Egovernment
elektronizace veřejné správy

ELIXÍR pojmů pro veřejnou správu

ODPOČÍTÁVÁNÍ U KONCE

A je to tady. Končí odpočítávání, start je nadohled. Datum 1. 7. 2018 je tak blízko, že větší horko už asi být nemůže. V den, kdy většina z nás sbalí kufry, vypne myšlenky na práci a zařadí se do fronty ostatních turistů lačnících po odpočinku, budou mít na Ministerstvu vnitra hodně napilno. Spustí Portál občana, tedy jakousi elektronickou bránu do veřejné správy. Pravda, nějaký portál tady už máme, seznam životních situací také a návody, jak a kde je řešit jsou dohledatelné. Alespoň, jak slibuje MV ČR, nyní to bude všechno lepší, komplexnější, přehlednější, srozumitelnější a dostupnější.

Pravda, nestane se tak hned 1. 7. 2018. Portál sice bude spuštěn, ale i jak sami pracovníci ministerstva připouštějí, jeho obsah nebude hned tak to rozsáhlý. K dispozici na počátku bude agenda Czech POINT, ČSSZ, některé další formuláře a některé typy trestního oznámení. Rovněž Magistrát hl. m. Prahy údajně připravuje nabídku služeb. K dispozici je e-recept a pravděpodobně, díky Kraji Vysočina, i vstup do Národního kontaktního bodu českého zdravotnictví. Ostatní nabídka bude postupně naskakovat spolu s jednotlivými dlaždicemi obcí, měst, krajů a institucí, které bude možné na Portálu dohledat. V současné době by mělo MV ČR mimo jiné intenzivně komunikovat s těmito subjekty a vysvětlovat i to, jak si mohou samy „svou" dlaždici v rámci Portálu vyvtořit a jejím prostřednictvím šířit nabídku svých služeb.

Stejně tak nebude rychlý nástup požadavků ze strany klientů. Vlastně se tak trochu počítá s tím, že Portál nezahltíme hned v úvodu jeho existence, a to z několika důvodů. Především, jak bylo řečeno, řada z nás bude v době startu projektu řešit spíše dostupnost opalovacího krému s ještě vyšším ochranným faktorem, zmrzliny, která se v tom vedru nerozteče, volného lehátka na beznadějně obsazené pláži, návodu, jak správně vytočit právě zakousnuté klíště či další z roztomilých libůstek, které poskytuje letní dovolená. Prostě na nějaký Portál v tu dobu ani nevzpomeneme. Dalším důvodem je skutečnost, že k portálu, pokud budeme chtít doopravdy něco vyřizovat, bude možné a vhodné se přihlásit – identifikovat. A to buď prostřednictvím datové schránky, ale tu nemáme všichni, anebo prostřednictvím elektronického občanského průkazu s čipem (eOP) a ten nemá nikdo z nás. Ten se začne vydávat rovněž 1. 7. 2018. Respektive, protože to je neděle, tak první žádost o vydání elektronické občanky můžete podat 2. 7. 2018. A tak bude skutečně chvilku trvat, než skončí léto, my se opálení i dopálení vrátíme zpět, zařídíme čipové doklady a mezi tím, doufejme, bude Portál naplněn obsahově i odladěn funkcionálně.

O stavu Portálu Vám budeme referovat na první poprázdninové konferenci e-government 20:10 v Mikulově. Do té doby si uvnitř tohoto čísla můžete přečíst poslední předstartovní informace o Portálu i eObčance, ale rovněž najdete rozhovor o nutnosti úpravy legislativy, bez níž nebude elektronizace tou elektronizací, která by nám skutečně život usnadňovala. Zamyslíme se také nad elektronickou identitou a nabídneme pohled na takové evergreeny, jakými je kyberbezpečnost či GDPR.

Hezké léto,

Ing. Michal Jirkovský
šéfredaktor

Obsah

V rámci České a Slovenské republiky vydává:

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

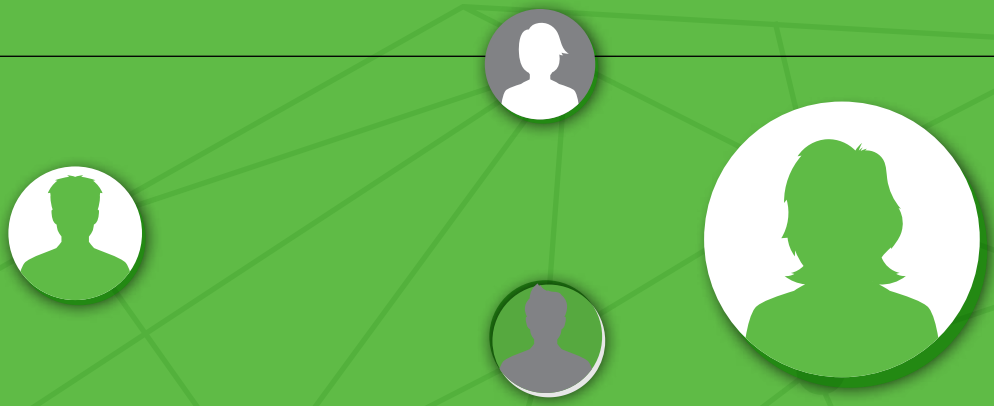
Šéfredaktor: Ing. Michal Jirkovský
Korektorka: PhDr. Helena Veverková
Asistentka: Patricie Stránská

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

ISSN 1801-9420

Registrace:

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



Šetříme váš čas

Spuštění e-občanky a Portálu občana se blíží. „Bude to začátek nové éry elektronizace veřejné správy," říká ředitel odboru e-governmentu ministerstva vnitra Roman Vrba, kterého jsme požádali o rozhovor chvíli před startem projektu.

Termín spuštění e-občanek a Portálu občana se blíží. Co máme čekat?

Rozhodně nečekejte webovou stránku. Portál občana je prostředí. Je to na jednom místě celá architektura služeb veřejné správy pro občany. Využijeme přitom všechno to, co jsme dosud budovali. Ke správné funkčnosti Portálu potřebujeme Centrální místo služeb, Informační systém základních registrů, eGSB a další systémy. A aby systém dobře fungoval, potřebovali jsme ještě poslední kamínek, kterým je elektronická identita. V našem případě zastoupená elektronickou občankou.

Jak jsme vlastně daleko v elektronizaci veřejné správy?

Možná Vás to překvapí, ale jsme vlastně úplně na začátku. Na začátku nové éry, kdy jsme zaměřeni na občana. Po letech obrovské práce a také velkých investic, kdy jsme budovali tzv. back-end, teprve teď můžeme ukázat občanům, k čemu všemu to bylo dobré. A když už jsme postavili ve front-endu například datové schránky, situace se obrátila tak, že je používají především úřady k posílání dopisů mezi sebou, nebo podnikatelé, kteří je mají povinně. V tomto smyslu jsme opravdu na začátku.

A jaký je cíl všeho toho počínání?

Ten cíl je jednoznačný. Poskytovat služby z jednoho místa, z Portálu veřejné správy – **gov.cz**. Přes tento portál bude moct občan komunikovat s celou veřejnou správou, ale najde tam i návod, jak se vyznat ve spleti úřadů. To uděláme tak, že na Portálu budou lépe popsány jednotlivé životní události.

Existuje nějaký vzor, nějaký stát, který to někde ve světě dělá tak, že bychom chtěli mít e-government postavený stejně?

