdílet data. Vývoj, který by měl následovat, tu podle něj už byl, a to v oblasti bank. Z počátku jsme každý chodil výhradně na „svou" pobočku. Když banky začaly sdílet data, mohli jsme chodit na jakoukoli pobočku, ale pořád jsme se museli někam fyzicky dostavit. Teprve internetové bankovnictví bylo krokem, který nám umožnil ovládat své účty a transakce z domova. Podobně jsme tedy podle jeho slov ve veřejné správě nyní ve fázi, kdy máme zkonsolidována data a díky CZECH Pointům jsme schopni poskytovat služby téměř na každé pobočce. Čeká nás tedy poslední krok, a to nabízet on-line služby. V praxi se jedná o vyčištění a konsolidaci dat na robustní infrastruktuře, aby si lidé obsluhovali požadované služby z domova.

Jak Zdeněk Zajíček upozorňuje, nemělo by se přitom jednat pouze o služby státu, ale také pojišťoven, bank, prostě každého, kdo by byl schopen takto on-line svoji službu poskytnout.

Jiří Běhounek je přesvědčen, že řada takových služeb v rámci veřejné správy dnes existuje, nikdo však o jejich nabídce neví, tudíž nejsou využívány. Je přesvědčen o tom, že pokud si takové služby veřejnost vynutila například u bank, musí k tomu dojít i u veřejné správy. Stačí, pokud se občanům existence těchto služeb a možnost jejich využití dá najevo.

Tomáš Prouza k tomu dodává, že takový přístup by umožnil dodržení základních principů, které sleduje Evropská unie:

- **vždy elektronicky** – vše, co lze realizovat elektronicky, by mělo být uskutečněno touto cestou, pouze v případě, že z nějakých důvodů skutečně nelze, teprve pak jsem nucen využít služeb přepážky;
- **pouze jednou** – tj., konkrétní data poskytuji veřejné správě pouze jednou, pak jsou již zanesena do registrů, veřejná správa je má k dispozici a co má k dispozici, nemusím dokládat znovu.

Iniciativa 202020 není zřejmě neuváženým krokem, protože je v úzkém kontaktu jak s MV ČR, tak například s premiérem vlády. Jaká je tedy představa o následujícím postupu?

Zdeněk Zajíček říká, že by právě na základě diskuzí s premiérem, Ministerstvem vnitra a dalšími zainteresovanými rádi iniciovali něco, co by se dalo nazvat poptávkovým řízením, pokud možno na všech úřadech. Tím by se zjistilo, jaké on-line služby ten který úřad poskytuje (nebo se chystá poskytovat) a přitom se o nich v širší veřejnosti neví. Během léta by se tato nabídka služeb měla setřídit a v září by, pod hlavičkou 2020.cz, byla zveřejněna jako ucelená nabídka veřejné správy, samozřejmě s vědomím, že bude postupně doplňována a rozšiřována.

Podle Jiřího Běhounka iniciativa požádala rovněž IT komisi Svazu měst a obcí, aby i ta poslala své nápady, myšlenky a stanoviska a rozšířila tak uvedenou nabídku. Podle něj by platforma iniciativy měla být v tomto směru naprosto otevřená a bez jakýchkoli animozit, aby mohl kdokoli přispět a kdokoli čerpat dle své potřeby.

Nejdůležitější je podle Zdeňka Zajíčka, aby všichni měli pocit, že jsou součástí iniciativy, jen tak může dojít ke spolupráci mezi územní samosprávou, obcemi, kraji a státem na jedné straně, ale také na té nejobecnější úrovni napříč politickým spektrem.

Jak upozorňuje Tomáš Prouza, e-government je nástrojem pro vládnutí, nikoli cíl vládnutí. Důchody se vždycky budou muset vyplácet, žádosti se vždycky budou posílat. Mělo by to být však co nejjednodušší a co nejlevnější. Nástroje, o kterých zde hovoříme, bude chtít používat každá vláda. Měli bychom se nyní na nich domluvit a shodnout tak, aby byly dlouhodobě udržitelné.

Jiří Běhounek doplňuje, že ambicí iniciativy 202020 je vybídnout ke spolupráci všechny strany, které jsou v současné době zastoupeny v Poslanecké sněmovně Parlamentu ČR. Podstatné je informovat strany o celém záměru a vysvětlit, že jde o nabídku služeb, kterou budeme potřebovat všichni, ať jsme z té či oné strany.

eGovernment 202020 pro občany a firmy

PROFILY:

Ing. Tomáš Prouza, MBA
(nar. 30. dubna 1973 Ostrava)

- český ekonom, v letech 2004 až 2007 náměstek ministra financí ČR.
- Od února 2007 do r. 2014 působil ve Světové bance, do října 2012 v Praze jako expert pro oblast finančních služeb, později jako seniorní expert v americkém Washingtonu, D.C.
- Od února 2014 státní tajemník pro evropské záležitosti při Úřadu vlády ČR a koordinátor digitální agendy.
- Člen ČSSD.

Mgr. Zdeněk Zajíček
(nar. 10. května 1967 Praha)

- politik, v 90. letech poslanec Poslanecké sněmovny za ODS.
- V letech 2006–2009 náměstek ministra vnitra (pro informatiku, legislativu veřejnou správu a archivnictví).
- 2009–2010 náměstek ministryně spravedlnosti,
- v letech 2010 až 2013 náměstek ministra financí,
- v březnu 2016 zvolen prezidentem ICT Unie.