To asi ne. Spíš si vybíráme od každého něco. V něčem je například hrozně daleko Jižní Korea nebo Dánsko. Elektronické služby státu jsou nejdále ve Velké Británii.

Víte vlastně, co občan od státu potřebuje? Kde byste mu nejvíc elektronizací mohli pomoct?

Podle mého soudu chce občan stát, který ho co nejméně obtěžuje. A když už ho obtěžuje, tak aby se obyčejný člověk měl šanci vyznat v tom, co po něm vlastně stát chce. Problémem je u nás teď nepřehledná legislativa.
Občané, kteří nejsou podnikatelé, se státem vlastně moc komunikovat nemusí. Když už, tak je to daňové přiznání. Nebo různé podpory z resortu práce a sociálních věcí. Tam je samozřejmě mírnou komplikací to, že například elektronizovanou sociální oblast využijí nejméně ti, kteří ji nejvíce potřebují. Senioři budou zřejmě vždy o trochu méně vstřícní vůči moderním elektronickým nástrojům.

Všechno se dá měřit. I to, kolik se uspoří, když budou lidé využívat elektronické nástroje. Jak to vychází?

Ano, měřit můžeme vše. A to nejen penězi, což by se nabízelo. Interně jsme například počítali efekt zavedení CzechPOINTů. Od roku 2007, kdy byl tento systém spuštěn, jsme vydali už téměř dvacet milionů výpisů. Když se tato suma přepočte na čas, který by museli lidé strávit někde na cestách vyřídit potřebný výpis na konkrétní úřad, dostali jsme se k číslu, že jsme ušetřili celkově čas stejný jako 30 lidských životů. V případě úřadů, představte si, kolik ubylo papírování, když se posílají dopisy elektronicky datovou schránkou. My tomu v nadsázce říkáme: *„Pošli datovku, zachraň strom."*

Jakub Knězů, MV ČR

18x O eOBČANCE A PORTÁLU VEŘEJNÉ SPRÁVY

1. Kde a kdy si můžu zažádat o eObčanku?

Občanský průkaz s čipem, který nově umožňuje zaručené prokazování totožnosti při využívání online služeb veřejné správy, získá automaticky každý, kdo po 1. 7. 2018 požádá o standardní občanský průkaz na pracovišti osobních dokladů na jakémkoliv úřadu obce s rozšířenou působností (příp. Úřadu městské části Praha 1–22).

2. Mohu si eObčanku vyřídit online?

Pokud digitalizovaná podoba občana nebo jeho podpisu jsou vedeny v evidenci občanských průkazů nebo v evidenci cestovních dokladů a od vydání dokladu, pro jehož účel byly pořízeny, neuplynula doba delší než 1 rok, nedošlo k podstatné změně podoby, lze žádost podat obecnímu úřadu obce s rozšířenou působností i v elektronické podobě na formuláři stanoveném ministerstvem. Tato žádost se zasílá obecnímu úřadu obce s rozšířenou působností na stanoveném formuláři prostřednictvím datové schránky; není-li doručena prostřednictvím datové schránky, musí být opatřena uznávaným elektronickým podpisem.

3. Kolik stojí vyřízení eObčanky?

V případě konce platnosti OP do půl roku, nebo změně ze zákona zapsaných údajů je to zdarma.

- Výměna před ukončením doby platnosti bez zákonných důvodů: 200 Kč (nad 70 let zdarma).
- Výměna při ztrátě, odcizení nebo poškození: 100 Kč.
- Vydání do 24 hodin (pracovní dny): 1000 Kč/do 15 let 500 Kč (převzetí na MV, podání žádosti na MV nebo na obecním úřadě ORP).
- Vydání do 5 pracovních dnů: 500 Kč/do 15 let 300 Kč (podání na MV nebo obecním úřadě ORP, převzetí na MV nebo na stejném obecním úřadě, jako byla podána žádost).

4. Jak rychle mohu získat eObčanku?

Standardní lhůta pro vydání je 30 dnů, za poplatek lze zažádat o vydání ve zkrácené lhůtě do 5 pracovních dnů nebo do 24 hodin (v pracovní dny).

5. Co si mohu nově s pomocí eObčanky vyřídit?

Kromě všech standardních funkcí, spojených s osobním prokazováním totožnosti, lze aktivovaný OP používat pro prokazování totožnosti při využívání online služeb veřejné správy, dále lze použít jako nosič kvalifikovaných a autentizačních certifikátů a používat např. pro podepisování elektronických dokumentů.

6. Jaké jsou výhody eObčanky?

Funguje jako identitní prostředek na nejvyšší úrovni záruk (LoA), není už nutné pamatovat si desítky přístupových údajů k jednotlivým službám veřejné správy, může sloužit jako nosič kvalifikovaných a autentizačních certifikátů, není nutné pořizovat další nosič (čipovou kartu, token).

7. Jaká jsou rizika eObčanky a Portálu veřejné správy? Nemůže mi někdo data ukrást?

Největší riziko je vždy spojeno s chováním uživatele. Údaje, které obsahuje identifikační certifikát, jsou chráněny identifikačním osobním kódem, který by měl znát pouze jeho držitel. Přístup na Portál občana je opět spojen se zadáváním přístupových údajů, data zde zobrazovaná jsou vždy načítána z informačních systémů veřejné správy po přihlášení uživatele, žádnou vlastní databázi portál nevytváří a nedrží.

8. Musím si svůj OP vyměnit za eObčanku?

Ne, občanské průkazy vydávané před 1. 7. 2018 budou i nadále platné až do skončení doby jejich platnosti, plošná výměna probíhat nebude.

9. Jak funguje čip na eObčance?

V zásadě jako jakýkoliv jiný kontaktní elektronický čip. Z výroby je v něm uložen identifikační certifikát, který nelze z čipu vyjmout, nahradit nebo smazat. Aby bylo možné funkce čipu používat, je nutné čip aktivovat (na pobočce obce s rozšířenou působností zadáním IOK a DOK). V případě nutnosti je možné čip deaktivovat. Deaktivovaný čip nelze znovu aktivovat, je nutné požádat o nový občanský průkaz. Do části čipu lze nahrávat vlastní elektronické podpisy, kvalifikované a autentizační certifikáty. Přímo s čipem komunikuje prostřednictvím čteč-

ky obslužná aplikace „eObčanka – identifikace“, která odesílá výsledky ověření přístupovými kódu systému, který zprostředkovává ověření totožnosti (Národní bod pro identifikaci a autentizaci). Aplikace pak provází uživatele procesem ověřování identity.

10. Potřebuji speciální zařízení ke svému počítači, abych mohl používat eObčanku v online styku s úřady?

Některé notebooky nebo klávesnice už v sobě mají zabudované čtečky čipových karet (Smart card). Pokud uživatel nemá zařízení s integrovanou čtečkou, musí si pořídit externí čtečku, kterou lze připojit pomocí konektoru (USB, PCMCIA) nebo bezdrátově (buetooth). Čtečky by měly splňovat základní parametry – soulad s normou ISO 7816, CCID (Chip Card Interface Device), kompatibilita s operačním systémem PC, na kterém má být čtečka používána.

11. Proč potřebuji čtečku k použití eObčanky?

Čtečka musí přečíst informace uložené na čipu a předat je do zařízení, na kterém uživatel pracuje.

12. Kde seženu čtečku k použití eObčanky?

Téměř v každém obchodě s elektronikou nebo u poskytovatelů služeb vytvářejících důvěru (kvalifikované elektronické podpisy apod.) jsou dostupné různé varianty od mnoha výrobců.