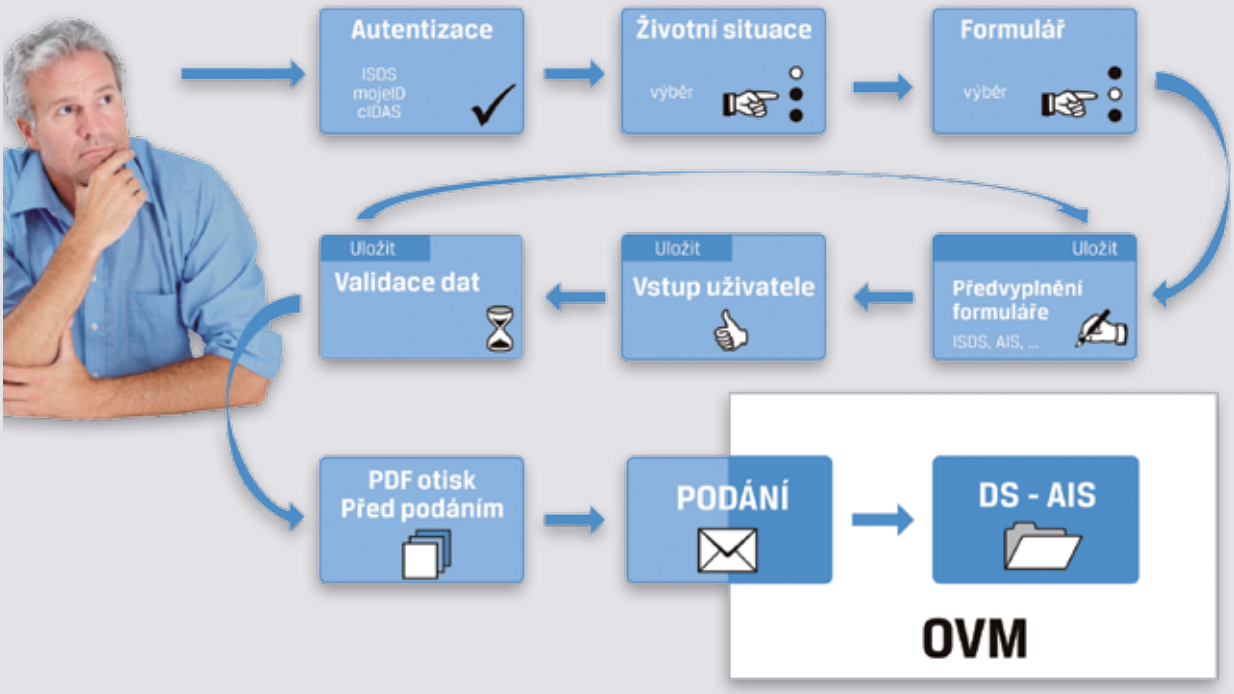
MUDr. Jiří Běhounek
(nar. 13. května 1952 Praha)

- lékař a politik,
- od roku 2008 hejtman Kraje Vysočina.
- Místopředseda Asociace krajů ČR (předseda komise rady AKČR pro informační technologie ve veřejné správě), od října 2013 poslanec Poslanecké sněmovny Parlamentu ČR.

Úplné elektronické podání

V loňském roce byla ukončena realizace* Strategie Smart Administrations, *která představovala vládní strategii na období 2007–2014. Jejím cílem bylo transformovat a zjednodušit postupy používané ve veřejné správě a pomocí finančních prostředků ze strukturálních fondů EU implementovat do veřejné správy moderní ICT nástroje a postupy.

Pro následující období přijala vláda Strategický rámec rozvoje veřejné správy České republiky pro období 2014 – 2020 (dále jen SR). Ačkoli se nejedná o standardní strategický dokument, jsou v něm definovány oblasti a etapy dalšího rozvoje a modernizace VS a e-governmentu. Globálním cílem Strategického rámce je zvýšit kvalitu, efektivitu a transparentnost veřejné správy. Tento cíl bude naplněn prostřednictvím realizace čtyř strategických cílů, které sestávají celkem ze 12 specifických cílů. Jedním ze strategických cílů je zvýšení dostupnosti a transparentnosti veřejné správy prostřednictvím nástrojů e-governmentu. Jeho dosažení je podpořeno realizací projektů spolufinancovaných z operačního programu IROP, z prioritní osy 3 Dobrá správa území a zefektivnění veřejných institucí. Cílem realizovaných projektů je dosáhnout vysoké kvality služeb veřejné správy koordinovaným propojením a sdílením informací a dat veřejné správy. Konkrétně se tak má stát dokončením procesu elektronizace agend VS a zavedením úplného elektronického podání.



Zatím ještě nepříjemná omezení

Již v současnosti legislativa umožňuje tzv. elektronické podání. To znamená, že občan nemusí osobně na úřad, ale vyřídí si agendu prostřednictvím tzv. inteligentního formuláře, který opatří elektronickým podpisem a zašle úřadu. Tento postup však má svá „omezení". Tzv. elektronické podání je totiž dostupné jen těm subjektům, které disponují elektronickým podpisem a/nebo jsou držiteli datových schránek. Současně je možné pouze pro poměrně omezený okruh agend. Nejčastěji se tedy v praxi setkáváme s tzv. neúplným elektronickým podáním, kdy je sice možné (jakýkoli) formulář vyplnit na počítači, ale ten je pak nutné vytisknout a přinést na úřad osobně. Případně je možné jej odeslat elektronicky, ale následně se dostavit na úřad k jeho autorizaci či doplnění. Že nejde o žhavou novinku, ale o v různé míře a kvalitě praktikované řešení, potvrzují i závěry statistického šetření ČSÚ o poskytování on-line služeb obcí a krajů s využitím formulářových řešení. Ze statistik vyplývá, že již v roce 2011 poskytovalo formuláře ke stažení 50,5 % obcí, formuláře k on-line vyplnění 14,3 % obcí a „úplné" elektronické podání umožňovalo 13 % obcí! Pojďme se tedy na pojem úplného elektronického podání (dále jen ÚEP) podívat podrobněji.

Abychom docílili záměrů Strategického rámce, že 85 % podání ze strany občanů vůči úřadům bude podáváno formou ÚEP a zároveň že žadatel nebude muset dokládat údaje vedené v datovém fondu veřejné správy, musí být zaveden tzv. portál subjektu práva (fyzických a právnických osob). Ten bude poskytovat služby typu moje data, moje formuláře, moje datové schránky, moje podání, můj archív. Prostřednictvím portálu, koncipovaného jako samoobslužné místo, bude možné realizovat prvoinstanční úplné elektronické podání pro vybrané agendy a sledovat průběh vyřizování úkonu. K tomu je zapotřebí, aby portál disponoval čtyřmi klíčovými komponentami:

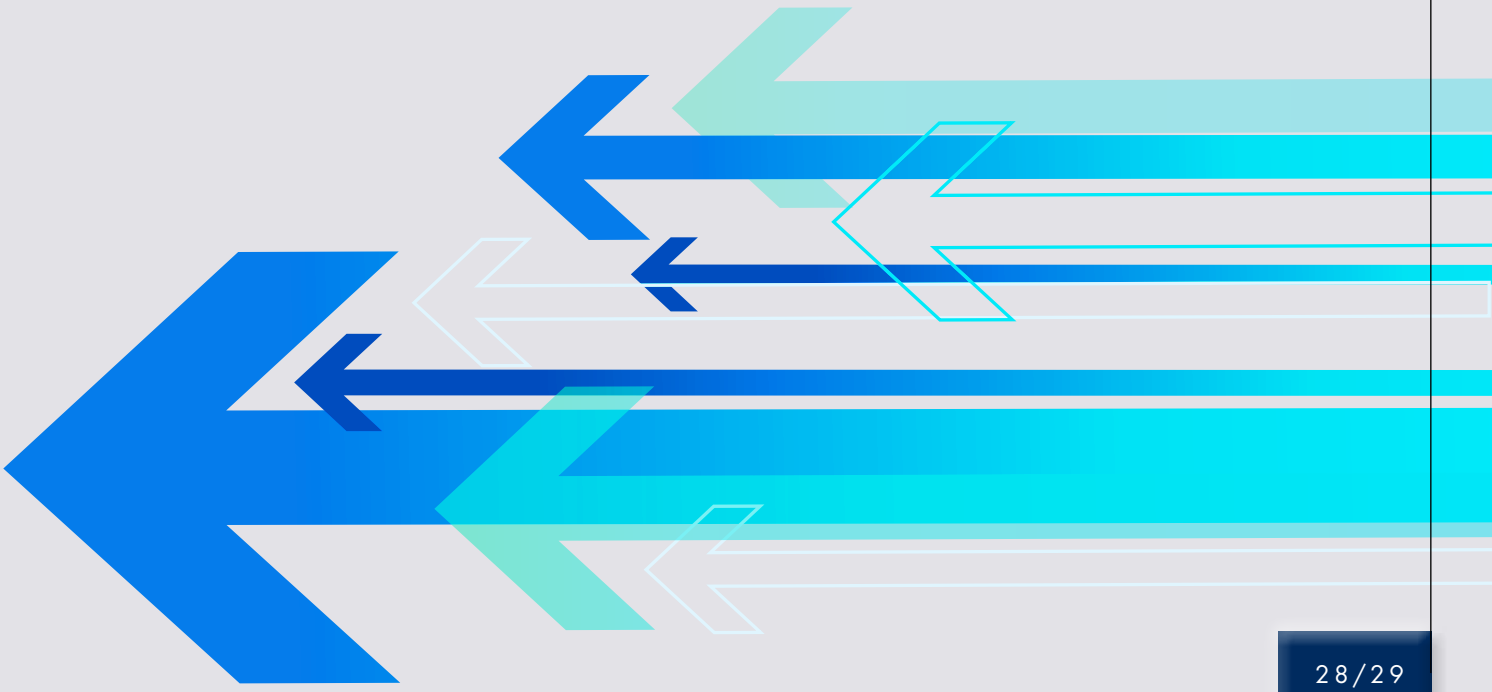
- důvěryhodnou elektronickou identitou;
- elektronickými formuláři;
- propojeným datovým fondem
- a transakčním mechanismem pro elektronické podání.

Užiteční pomocníci

Důvěryhodná elektronická identita zajistí identifikaci a umožní autentizaci subjektu jak na straně žadatele–klienta, tak na straně zpracovatele–úředníka. Na straně uživatele služby/podání se jedná o identitu z ROB/ROS; pro autentizaci lze využít DS, MojeID, eOP či JIP/KAAS.

Elektronický formulář pak vystupuje v roli „uživatelského rozhraní", které zprostředkovává komunikaci mezi klientem a poskytovatelem této služby – subjektem zveřejňujícím formulář. Pro tvorbu elektronických formulářů se nejčastěji využívají tzv. inteligentní formuláře, které jsou uzpůsobeny potřebám jednotlivých agend a pro výkon samosprávních činností i „pravidlům" daného úřadu, která vycházejí např. z obecně závazné vyhlášky. Skutečně inteligentní formulář dokáže klienta-žadatele nejen provázet procesem samotného vyplnění, ale dokáže i automaticky předvyplňovat požadované údaje a validovat jejich správnost. To vše právě díky propojení s datovým fondem VS.

Sdílený datový fond neslouží jen jako zdroj údajů pro předvyplňování formulářů, ale poskytuje i údaje potřebné pro vydání rozhodnutí či autorizovaný výpis. Může se jed-



nat o referenční údaje ze ZR, nereferenční údaje editorů ZR poskytované prostřednictvím tzv. kompozitních služeb, nereferenční údaje AIS publikované na eGON Service Bus (eGSB), či vlastní nereferenční údaje příslušného AIS. Transakční **mechanismy pro elektronické podání** nejsou ničím složitým – většina z nich již existuje a je běžně využívána. Jedná se například o datovou zprávu zaslanou přes ISDS, odeslání elektronicky podepsaného dokumentu e-mailem nebo prostřednictvím asistovaného podání přes úředníka Czech POINTu. Nejméně praktikovaným způsobem pak zůstává přímé vložení autentizovaného uživatele do portálu.

Portál to řeší

Jak je z popisu patrno, faktický rozdíl mezi elektronickým podáním, dnes praktikovaným, a plánovaným ÚEP není příliš velký. Praktický dopad na klienta je však zásadní, a to v pozitivním smyslu. Odpadne nejen místní a věcná příslušnost, ale i neustále se opakující dokládání údajů. Přiznejme si však, že pro realizátory a implementátory řešení může jít, s ohledem na technologickou náročnost takového řešení a na ne zcela připravené legislativní a technické prostředí, o noční můru. Příkladem takového řešení může být portálové řešení HELIOS d.portál, který je společným produktem tří předních dodavatelů ICT řešení – firmy Asseco Solutions, DATRON a Software 602. **HELIOS d.portál** je koncipován v souladu se Strategickým rámcem jako jednotné místo služeb, a to jak z pohledu občana, tak z pohledu úředníka. Jeho nespornou výhodou je také platformní nezávislost a možnost rozšíření o mnoho dalších služeb. Do portálu občana lze integrovat například data a služby zřizovaných a zakládaných organizací, obecní spolky a další občanské aktivity; do portálu úředníka lze zase integrovat vybrané komponenty všeho IS.

Alžběta Křídlová
Produktový manažer
HELIOS

Alžběta se v prostředí veřejné správy pohybuje přes 20 let a má bohaté zkušenosti, jak z pohledu zákazníka, tak z pohledu dodavatele informačního systému. Své zkušenosti zužitkovává zejména při procesních návrzích informačního systému a při analyticko-metodické podpoře ÚSC.

Alžběta Křídlová, produktová manažerka
e-mail: alzbeta.kridlova@assecosol.com
Asseco Solutions, a.s.