13. Kolik stojí čtečka k použití eObčanky?

Nejlevnější čtečky pro připojení přes USB začínají už pod 200 Kč. Čtečky s vlastní klávesnicí nebo pro připojení prostřednictvím bluetooth jsou násobně dražší.

14. Dá se eObčanka využít i pro osobní identifikaci a komunikaci s úřady v rámci EU?

Toto bude možné v okamžiku notifikace Národního identitního systému v EU, předpokládáme to do dvou let.

15. Mohu cestovat na eObčanku?

eObčanka má všechny funkce jako dosavadní občanský průkaz, tudíž ji lze použít jako cestovní doklad v rámci EU.

16. Kam mám zavolat v případě, že potřebuji asistenci s použitím eObčanky?

Help desk +420 225 514 777 Správy základních registrů (stejné číslo pro deaktivaci čipu) poskytuje základní uživatelské informace a podporu při řešení problémů (kontaktovat lze i emailem), kompletní návody a popisy jsou na info.eidentita.cz/eOP. V případě problémů lze odeslat report přímo z obslužné aplikace eObčanka.

17. K čemu slouží elektronická identita občana?

Pro vzdálené prokazování totožnosti při využívání online služeb veřejné správy. Základ elektronické identity občana je v podobě údajů uložených v základním registru obyvatel. Občan si zvolí prostředek, kterým se chce identifikovat (např. eOP), musí jít ale o tzv. kvalifikovaného správce – poskytovatele identitních prostředků – který získal akreditaci ministerstva vnitra a je napojen na Národní bod pro identifikaci a autentizaci.

18. Co to je Národní identitní autorita?

Zákon o elektronické identifikaci definuje Národní bod pro identifikaci a autentizaci jako informační systém, který zajišťuje zprostředkování elektronické identifikace mezi poskytovateli prostředků, kterými uživatel prokazuje svoji identitu, a poskytovateli online služeb, a to včetně napojení na další ohlášené systémy v rámci EU pomocí mezinárodního uzlu. Národní bod je součástí širší technologické platformy Národní identitní autority, která v sobě zahrnuje další součásti navázané na proces elektronické identifikace, jako jsou státem poskytované prostředky pro samotnou elektronickou identifikaci nebo nástroje pro správu vlastního identitního účtu uživatele. Veřejným rozhraním **Národní identitní autority** pro přístup uživatelů a poskytovatelů online služeb bude portál **eIdentita.cz**.

Pavel Novák, MV ČR

2018

Pojeďte s námi za e-GOVERNMENTEM

4.–5. 9.

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

8. – 9. 11.

Setkání informatiků
PLZEŇ

19. 11.

Egovernment The Best 2018
PRAHA

Více na: **www.egovernment.cz**

Kde je vůle, tam je cesta!

Současný prezident ICT Unie Zdeněk Zajíček za sebou má dlouhou cestu českým eGovernmentem. Jeho vzdělání a praktická znalost chodu úřadů různého typu z něj pak dělá odborníka, který, když hovoří o potřebě úpravy legislativy, zřejmě nemluví jen o kosmetických změnách. Nejen jeho zvolení do čela výboru pro digitálně přívětivou legislativu pod RVIS pro nás tedy bylo vhodnou záminkou pro tento rozhovor.

Nedávno jste byl jmenován do vedení Stálého pracovního výboru pro digitálně přívětivou legislativu RVIS. Co si máme pod pojmem digitálně přívětivá legislativa představit?

Od prvopočátku procesu digitalizace jsme vždy upozorňovali na zásadní význam legislativy. Digitálně přívětivá legislativa je proto jedním ze základních pilířů digitalizace a zjednodušeně lze říct, že se jedná o takové zákony a podzákonné normy, které nebudou bránit využívání moderních technologií v úřadování. Občanů, kteří jsou zvyklí vyřizovat si své potřeby přes internet prostřednictvím počítačů, mobilních zařízení či chytrých telefonů, přibývá a naší povinností je jim takovou službu nabídnout. Digitální gramotnost je u nás vysoká, když se podíváte, kolik z nás využívá internetové bankovnictví, pojišťuje se on-line, nakupuje přes internet, sleduje IPTV, komunikuje na sociálních sítích. Když to sečtu, tak je tady odhadem kolem 4 milionů lidí, kteří ve svém životě aktivně používají digitální technologie k vyřízení svých záležitostí. Bohužel zatím jen velmi málo v komunikaci s veřejnou správou.

Proč je z Vašeho pohledu tak důležitá právě legislativa? Nemyslíte si, že více energie by se mělo věnovat hlavně eGovernmentu?

Veřejná správa může dělat jen to, co jí ukládají zákony. Takže když potřebuje nějaký úřad vybudovat svůj informační systém, musí mu to konkrétní zákon uložit. Nebo chceme-li sdílet jednou pořízená data, opět to musíme mít v zákoně. Legislativa je tedy pro eGovernment zcela zásadní. Bohužel dodnes si řada tvůrců legislativních návrhů neuvědomuje význam tohoto principu, zejména právě v oblasti digitalizace, kde dopady jakékoliv změny je třeba promítnout do celého legislativního rámce ve vzájemných vazbách a přetrvávající překážky také odstranit. A to je to, co nás stále významně limituje. Český právní řád stále ještě neobsahuje některé základní principy eGovernmentu jako například sdílené služby a zároveň řada zákonů stále ještě obsahuje ustanovení, která neumožňují digitalizaci.

Jaké jsou úkoly tohoto stálého výboru a na co se chcete nejvíc zaměřit?

Naše cíle bych rozdělil do dvou částí. Krátkodobé cíle vidíme v podpoře co nejrychlejšího prosazení zákona o právu občanů a firem na poskytnutí digitálních služeb a novelizaci těch zákonů, které jsou pro úspěšnější digitalizaci zcela zásadní. Jedná se o zákony definující rámec českého eGovernmentu jako např. zákon o základních registrech, zákon o informačních systémech veřejné správy nebo zákon o elektronických úkonech a autorizované konverzi. Potřebujeme co nejrychleji dotvořit právní rámec pro naplnění všech devíti evropských principů digitalizace, ale zejména pro povinné sdílení dat, preferenci digitální formy výkonu agend, využívání sdílených služeb, cloudové služby, atd.

Dlouhodobě jsou naše cíle dva. Prvním je snaha průběžně iniciovat změny stávající legislativy, která stále ještě není digitálně přívětivá a brání efektivnější digitalizaci. Druhým, neméně důležitým, je příprava a prosazení rozšíření hodnocení dopadů regulace tzv. RIA nově i o zhodnocení souladu legislativních návrhů s cíli a principy digitalizace. Tedy, že předložený legislativní návrh je digitálně přívětivý. Již v loňském roce jsme se podíleli na přípravě rozšíření hodnocení dopadů regulace RIA o posouzení souladu návrhů s principy digitalizace. Minulá vláda však odmítla začlenění přímo do RIA a naše návrhy tak byly prozatím promítnuty pouze do doporučených zásad pro digitálně přívětivou legislativu.

Jaké je složení stálého výboru? Měl jste třeba možnost i některé své odborníky do výboru nominovat?

Stálý výbor je složen z odborníků s dlouholetými praktickými zkušenostmi s digitalizací veřejné správy. Jedná se o odborníky z veřejné správy, komerční i akademické sféry. Ano, měl jsem možnost většinu kandidátů i sám navrhnout, za což jsem velmi rád, protože i tímto krokem bude zajištěna kontinuita v boji za digitálně přívětivou legislativu a digitalizaci.

Je zajímavé, že jste se do této funkce dostal jako prezident ICT Unie. Jak si vysvětluje tento krok vedení RVIS?

Možná je to trochu tím, že mám určité zkušenosti v otázkách digitalizace a hlavně problémech s tvorbou legislativního rámce. Ale nemyslím si, že tento předpoklad je tím nejsilnějším důvodem. Hlavním důvodem je změna přístupu na straně státu. Po několika posledních letech stagnace v oblasti eGovernmentu, která byla způsobena mimo jiné i neochotou spolupracovat se soukromým sektorem, se dnes tato situace zásadně mění. Pro stávající politickou reprezentaci se opět po několika letech oblast digitalizace stává jednou z velmi významných priorit a pomalu se snaží napravit předchozí nedostatky zejména v komunikaci mezi veřejným a soukromým sektorem. Velmi pozitivně vnímám zájem a podporu napříč politickým spektrem ze strany vrcholných představitelů politických stran zastoupených v parlamentu, vlády v čele s premiérem a na denní bázi ze strany zmocněnce vlády pro informační technologie a digitalizaci Vladimíra Dzurilly. Jsem potěšen, že můžu s takto odborně kvalifikovaným, manažersky zkušeným a komunikačně zdatným člověkem spolupracovat. Od jeho nástupu do funkce sleduji velkou snahu změnit celý systém řízení oblasti ICT ve veřejné správě a aktivní snahu vrátit Českou republiku zpět na přední místa v mezinárodním měřítku. Věřím, že společně jsme schopni dosáhnout náš deklarovaný cíl, a to do konce roku 2020 skočit v oblasti eGovernmentu mezi prvních 20 států na světě (202020.cz). ICT Unie je jako největší profesní sdružení, zastupující více než 70 největších a nejúspěšnějších obchodních společností, které nabízejí své služby a produkty v oblasti ICT, připravena v tomto směru maximálně pomoci.

To jsou pozitivní informace. Ale já vím, že ICT Unie zřejmě nečekala takovou změnu a že sama již několik měsíců aktivně připravuje své vlastní legislativní návrhy. Můžete popsat, o jaké snahy jde, co je jejich cílem a také jak tyto aktivity chcete prosazovat?

Ano, je to pravda. ICTU byla iniciátorem vzniku právě Iniciativy 202020, jejímž cílem bylo napomoci ke zlepšení mezinárodního hodnocení České republiky v rámci posuzování indexu EGDI (OSN), ale i evropského indexu DESI. V minulém volebním období ICT Unie sama a de facto bez skutečné podpory odpovědných úřadů, s výjimkou Úřadu vlády a některých poslanců a senátorů, provedla identifikaci a ověření funkčností všech existujících digitálních služeb veřejné správy. Takto jsme identifikovali více než 700 digitálních služeb, ověřili jsme jejich funkčnost, přístupnost pro občany a další atributy každé služby. Následně jsme navrhli jejich klasifikaci a rozdělení do čtyř kategorií. Podle našeho návrhu následně VŠE, dle zadání Úřadu vlády, provedla v rámci projektu financovaného Technologickou agenturou ČR rozdělení digitálních služeb do jednotlivých kategorií dle klasifikace. Všechny takto získané, ověřené a verifikované informace o každé digitální služ-

bě jsme souhrně předali odpovědným úřadům k optimalizaci a standardizaci. Celá tato aktivita byla financována výhradně ICT Unií. Ani přes tuto negativní zkušenost jsme v ICT Unii nerezignovali na další snahu pomoci státu zlepšit stav digitalizace, ale zaměřili jsme se na to, co podle našeho názoru může skutečně skokově a relativně rychle zlepšit reálné podmínky života našich občanů. A tím je právě digitálně přívětivá legislativa jako nástroj k další digitalizaci společnosti. Naši aktivitu označujeme jako legislativní balíček. Naší snahou bylo identifikovat zákony, které nejvíce brání efektivnější digitalizaci a připravit nápravu. Zpracovaný legislativní balíček není jen návrhem ICT Unie, ale také dalších devíti partnerů, a to Hospodářská komory ČR, Svazu průmyslu a dopravy ČR, Sdružení pro internetovou reklamu, Asociace poskytovatelů mobilních sítí, Česká asociace elektronických komunikací, České bankovní asociace, České asociace pojišťoven, CACIO a CZ. NIC. Společná diskuze zainteresovaných nás postupně přivedla k tomu, že jen změna vybraných zákonů nestačí. I díky zahraniční inspiraci jsme dospěli k názoru, že skutečnou změnu přinese posílení práv občanů na digitální služby zvláštním zákonem. Tento návrh je finalizován a předpokládám jeho brzké předložení do diskuze s jednotlivými parlamentními stranami. Průběžně je tento návrh také konzultován se zmocněncem vlády pro informační technologie a digitalizaci, Digitálním šampionem ČR a dalšími reprezentanty eGovernmentu.

V tomto směru je potřeba zdůraznit, že snahou je posílit práva těch občanů, kteří chtějí komunikovat digitálně. Pro ty, kteří digitalizaci nepreferují, budou samozřejmě zachována fyzická forma nebo asistovaná forma komunikace.

Myslíte si, že se tedy v digitalizaci opravdu blýská na lepší časy?

Já v to opravdu věřím. Víme totiž, že k tomu abychom se opět dostali na evropskou špičku v digitalizaci nepotřebujeme mnoho. Často od politiků slýchám otázku, proč nejsme jako v Estonsku? A já na to vždy odpovídám. Nechybí nám toho moc. Česká veřejná správa má technologicky i procesně jedinečný systém centrálně sdílených služeb, který nemají takto komplexně vybudovány nikde jinde na světě. Czech POINTy, Datové schránky a Základní registry nám závidí i státy, které jsou v hodnoceních před námi. My bohužel tyto nástroje pro sdílení dat, státem garantovaný doručovací kanál a univerzální podací, ověřovací a informační místo neumíme plnohodnotně využívat. Občané a firmy by už dávno nemuseli některé úkony činit a stát by je mohl dělat za ně. Bohužel nám někdy chybí odvaha a někdy správná zákonná úprava. Proto přicházíme se zákonem o právu na poskytnutí digitálních služeb, protože ten teprve vytvoří správný tlak na stát, aby nám digitálně sloužil.

Nezastírám, že nás čeká velmi složité a náročné období. Nejen že musíme legislativní balíček dokončit, ale hlavně musíme přesvědčit o správnosti naší cesty většinu politiků a veřejnost. A víme, že naše návrhy budou zpočátku narážet na odpor těch, kteří chtějí úřadovat postaru a papírově.

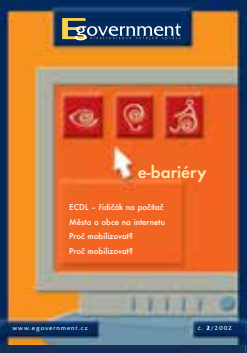
A máte časovou představu, kdy by bylo potřeba prosadit tyto změny?