Jaromír Látal
Technický ředitel

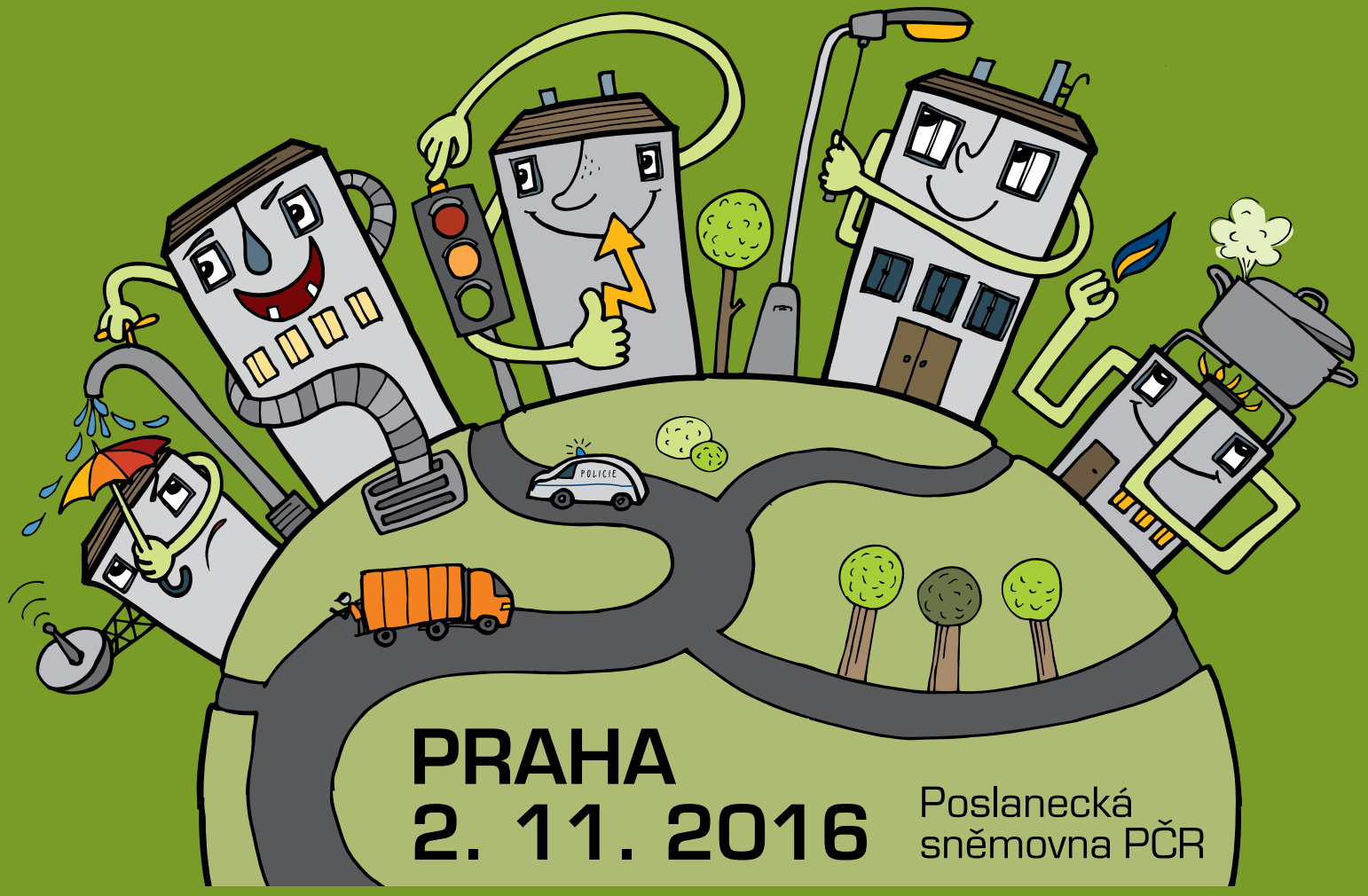
Jaromír má bohaté zkušenosti s řízením ICT projektů v komerční sféře i v oblastech veřejné správy. Přes 15 let působil jako projektový manažer, především pro oblast integrace systémů, správy identit a portálových řešení. Poslední rok řeší obdobné projekty na pozici ředitele technologického oddělení. Zkušenosti z řízení integračních projektů a technologií ICT komerční sféry plně využívá pro obdobné projekty v rámci veřejné správy.

Jaromír Látal, technický ředitel
e-mail: jlatal@datron.cz
DATRON, a.s.

CHYTRÉ MĚSTO

- lepší místo pro život

Egovernment

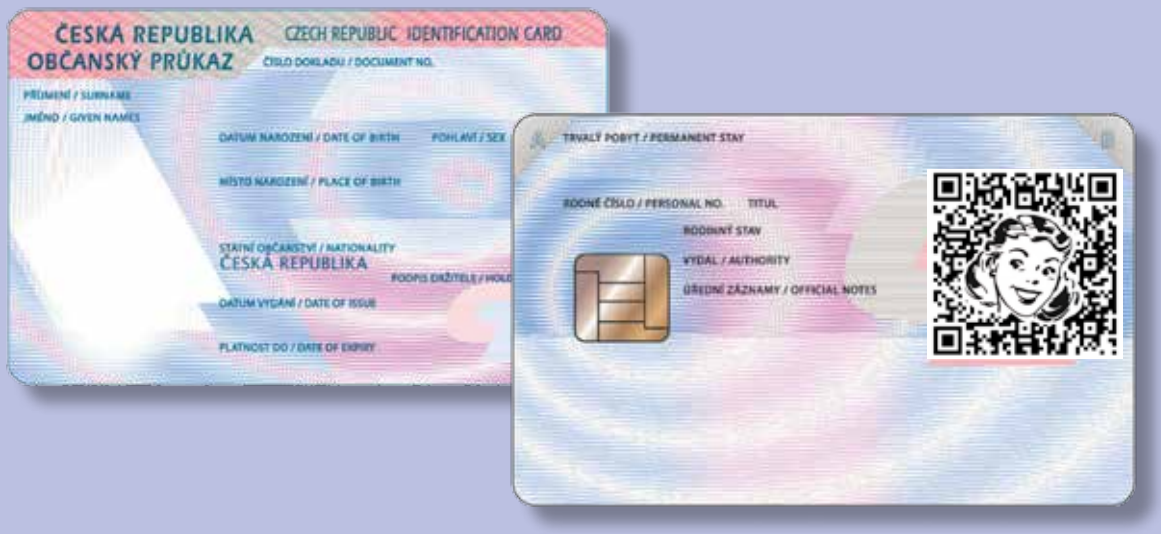


PRAHA
2. 11. 2016

Poslanecká sněmovna PČR

Jak chytrá města ovliňují naše životy?
Jaký vliv má nasazení IT v řízení města
pro větší spokojenost jeho obyvatel,
vyšší efektivitu či lepší životní prostředí?