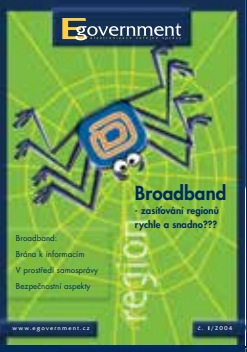
Ano. Jsme přesvědčeni, že je nezbytné uvedené legislativní změny prosadit v Poslanecké sněmovně ještě do konce tohoto roku, aby bylo možné zajistit jejich účinnost nejpozději v polovině příštího roku, tedy téměř v polovině mandátu této Poslanecké sněmovny. Pak je šance, že u nás dojde ke skutečné digitální revoluci a začnou od nás „opisovat" i jiné státy na světě. Není důvod se podceňovat. I my se můžeme zařadit mezi evropské a světové lídry v eGovernmentu. Kde je vůle, tam je cesta!

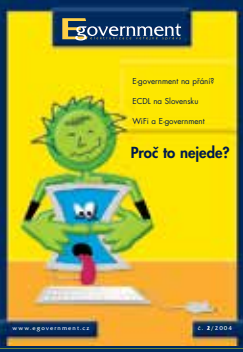
MJ

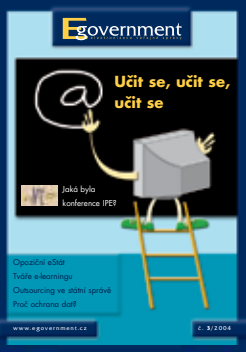
Egovernment

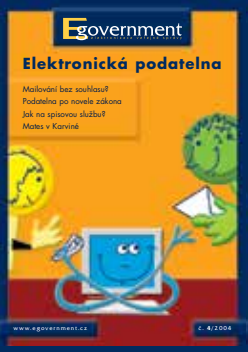
elektronizace veřejné správy

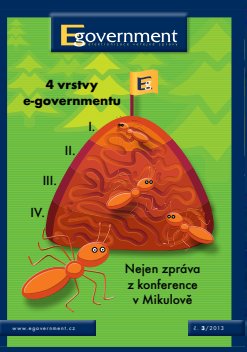












Vše o elektronizaci veřejné správy
- srozumitelně a zdarma:

www.egovernment.cz

Když jde o kyberbezpečnost, méně je někdy více

Již od 1. 1. 2015, tedy už přes 3 roky, se veřejné instituce musejí řídit zákonem o kybernetické bezpečnosti. Ten v pátém paragrafu rozděluje bezpečnostní opatření na organizační a technická, kterých je celkem dvanáct. Mezi ně patří například nasazení nástrojů na ochranu před škodlivým kódem či nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí. I když cílem je definovat povinnosti tak, aby poskytly komplexní ochranu a pokryly mnoho oblastí, přesto v oblasti kyberbezpečnosti platí jedna klíčová zásada: méně totiž často znamená mnohem více.

Celých 72 % bezpečnostních profesionálů v průzkumu Cisco 2018 Security Capabilities Benchmark Study uvedlo, že primárně kupují to nejlepší řešení, které si mohou dovolit. Pouze 28 % bezpečnostních profesionálů pak primárně vybírá řešení tak, aby byla integrována se stávající infrastrukturou. A tak není divu, že (jak z průzkumu dále vyplývá) 70 % organizací využívá bezpečnostní řešení od 6 a více dodavatelů. Přitom v roce 2016 takto odpovědělo „pouze" 55 %. 5 % respondentů dokonce říká, že používají produkty od více než 50 dodavatelů.

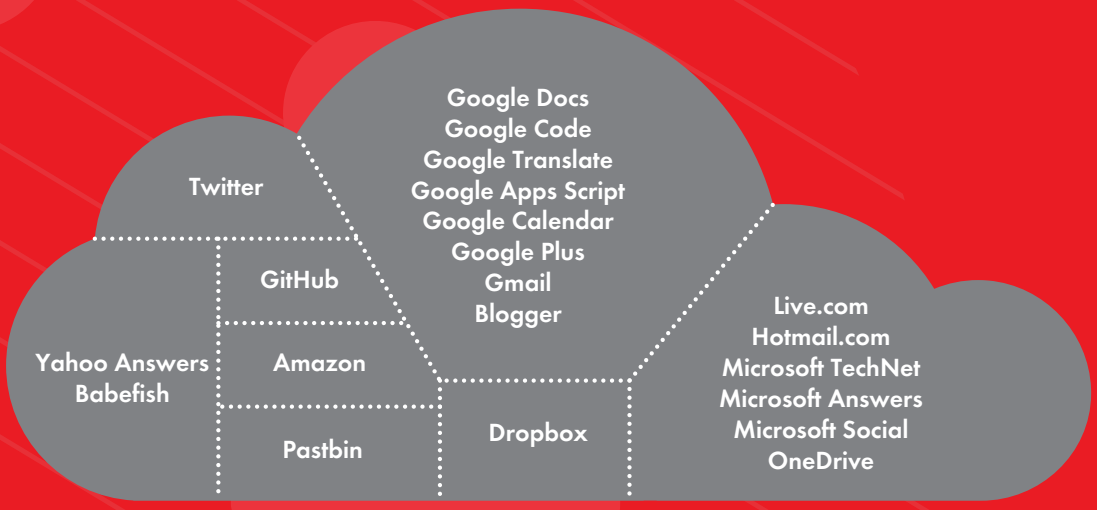
„Tyto organizace si ale neuvědomují dva základní problémy, kterým jdou tímto přístupem naproti. Zaprvé, na trhu je již dnes velký nedostatek bezpečnostních specialistů, a pokud organizace vyžaduje experta, který umí pracovat s desítkami bezpečnostních nástrojů napříč portfoliem mnoha výrobců, může snadno narazit na limity trhu," říká Milan Habrcetl, bezpečnostní expert společnosti Cisco, a dodává: *„Druhý potenciální problém se týká nízké míry integrace všech nástrojů. Jinými slovy, pokud odhalí problém jedna část architektury, nemusí informovat tu další a vznikají tak paradoxně nové bezpečnostní díry. Nehledě na to, že je pak velmi těžké udržet si přehled o tom, v jakém stavu je konkrétní řešení instalováno a konfigurováno."*

OCHRANA, TO NENÍ JEN PREVENCE

Výše zmíněný zákon o kybernetické bezpečnosti dále ukládá orgánům veřejné moci povinnost zajistit reaktivní a ochranná opatření. Společnost Cisco přístup komplexní ochrany prosazuje dlouhodobě. *„Bezpečnostní architekturu je nutné budovat tak, aby dokázala pokrýt všechny fáze útoku – tedy před, během něj i po něm, neboli zaměřit se nejen na prevenci, ale i detekci a následnou reakci,"* vysvětluje Milan Habrcetl. Prevence spočívá ve vybudování integrovaného řešení, ale důležitou součástí je i rychlá detekce. Tradičním řešením na trhu totiž trvá v průměru 100 až 200 dní, než dokážou odhalit novou hrozbu.

Útočník tak má běžně i půl roku na to, aby dokázal svůj škodlivý software v počítačové síti rozšířit a zjistit tak veškeré údaje, které potřebuje. Společnost Cisco v posledním měření odhalování nových hrozeb v rámci studie Cisco 2018 Annual Cybersecurity Report dosáhla mediánu 4,6 hodin pro odhalení takzvaných zeroday útoků, tedy hrozeb, se kterými se její bezpečnostní systémy dříve nesetkaly. To je možné díky globálnímu monitorování sítí

Příklady legitimních služeb, které se zneužívají ke vzdálenému řízení aktivity malwaru *Zdroj: Anomali*



a zapojení umělé inteligence a strojového učení. Úspěšné nasazení těchto metod funguje pouze za předpokladu dostupnosti enormního množství dat, nad kterými lze detekční algoritmy zdokonalovat. Algoritmy společnosti Cisco, zaměřené na analýzu síťového provozu, totiž globálně každý den blokují zhruba 20 miliard potenciálně škodlivých spojení. V nich denně naleznou průměrně 1,5 milionu nových malwarových vzorků, které organizace ještě nezaznamenaly. Průměrně se v síti organizace vyskytuje 1 % zařízení, na kterém se nachází zatím nedetekovaná nákaza. Nicméně právě toto 1 % způsobuje 99 % škod.

Zákon o kybernetické bezpečnosti dále daným orgánům veřejné moci dává za povinnost bez zbytečného odkladu oznámit Národnímu úřadu pro kybernetickou a informační bezpečnost provedení reaktivního opatření a jeho výsledek. Je ale velmi důležité, aby instituce dokázaly monitorovat útok v jeho plném rozsahu. *„Klíčovým faktorem pro třetí fázi kybernetického útoku, tedy fázi, která nastává až po něm, je zmapování a minimalizace škod. Klíčovou roli při tom hraje viditelnost síťového provozu. Dnešní kybernetické útoky totiž dokážou zcela proměnit svoji strukturu během 24 hodin,"* popisuje Milan Habrcetl.

Trendy v aktualizaci zařízení internetu věcí *Zdroj: Qualys*

Zranitelná zařízení

Úplně aktualizovaná zařízení	**1206**
Zařízení s kritickou zranitelností	**6095**
Celkový počet zkoumaných zaříze	**7328**

A právě zde se projevují výhody technologií využívající strojového učení. Kromě toho, že se algoritmy rychle učí chování nově objevených hrozeb v síti, dokážou také nové poznatky implikovat zpětně v čase. Je-li tedy odhalena nová hrozba v jednom zařízení, jsou varovány organizace po celém světě a jejich systémy zpětně zkontrolovány.

HLAVNÍ KYBERHROZBY OHROŽUJÍCÍ VEŘEJNÝ SEKTOR

Studie Cisco 2018 Annual Cybersecurity Report mapovala nejdůležitější trendy, které mají dopad na veřejný sektor. Výzkumníci se zaměřili na útoky a jejich techniky, které pro tyto organizace v současné době představují největší rizika. Mezi ty hlavní patří:

- **sofistikovaný malware s ničivým dopadem:** vyděračský software, neboli ransomware, se v posledních letech stal noční můrou nejedné organizace. I když technika zašifrování souborů a následného vydírání oběti je již dlouho známa, v loňském roce ji útočníci posunuli na novou úroveň. Zatímco dříve, aby byl počítač zašifrován, musel uživatel omylem stáhnout malware (nejčastěji prostřednictvím infikovaného e-mailu), dnes dokážou tyto útoky skenovat sítě a automaticky se šířit. Mnoho z nich navíc už nemá za hlavní cíl maximalizovat zisk z výkupného, ale napáchat maximální škody;
- **zneužívání legitimních služeb:** mnoho uživatelů dnes spoléhá na služby, jako jsou Google Docs, Dropbox či Twitter, protože představují efektivní pracovní nástroj. Právě toho útočníci využívají, neboť jejich taktikou je za každých okolností splynout s davem. A právě skrze tyto služby maskují své aktivity, které se pro IT správce mohou jevit jako zcela běžný provoz;
- **zneužívání bezpečnostních mezer v zařízení internetu věcí:** neaktualizovaná a nemonitorovaná zařízení internetu věcí (například čidla pro monitorování teploty, čtečky karet či bezpečnostní kamery) nabízejí útočníkům zajímavou možnost, jak se dostat do sítě. Navíc roste velikost botnetů, které doručují automatizované pokročilé DDoS útoky.

SLOŽITÝ SVĚT VYŽADUJE JEDNODUCHÁ ŘEŠENÍ

Všechny tři trendy ukazují, že na vládní a další organizace veřejného prostoru míří nejpokročilejší hrozby. I proto jsou jejich povinnosti ukotveny v české legislativě. Nicméně teorie a praxe bývají občas dvě různé věci. Pokud se mají veřejné instituce efektivně bránit, měly by postavit takové řešení, které funguje silně jako jeden celek, pokrývá všechny fáze, které jsou s útokem spojeny, a využívá nejmodernější bezpečnostní technologie. Samozřejmostí je pak nasazení umělé inteligence a strojového učení. Nicméně zde platí jedno klíčové pravidlo. Kvalita takového řešení je úměrná objemu dat, která dokáže analyzovat.

CISCO

info◆com

- Sympozia
- Konference
- Kongresy

Na Zatlance 10, Praha 5 • Tel.: 241 412 518 • infocom@infocom.cz • www.infocom.cz

Proč dnes kybernetická bezpečnost selhává?

Kyberprostor, cloud, bezpečné uložiště, ověřování osob, strojů a další milion známých a neznámých pojmů, které by měl mít obyčejný smrtelník na paměti v momentě, kdy sedne ke klávesnici počítače, aby napsal své heslo a přihlásil se do prostoru jedniček a nul. Kybernetický prostor je totiž pro běžné uživatele velká neznámá. Často začíná klávesou ENTER a končí zobrazením dat na obrazovce počítače.

Z jejich pohledu je poměrně jedno, kam data putují. Oddělení informačních technologií by se ale mělo postarat o to, aby v případě, že data opouštějí datové centrum, či lokální síť, byla zašifrována, a tudíž pro okolní svět nečitelná. Na zaměstnancích pak je, aby se chovali zodpovědně, neotevírali přílohy, které neznají, a veškeré chyby a bezpečnostní incidenty hlásili. Důležité může být každé vyskakovací okno, e-mail s chybnou češtinou, nebo žádost o pomoc či poskytnutí čísla účtu.

Podle PwC se počet počítačových útoků se meziročně zvýšil o 38 procent. Ještě znepokojivější je skutečnost, že tyto útoky jsou stále více sofistikované a úspěšnější. Firma Institut Ponemon odhadla, že náklady na kybernetickou kriminalitu u amerických firem vzrostly za posledních šest let o 82 procent. V roce 2016 denně docházelo k více než 4000 kybervyděračským útokům, nemluvě o devastujících účincích škodlivého softwaru, jako WannaCry, kdy i nemocnice ztratily přístup k životně důležitým údajům, včetně lékařských záznamů svých pacientů. V reakci na tyto útoky samozřejmě stouply výdaje na kybernetickou bezpečnost (v r. 2017 přesáhly 86,4 miliardy dolarů) a podniky a organizace zavádějí dodatečné linie obrany okolo svých systémů.

Zabezpečení nemůže být účinné, budeme-li se pouze snažit držet krok s vývojem kybernetických hrozeb a útoků – vždy totiž budeme o krok pozadu. Stanovení toho, jak se nejlépe bránit před touto lavinou kybernetických útoků, je klíčovou prioritou každé organizace, která jde vpřed. Ale možná překvapivě mnoho organizací považuje za náročné vyvinout koherentní strategii. Nedávný celosvětový průzkum ukázal, že zatímco lídři v podnikání mají tendenci strategicky a dlouhodobě přemýšlet, vedoucí představitelé bezpečnosti upřednostňují zaměřovat se na individuální řešení každého možného útoku.