www.egovernment.cz/chytremesto



eObčanka jako jeden z dalších kroků k modernímu úřadu

V dnešní době, kdy jsme zvyklí na chytrá elektronická zařízení a online služby, jako jsou internetové bankovnictví nebo e-shopy, je přirozené požadovat stejnou dostupnost a kvalitu i od veřejné správy. Právě zmíněné online služby přitom mohou být pro veřejnou správu studnicí zkušeností a vzorů, ze které lze čerpat.

Ministerstvo vnitra se dlouhodobě zabývá modernizací veřejné správy. Všechny nové kroky v této oblasti cílí na zvyšování dostupnosti veřejné správy a posílení komfortu pro občany. Jak takové kroky k modernímu úřadu vypadají, například pokud si půjdete vyřídit výměnu občanského průkazu?

Příklad 1:

Paní Novákové *se blíží konec platnosti občanského průkazu, proto se buď formou SMS zprávy, nebo přes online rezervační systém objedná na konkrétní termín na libovolný obecní úřad obce s rozšířenou působností. Poté se dostaví na vybraný úřad a bez zbytečného čekání přejde přímo k vyřizování. Úředník s ní vyplní žádost a na místě ji vyfotografuje. Paní Nováková si tedy s sebou nemusí brát nic víc než dosud platný průkaz. V případě, že ho nemá, předkládá jiný doklad, který je veřejnou listinou. Výměna průkazu je zdarma. O tom, že je nový průkaz již připraven k vyzvednutí, bude informována prostřednictvím SMS zprávy.*

Zmíněné možnosti zatím fungují v různé míře. Celostátně platí možnost zvolení si libovolného obecního úřadu obce s rozšířenou působností a vyřizování žádosti, včetně vyfotografování, na místě. Využívání ostatních, hlavně tedy technických, prvků obecními úřady je ovšem pozvolnější, i když stále častější.

Online rezervační systémy přitom pro občany obvykle nabízejí tři velmi cenné služby. Za prvé online objednání na konkrétní den a čas, a to zejména pro agendy odborů dopravy a správních agend, tedy hlavně v případech vydávání dokladů a evidence obyvatel a vozidel. Za druhé webový ukazatel aktuálního počtu čekajících osob na vyřízení u jednotlivých přepážek. A za třetí informo-

vání o možnosti vyzvednutí hotového dokladu přes SMS zprávu. Jistě by nebylo od věci i zde rozšířit využívání technologií, například by bylo přívětivé zasílat SMS zprávu nebo e-mail upozorňující na blížící se datum skončení platnosti průkazu, jako je tomu nyní u některých bank v případě konce platnosti platebních karet.

Tyto elektronické pomůcky chce Ministerstvo vnitra rozšířit komplexním systémem elektronické identity, jejímž hlavním nástrojem je elektronický občanský průkaz s čipem, tzv. e-občanka, která v budoucnu, dle aktuálního záměru, nahradí běžné občanské průkazy. Již nyní lze e-občanku pořídit za poplatek, ale dle nového návrhu bude vydávána zdarma, přičemž je snahou rozšířit nabízené funkce.

Cílem je, aby se stala praktickou a uživatelsky přívětivou, jako je dnes platební karta. Pokud občan nebude chtít využívat možnosti e-občanky, bude mít nadále možnost používat ji pouze jako identifikační průkaz, v opačném případě se ovšem uvažuje o nových aplikacích, které bude možné do e-občanky nahrát. Plošné zavedení e-občanky by tedy znamenalo další významný krok v elektronizaci veřejné správy.

Dle aktuálního záměru by se paní Nováková z našeho příkladu s e-občankou dostala do elektronických aplikací veřejné správy (například do elektronické verze pracoviště Czech POINT, Portálu veřejné správy, Daňového portálu, ePortálu) a tím se jí úřady přiblíží doslova na dosah ruky. Díky nahranému identifikačnímu certifikátu získá přístup k výpisům z registrů a vyřídí například daňové přiznání a jiná e-podání. Právě státem garantovaný identifikační certifikát má vytvořit důvěryhodnou elektronickou identitu, která umožní provádění úředních úkonů bez fyzické přítomnosti občana na úřadu.

Příklad 2:

*Ověřený elektronický přístup také může urychlit komunikaci s úřady a dalšími institucemi. Kupříkladu **pan Dvořák** si přes Portál veřejné správy nastaví, že o změně údajů vedených v registru obyvatel budou informovány i jím vybrané instituce (zaměstnavatel, banka, pojišťovny, dodavatelé vody a energií apod.), pan Dvořák přitom může přesně určit, jaké údaje se ta která instituce dozví. Když se tedy v budoucnu přestěhuje a ohlásí změnu trvalého pobytu na ohlašovně, jím vybrané instituce o tom budou zpraveny. Dnes je tato možnost vázaná na zřízení datové schránky. Rovněž další úřady (např. katastrální, finanční, živnostenský) se o změně dozví automaticky ze základních registrů.*

Příklad 3:

*E-občanka také může otevřít online cestu k informativním výpisům z registrů, které jsou nyní podmíněny zřízením datové schránky. Například **pan Malý**, který se dopustil již několika dopravních přestupků, bude moci v rychlosti obdržet výpis z bodového hodnocení řidiče a zjistit přestupky, za něž mu byly v minulosti uděleny body. Obdobně se pan Malý dostane k výpisům i z obchodního, insolvenčního nebo živnostenského rejstříku.*

Jak konkrétně bude technické řešení vypadat, je věcí dalších jednání. Jedno je však jasné již dnes. Naším cílem musí být moderní úřad, který se bude k občanům chovat přívětivě a který jim umožní, aby si maximum úředních záležitostí mohli vyřizovat z tepla domova. Stejně tak, jako se k občanům chovají ty nejlepší internetové aplikace v komerčních službách.

Mgr. Jana Vildumetzová
náměstkyně ministra vnitra
pro řízení sekce veřejné správy

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

OSOBNOST eGOVERNMENTU 2016

Magazín Egovernment připravil pro letošní rok novou soutěž. Po soutěžích zaměřených na projekty (Egovernemnt The Best) a krásné dámy (Miss Egovernment) jsme se tentokrát chtěli věnovat osobnostem, které se výrazně zasloužily o rozvoj elektronizace veřejné správy v ČR. Abychom získali skutečně nezávislé tipy na osobnosti, které si za svůj přístup zaslouží poděkování, požádali jsme o spolupráci naše čtenáře. Ti mohli, prostřednictvím webového formuláře, posílat do redakce své návrhy.

Každý takový návrh byl strukturovaně komentován, aby bylo zřejmé, proč a za co je ta která osobnost do soutěže nominována. Nemuselo se přitom jednat pouze o pracovníky v oblasti IT. Zasloužit se o rozvoj elektronizace veřejné správy je možné nejen realizací konkrétního technického projektu, ale rovněž například návrhem určité normy, zákona či vyhlášky. Rovněž propagace konkrétních projektů či přesvědčování rady města, nebo kraje o vhodnosti takového projektu jsou kroky, které je dobré ocenit. Nominováni tedy mohli být například i vedoucí úřadů či pracovníci tiskového oddělení atp. V rámci nominací bylo rovněž možné určit, do které kategorie soutěžících by měl být nominovaný zařazen. Soutěžilo se konkrétně v eOsobnosti obcí, měst a městských částí, krajů a centrálních úřadů či institucí.

Z nominací, které dorazily do redakce, jsme pak v rámci vnitřního hodnocení (neboť toto je skutečně hodnocení magazínu Egovernment) vybrali v rámci každé kategorie pořadí jednotlivých osobností. Slavnostní vyhlášení výsledků a ocenění eOSOBNOSTÍ EGOVERNMENTU proběhlo v Náchodě dne 2. 6. 2016 v rámci společenského večera konference ROK INFORMATIKY.

eOSOBNOST OBCÍ

V této kategorii jsme asi nejvíce spoléhali na spolupráci čtenářů a doufali v jejich nominace. Přece jen mít přehled o osobnostech všech obcí je trochu komplikované. Bohužel však zde počet nominací značně zaostal za očekáváním, a tak jsme udělili pouze dvě ocenění.

Ocenění této kategorie předávali **David Sláma**, ředitel odboru strategického rozvoje a koordinace veřejné správy MV ČR, který zastupoval náměstkyni ministra vnitra pro řízení sekce veřejné správy **Janu Vildumetzovou**, pod jejíž záštitou se eOSOBNOST EGOVERNMENTU realizovala, a **Vladan Zalejský**, ředitel divize pro veřejnou správu společnosti Asseco Solutions, která byla jedním z partnerů večera.

eOSOBNOST OBCÍ 2016

Lubomír Pospíchal, starosta obce Okrouhlice.

Důvodem jeho nominace a volby byla skutečnost, že se jako starosta obce podílel na technické realizaci řady projektů, významných pro obec (V Okrouhlici plaťte, jak potřebujete, Našim knihám narostly nožičky, SMS informační portál pro občany, online odběr novinek, elektro-

nický i tištěný zpravodaj obce, elektronické podklady rozpočtu pro zastupitele obce, elektronické podklady pro radní atp.). Kromě takovéto technické pomoci byla jedna z nominací formulována i vyloženě obdivně, když hovořila o tom, že pan starosta „umí přepojit PC na podatelně ze záložního zdroje po bouřce během 2 minut tak, aby zase fungovalo".

Na druhém místě v této kategorii

se umístil **Zdeněk Souček**, starosta obce Rudíkov. Jeho nominace byla spojena s projektem on-line informovanosti občanů obce Rudíkov, především za SMS servis, e-mailový servis a facebookový profil obce. Podle nominací se pan starosta výrazně zasloužil o technickou realizaci uvedených projektů, když navrhl a realizoval uvedené projekty.

eOSOBNOST MĚST A MČ

Na rozdíl od předchozí kategorie se u měst a městských částí sešel značný počet nominací, a tak nakonec došlo k tomu, že jsme udělili dvě třetí místa. Ocenění v této kategorii rovněž předávali David Sláma, ředitel odboru strategického rozvoje a koordinace veřejné správy MV ČR, a Vladan Zalejský, ředitel divize pro veřejnou správu společnosti Asseco Solutions.

Na prvním místě v této kategorii se umístil a eOSOBNOSTÍ MĚST A MČ 2016 se stal

Pavel Rous, vedoucí odboru informatiky z Magistrátu města Kladna. Důvodem jeho nominace a ocenění byla dlouholetá podpora a realizace vize integrovaného informačního systému města.

Pavel Rous vedl tým, který projekt IZS realizoval, přišel s návrhem na jeho realizaci, přesvědčoval několik let vedení úřadu o nutnosti této realizace a výrazně prezentoval a propagoval projekt v rámci svých vystoupení, a to ještě předtím, než se funkce IZS staly pilíři státní politiky e-governmentu. Kromě uvedeného technického přístupu byl Pavel Rous rovněž oceněn a navržen za svoje dlouhodobé aktivity v komisi informatiků Svazu měst a obcí ČR.

Druhé místo obsadil

Milan Čigáš, tajemník MÚ Litoměřice.

Ten byl nominován a oceněn především za projekt Potřebuji si vyřídit, tedy návody na webu města, jak řešit životní situace. Milan Čigáš od počátku svého nástupu do funkce

tajemníka úřadu nastavil otevřenou komunikaci jak s kolegy, tak s veřejností a uvedený projekt je jedním z důkazů. Milan Čigáš byl podstatnou součástí týmu, který jej realizoval, prosazoval a výrazně podpořil realizaci projektu a v rámci svých vystoupení jej prezentoval a propagoval.

Jak bylo řečeno, třetí místa v této kategorii byla udělena dvě.