Problémem tohoto taktického přístupu je, že množství a typ útoků neustále roste a vyvíjí se. Snažíme se bránit útoky na všech frontách jednotlivě, reagovat na nejnovější a největší hrozbu. Samotný počet úspěšných kybernetických útoků je ale důkazem toho, že tento reaktivní taktický přístup k bezpečnosti dosáhl hranic své účinnosti. Je čas na nový přístup.

Jsme schopni poměrně dobře ovlivnit technologie, chování uživatelů už bohužel ovlivnit nemůžeme. Proto jsou technologie VMware primárně navrhovány tak, aby dokázaly eliminovat případné nevhodné chování či chyby uživatelů. Aby šlo případnou nepříznivou situaci napravit, je totiž nutné vkládat bezpečnostní prvky přímo do IT systémů. To se snadněji řekne, než udělá – ale s pokročilými technologiemi a novými schopnostmi, které poskytuje cloud a mobilní technologie, to je dnes nejen možné, ale i nezbytné.

Flexibilní obrana založená na architektuře umožňuje, aby Vaše oddělení IT – jakmile došlo k oznámení o útoku – identifikovalo, zmírňovalo a omezovalo útok. Přerušení dat je jako onemocnění; pokud je můžete vidět a léčit dříve, můžete snížit závažnost účinků.

To, kvůli čemu zůstáváme stále zranitelní, je způsob myšlení. Zastaralé systémy, bez ohledu na to, kolika vrstvami ochrany je obalíme, zůstávají zastaralé. Vzhledem k alarmujícímu tempu a rozsahu narušování bezpečnosti by bylo záhodno, aby podniky a organizace začaly praktikovat základní kyberhygienu a chránit své klenoty – aplikace a data, bez nichž nemohou fungovat.

CO JE TO KYBERHYGIENA?

Stručně řečeno, jedná se o základní principy, s nimiž by měly být obeznámeny všechny podniky a organizace, které provozují nějaký IT systém, a tyto principy uplatňovat v každodenním provozu. VMware popisuje pět základních principů. Nejedná se o nápady nové, jen někdy pozapomenuté. A naopak, bezpečnostní protokoly někdy nejsou udržovány zcela aktuální s ohledem na vývoj stavu techniky.

ZÁKLADNÍ PRINCIPY

1. Nejnižší nutná oprávnění

I když plně důvěřujete všem zaměstnancům, není nutné, aby měla recepční stejná přístupová oprávnění jako generální ředitel. Přidělte uživatelům nejnižší nutná oprávnění a výrazně omezíte možnost útoku na svoje nejcennější data. V hotelu byste také nedali každému hostu univerzální klíč od všech pokojů.

2. Mikrosegmentace

Že dávno neužíváme padací mosty a hradby, má dobrý důvod – tato opatření dávají falešný pocit bezpečí a podporují laxní přístup k bezpečnosti uvnitř opevnění. Jakmile se útočníkovi podaří vnější obranou proniknout, hrozba je uvnitř a není, jak se před ní skrýt. Rozčlenění sítě na vrstvy a samostatné jednotky udržuje celý systém v bezpečí a zajišťuje, že přístupové body nejsou ponechány zranitelné v případě útoku. Nezanedbávejte vnější obranu, ale ani na ni nespoléhejte jako na samospasitelnou.

3. Šifrování

Šifrování považujte za poslední zbraň proti hackerům ve svém arzenálu – kromě toho, že díky němu máte v zabezpečení navrch. Pokud vše ostatní selže a útočníkovi se podaří proniknout skrze firewally a přístupové protokoly, díky šifrování mu budou veškerá důležitá data k ničemu. Podobně jako je obtížné složit Rubikovu kostku, pokud neznáte správný postup, rekonstruovat šifrovaná data je velmi obtížné. Součástí základní kyberhygieny by mělo být šifrování souborů a dat před jejich sdílením. Totéž platí o šifrování síťového provozu všude tam, kde je to možné.

4. Vícefaktorové ověřování

Zabezpečení se posouvá na osobnější úroveň a využívá otisky prstů, rozpoznávání tváře a jiné biometrické metody. I základní dvoufaktorové ověřování dokáže zastavit první vlnu útoků. Ale čím osobnější ověřování bude, tím bezpečnější budou naše sítě. Vždyť otisk prstu je podstatně složitější ukrást než PIN kód.

5. Aktualizace

Systémy vyžadují aktualizace z dobrého důvodu. Pokaždé, když škodlivý software získá nové schopnosti, Váš poskytovatel služeb reaguje aktualizacemi systémů a softwaru. Nesetrvávejte v minulosti. Aktualizujte a upgradujte, abyste měli nad útočníky vždy navrch.

Seznámit se s těmito principy je jedna věc, ale uvést je do praxe je naprosto nezbytné. Každý ve Vaší organizaci by měl chápat, proč je kyberhygiena důležitá. Ale zásadnější je, aby Vaši IT manažeři a další odpovědní pracovníci pochopili, jak je reálně praktikovat. Stejně jako čistění zubů a mytí rukou totiž pomáhají správné kyberhygienické návyky chránit každého.

Ondřej Micka a Ondřej Číž

vmware®

GORDIC představil automatizované nástroje pro naplnění požadavků GDPR

Zřejmě žádná legislativní změna či novinka nedostala v médiích v posledních měsících více prostoru než GDPR. O vteřinovém odpočtu směřujícím k datu 25. 5. 2018 se muselo mnoha dotčeným osobám snad i zdát. Byla panika opravdu na místě, nebo šlo pouze o přehnané a neadekvátní obavy? Pravdu nalezneme asi někde uprostřed. Pokud firmy uchopily přípravu zodpovědně a vyhnuly se podvodným společnostem, které slibují rychlé zajištění souladu s nařízením pomocí univerzálních řešení, přenesly se přes pětadvacátý květen s naprostým klidem.

Naštěstí jsou na trhu i firmy, které s přípravami opravdu pomohly. Skutečná pomoc ale vyžaduje aplikaci značně specifických opatření. Platforma KYBEZ, zaštiťovaná společností GORDIC, v minulých měsících řadě společností zajistila soulad s GDPR. Pokaždé šlo o „utkání sítě" procesů a opatření na míru konkrétní firmě, kterému předcházela podrobná analýza procesů, rizik, systémů a dalších klíčových aspektů. Na trhu bylo však mnoho firem, které na nařízení GDPR dlouho nebyly připraveny a nutná opatření nechávaly na poslední chvíli. Tyto firmy více než ostatní ocenily převratné novinky od firmy GORDIC, které dovedou celý proces vedoucí k souladu s obávaným nařízením výrazně urychlit – trio nástrojů, díky kterému mohou firmy provést kompletní analýzu samy. Ani přečtení názvů jednotlivých nástrojů mnoho času nezabere – GDA, PDL, PIL. U všech jsou samozřejmě zachovány postupy metodologie GORDIC GDPR, které byly vytvořeny pro účely souladu s nařízením.