Obě však míří do Děčína a oceněnými jsou **Martin Strnad** z oddělení IT a **Tomáš Kejzlar**, vedoucí odboru informačních technologií, oba z Magistrátu města Děčína. Nominace a ocenění se týká projektu Otevřená data města, kterým Děčín jako první město otevřelo svá data (data.mmdecin.cz), a zároveň projektu Elektronizace služeb statutárního města Děčín. Oba pánové se zasloužili o technickou realizaci a řízení uvedených projektů.

eOSOBNOST KRAJŮ

Ceny v této kategorii předávali za partnera večera, společnost O2 IT services, její generální ředitel **Zdeněk Kaplan** a **David Sláma**, ředitel odboru strategického rozvoje a koordinace veřejné správy MV ČR.

eOSOBNOSTÍ 2016 KRAJŮ se stal

Petr Pavlinec, vedoucí odboru informatiky z Kraje Vysočina. Nominace jeho osoby obsahovaly bohatý výčet aktivit a projektů. Jen stručně – jednalo se například o eMEDOCS, EIDAS, NGA sítě, eDotace, MUZEUM4U, ROWANET, IZS, Portál příspěvkových organizací, Kalendář Kraje Vysočina, Registr sítí, IDM, eAmbulance, Digitální Vysočina, Chytré zásuvky atp.

Hodnoceno bylo rovněž to, že Petr Pavlinec je neúnavným propagátorem řízení kvality organizace, podílel se na koncepci technologických center krajů, organizoval řadu odborných konferencí atp. Kromě uvedeného je Petr Pavlinec jednou z vedoucích postav informatiky v krajích a jedním ze styčných „důstojníků" mezi kraji a ministerstvem vnitra.

Druhou příčku v této kategorii obsadil

Ivo Grüner, náměstek hejtmana Plzeňského kraje, a to především za projekt Digitální mapa veřejné správy Plzeňského kraje. Jedná se o ojedinělé řešení v rámci ČR a nynější iniciativy tohoto projektu přesahují hranici kraje, přičemž mají rovněž výrazný vliv na dění v oblasti geoinformatiky v ČR. Ivo Grüner byl podstatnou součástí týmu, který uvedený projekt realizoval, přesvědčoval vedení úřadu o nutnosti takového projektu a ve svých vystoupeních a jednáních prezentoval a propagoval projekt Digitální mapy veřejné správy. Z časových a pracovních důvodů se náměstek Grüner nemohl večera zúčastnit. Protože se tak stalo na poslední chvíli, nebylo možné zajistit náhradníka, který by za něj ocenění vyzvedl.


Tomáš Kejzlar

Na třetím místě v této kategorii se umístil rovněž vedoucí krajské informatiky, a to

Jan Jelínek, vedoucí odboru informatiky a organizačních věcí Ústeckého kraje. Ten byl nominován za propagaci elektronizace veřejné správy a účast na významných projektech. Ze své pozice se výrazně zasloužil o propagaci elektronizace veřejné správy a patří k hlavním koordinátorům projednávání připomínek krajských informatiků vůči MV ČR. Jan Jelínek byl rovněž pracovně blokován, do Náchoda tedy vyslal své kolegyně Hanu Frýdovou a Lenku Gallovou, které jej zastoupily nejen v dopoledním odborném programu, ale rovněž při večerním přebírání cen.


Petr Pavlinec Zdeněk Kaplan


Hana Frýdová a Lenka Gallová

eOSOBNOST CENTRÁLNÍCH ÚŘADŮ A INSTITUCÍ

Poslední kategorie byla zaměřena na centrální úřady, proto se ceny v jejím rámci předávaly pod záštitou náměstka ministra vnitra pro státní službu RNDr. **Josefa Postráneckého**. Ten byl slavnostnímu večeru přítomen a osobně ocenění předával. Pomáhal mu generální ředitel společnosti O2 IT services **Zdeněk Kaplan**.

eOSOBNOSTÍ CENTRÁLNÍCH ÚŘADŮ–INSTITUCÍ 2016 se stal

Tomáš Holenda z Českého úřadu zeměměřického a katastrálního. Z technického pohledu byl důvodem pro ocenění jeho podíl na projektu Registr územní identifikace, adres a nemovitostí, když se výrazně zasloužil o jeho realizaci a vedl tým, který projekt realizoval. Vedle toho však byl nominován a oceněn pro svoji neskutečnou pracovitost, zapálení pro věc, obětavost, spolupráci s jednotlivci i obcemi a především celoživotní práci ve veřejné správě, a to i na úkor svého vlastního volna.


Tomáš Holenda

Na druhé pozici v této kategorii se umístil

Vladimír Weis z odboru e-governmentu MV ČR.
Zde byl ohodnocen jeho podíl na novele zákona o občanských průkazech, když přesvědčil vedení úřadu o potřebě takové novely, je autorem uvedené zákonné úpravy a v rámci svých aktivit podporoval její vznik a zavedení.

Třetí příčku obsadil

Karel Chod, zástupce ústředního ředitele České správy sociálního zabezpečení, a to za projekt ePortál ČSSZ, když se zasloužil o technickou realizaci projektu, neboť vedl tým, který tento projekt realizoval, a v rámci svých vystoupení jej neúnavně propagoval. ePortál ČSSZ zvyšuje výrazně produktivitu zpracování agendy na straně státu, ale zároveň usnadňuje plnění zákonných povinností veřejnosti. Elektronicky již bylo prostřednictvím portálu realizováno více jak 19,5 milionu podání.


Karel Chod

Takové bylo tedy předávání cen prvního ročníku eOSOBNOST EGOVERNMENTU, které proběhlo v nádherných secesních prostorách divadla v Náchodě. Magazín Egovernment tímto děkuje všem svým čtenářům, kteří posílali nominace a jejich odůvodnění, stejně jako za připomínky pro příští ročník. Budeme se jimi zabývat a již nyní začínáme pracovat na přípravě a detailech dalšího ročníku soutěže eOSOBNOST EGOVERNMENTU 2017.


Josef Postránecký Vladimír Weis

ISSS/V4DIS 2016
19. ročník skončil, přípravy jubilejního 20. začínají

Na devatenáctém ročníku konference ISSS, jenž skončil v královéhradeckém kongresovém centru Aldis v úterý 5. dubna a který již potřinácté doplnila visegrádská konference V4DIS, se jako obvykle sešli politici, vedoucí pracovníci ministerstev, hejtmani, primátoři, šéfové státních organizací, poslanci Parlamentu ČR i hosté ze zahraničí se zástupci veřejné správy, odborníky na informatizaci i dodavateli technologií a služeb do segmentu státní správy a samosprávy. Jedním ze vzácných hostů letošního ročníku byla i komisařka pro spravedlnost, ochranu spotřebitelů a otázky rovnosti pohlaví EK Věra Jourová. Během dvou dnů konference se do registračních knih zapsalo 2372 účastníků, uskutečnilo se přes 200 přednášek a diskusí a ve výstavní části se představila stovka firem a organizací, včetně oficiální delegace několika tchajwanských společností pod hlavičkou Tchajpejské hospodářské a kulturní kanceláře.

„Děkuji organizátorům za pozvání na tuto konferenci, jsem tu už potřetí," prohlásila Věra Jourová během slavnostního zahájení konference. „Poprvé jsem tu byla jako tajemnice městského úřadu, před dvěma lety jako ministryně pro místní rozvoj, kdy jsem si tady pěkně zaslibovala, a nyní. Dnes nebudu nic slibovat a doufám, že vám nezkazím náladu, protože jsem se rozhodla, že tu nebudu dlouze hovořit o tom, co dělá komise v rámci silného tématu, kterým je digitální společný trh, ale budu mluvit – a nemohu jinak – hlavně o otázkách bezpečnosti a o tom, jak je digitální sféra v dnešní době důležitá, zejména proto, aby dokázala čelit hrozbám, které na nás číhají nejenom zvenčí EU, ale bohužel i zevnitř."

Akce se jako obvykle konala pod oficiální záštitou premiéra, místopředsedů obou komor Parlamentu, vicepremiéra, ministra vnitra, několika dalších ministrů a Asociace krajů ČR. Spolupořadatelem mezinárodní části konference byl

Nejsledovanějším bodem programu bylo jako obvykle slavnostní zahájení

Český zavináč 2016 si odnesl Jiří Peterka, publicista, pedagog a radní ČTÚ

Cenu ministra vnitra za dlouhodobý přínos k rozvoji e-governmentu převzal z rukou náměstka Jaroslava Strouhala dlouholetý digitální šampion ČR Ondřej Felix

Kraj Vysočina, který se stal rovněž garantem odborného bloku věnovaného elektronizaci zdravotnictví.

Program konference začal již v neděli vpodvečer seminářem věnovaným nařízení eIDAS ve vztahu k legislativnímu prostředí ČR a poté VIP setkáním v Klicperově divadle. Od pondělního rána pak běžely prezentace, jednání a diskusní setkání až do úterního odpoledne. Mezi tématy dominovalo hodnocení aktuálního stavu e-governmentu, plány pro nejbližší budoucnost, problematika unijního nařízení eIDAS, důvěryhodných elektronických služeb a elektronické identity obecně, otevřená data, informace o nových trendech a technologiích, stejně jako záležitosti spojené s populárním „internetem věcí" a konceptem tzv. „chytrých měst". Nechyběla ani další témata, včetně komunikační infrastruktury veřejné správy, mobilních technologií a sdílených služeb, kybernetické bezpečnosti apod. Stranou nezůstaly ani specifické oblasti, jako třeba veřejné zakázky, elektronizace zdravotnictví a sociálních služeb, e-justice či geoinformační politika státu.

V rámci programu se uskutečnila i řada doprovodných akcí, například setkání Komise pro informatiku SMO ČR, diskuse zástupců akademické sféry s poslanci Parlamentu ČR a odborníky na téma vědy, výzkumu, hodnocení vysokých škol a spolupráce s veřejnou správou, jednání Sdružení tajemníků městských a obecních úřadů či diskusní setkání věnované budoucnosti kongresového turismu v Hradci Králové.

V průběhu konference byly podobně jako v předchozích letech vyhlášeny výsledky populárních soutěží – přehled oceněných lze najít na www.isss.cz.

Hlavním organizátorem konference byla společnost Triada, tradičně se podílel spolek Český zavináč, časopis Obec a finance, firma Ponca a významnou roli při přípravě celkové koncepce hrál i Kraj Vysočina.

Generálním partnerem konference se stala Česká spořitelna, hlavními partnery společnosti Atos, Bureau of Foreign Trade Tchajwan, Cisco, Česká pošta, ICZ a VITA software, hlavním odborným partnerem Microsoft, partnery pak Adastra, Alef, Asseco, Autocont, AV media, Citrix, Comparex, Fujitsu a Gordic. Díky patří i partnerům odborných bloků a spolupracujícím subjektům veřejné správy, mezi nimiž nechybí Ministerstvo vnitra, Ministerstvo pro místní rozvoj, Ministerstvo spravedlnosti, Královéhradecký kraj, město Hradec Králové, fond Regina, ČTÚ, ČÚZK, CZ.NIC, ČIMIB, Deloitte, ICT Unie, NSM cluster, Sdružení tajemníků městských a obecních úřadů či analytický partner konference, společnost IDC CEMA.

Přízemí KC Aldis letos dominovala expozice tchajwanských dodavatelů

Prokop Konopa

MISS EGOVERNMENT 2016

Magazín Egovernment spustil přihlašování do nového ročníku soutěže o nejsympatičtější dámu ve veřejné správě. Jste sympatická a komunikativní, nebo máte kolem sebe takové kolegyně? Stačí vyplnit on-line formulář.

CO JE MISS EGOVERNMENT

Jedná se o soutěž, kterou vyhlašuje magazín Egovernment a která je určena všem sympatickým dámám, které pracují v rámci elektronické veřejné správy. Díky zprovoznění základních registrů je možné tvrdit, že na výkonu elektronické veřejné správy se nyní podílí úplně každý pracovník veřejné správy a proto je i tato soutěž určena všem dámám, které v ní pracují. To znamená, že soutěžit může referentka, tisková mluvčí, vedoucí odboru, obsluha Czech POINTu, starostka, pracovnice spisové služby ... prostě každá dáma, která pracuje ve veřejné správě. Věková hranice není nijak omezena. Stačí, když se jedná o sympatickou, komunikativní dámu.

Soutěž je poděkováním všem, kteří se věnují výkonu elektronické veřejné správy. Zároveň chceme představit sympatické dámy, neboť převážně ony ve veřejné správě pracují, a také trochu navodit příjemnou a zábavnou atmosféru jako poděkování za jejich práci.


2009


2010


2011


2012


2013


2014


2015

Přihlásit se mohou jak přímo samotné dámy, nebo je mohou přihlásit jejich kolegové. Podrobné informace a registrační formulář naleznete na **www.egovernment.cz/miss**

Finále se koná 6. 9. 2016 na zámku Mikulov v rámci společenského večera konference **e-government 20:10, aneb žijem si jak na zámku, ať to trvá věčně** (www.egovernment.cz/mikulov). Vítězku čeká tradičně hodnotná a zajímavá cena.

e-government 20:10 aneb žijem si jak na zámku, ať to trvá věčně

WWW.EGOVERNMENT.CZ/MISS