GDA

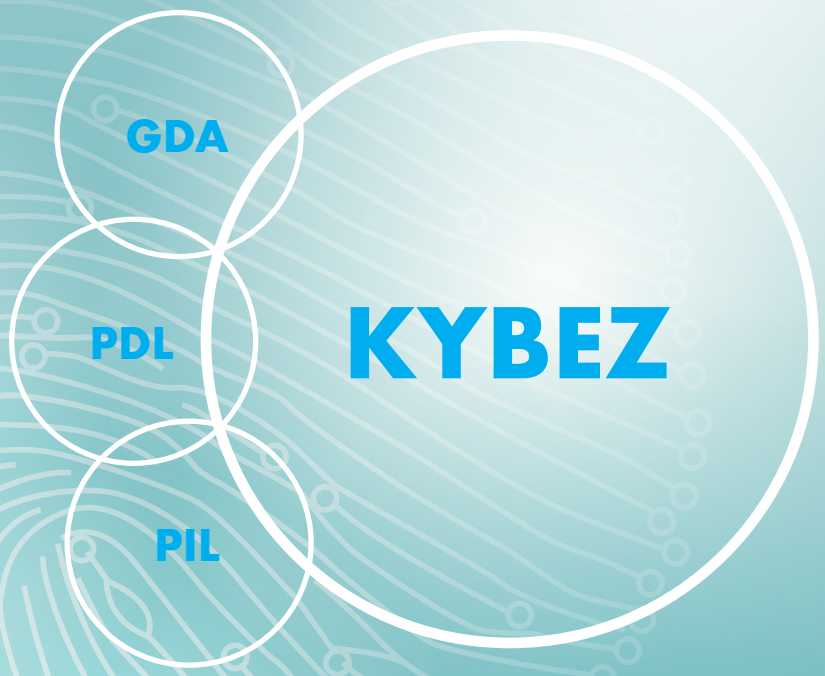
Díky **GDPR Analysis** lze identifikovat skutečný stav organizace v oblasti nakládání s osobními údaji a provést tak komplexní analýzu organizace na soulad s GDPR. To vše je umožněno v sofistikovaném online prostředí. Nástroj GDA pomůže najít potenciální rizika plynoucí z jednotlivých zpracování osobních údajů a pružně na ně reagovat. Výstupem jsou kompletní doporučení v podobě elektronických dokumentů hodnotících situaci analyzované organizace. Jak jistě víme, GDPR není jedinou právní úpravou ochrany osobních údajů. Analyzovat je nutné i soulad se zákonem o kybernetické bezpečnosti a zákonem o spisové službě a archivnictví. I s tímto GDPR Analysis dovede pracovat a zákazníkovi pomoci.

PDL

Zkratka skrývající anglický název **Personal Data Lookup** označuje nástroj mapující výskyt osobních údajů na databázové vrstvě nebo v souborových dokumentech. Díky pokročilým vyhledávacím metodám a algoritmům identifikuje místa, kam byly záměrně či zcela náhodně uloženy osobní údaje. Výstupem je tak podrobný podklad pro analýzu připravenosti na GDPR ve formě webové prezentace a CSV dokumentu. Nezáleží tedy na tom, jestli se dostaly osobní údaje do textových dokumentů, nebo si hoví kdekoliv v databázích, PDL si na ně posvítí!

PIL

Personal Identity Lookup (PIL) slouží k vyhledávání všech osobních údajů spojených s konkrétním subjektem napříč databázemi a souborovými dokumenty. Svoji využitelnost tak nachází například při požadavcích na přenositelnost, výmaz nebo k vyhledávání údajů vztahujících se ke konkrétnímu subjektu. Stejně jako i dva předešlé nástroje poskytuje PIL výstupy, které s rezervou poslouží jako důkaz-



ní materiál pro kontrolní orgány. Práce s nástrojem PIL je jednoduchá a poměrně intuitivní. Pro vyhledávání údajů konkrétního subjektu stačí zadat pouze jeden jediný údaj, o zbytek se PIL postará.

DRMS KYBEZ

GORDIC představil kromě výše zmíněné trojice analytických nástrojů i spisovou službu, která ve všech ohledech splňuje požadavky nařízení GDPR, zákona o kybernetické bezpečnosti (ZoKB) a zákona o archivnictví a spisové službě. Spisová služba od firmy GORDIC si našla v minulosti velké množství příznivců. Stávající zákazníci s novinkou DRMS KYBEZ získali jistotu souladu s platnou legislativou, aniž by se měnilo rozhraní systému, ve kterém jsou zvyklí pracovat. Pro nové zákazníky může být pořízení DRMS KYBEZ taktéž lákavější než kdykoliv dřív. Získají tak nástroj řízení záznamů a dokumentace s vysokým stupněm zabezpečení, datovou provázaností jednotlivých částí a otevřeným rozhraním – to vše v souladu s aktuálně platnou legislativou i s GDPR.

Externí DPO – pověřenec na ochranu osobních údajů jako služba

Tím ale není výčet novinek souvisejících s GDPR u konce. Pro mnohé organizace totiž přináší nařízení i změnu v podobě zavedení pověřence pro ochranu osobních údajů (DPO), který zodpovídá za celkovou agendu ochrany osobních údajů. Nicméně vyškolit vlastního zaměstnance na funkci DPO může představovat vysoké výdaje, nehledě na eventuální komplikace, jako dovolená či nemocenská, během nichž nebude moci DPO vykonávat svoji práci. Z tohoto důvodu velká část organizací volí možnost DPO jako externí služby, která je dostupná nepřetržitě a jejíž dodavatelé disponují znalostmi a zkušenostmi z více oborů a typů subjektů.

Při tvorbě nástrojů zúročila společnost GORDIC praxi v oblasti kybernetické bezpečnosti i zkušenosti s implementací opatření vedoucích k souladu s GDPR u řady společností. Stejným analytickým principům a implementačním postupům dokázal GORDIC vdechnout automatizovaný rozměr. Díky inovativním automatizovaným nástrojům si tak zákazníci mohou analýzu provést sami, opakovaně a v jakoukoli denní dobu. Kvalitní cestou k naprostému souladu s GDPR tak stihne před šibeničním 25. květnem projít mnohem více společností.

GORDIC®

Elektronická identita

Elektronická identita je pojem, se kterým se setkáváme zejména od doby, kdy byly známy první návrhy nařízení eIDAS. Tento právní předpis definuje elektronickou identifikaci jako „postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo fyzickou osobu zastupující právnickou osobu".

V nařízení eIDAS je výslovně uvedeno, že nemá za cíl zasahovat do systémů správy elektronické identity a souvisejících infrastruktur zřízených v členských státech. Jeho cílem je zajistit, aby u přístupu k přeshraničním on-line službám poskytovaným členskými státy byla možná bezpečná elektronická identifikace a autentizace, a to zejména v případě veřejných služeb.

V krátkosti připomeňme význam uvedených pojmů, resp. otázek, na které se vyžaduje odpověď:

- **identifikace** – „kdo jsi?", tj. určení/sdělení, kým jsem, za koho se vydávám, lze řešit například zadáním uživatelského jména. Příklad: systém se snaží zjistit identitu uživatele prohledáváním v databázi záznamů všech uživatelů. Subjekt sám o sobě nepředkládá tvrzení o své identitě, jedná se o porovnávání 1:n;
- **autentizace** – „jsi skutečně ten, za koho se vydáváš?", tj. prokázání, že jsem skutečně tím, za koho se vydávám. Realizuje se v nejjednodušším případě pomocí hesla (prokazuji jeho znalost), často pomocí jednorázového hesla (OTP) nebo pomocí autentizačního certifikátu. Jedná se o náležitost každého bezpečného systému. Příklad: systém se snaží ověřit identitu uživatele poté, co ji uživatel sám udá (např. zasunutím čipové karty, napsáním přihlašovacího jména či osobního identifikačního čísla). Jedná se o porovnávání 1:1. Autentizaci lze chápat jako podmnožinu identifikace;
- **autorizace** – „máš sem skutečně přístup?", tj. získání souhlasu/oprávnění k určitému úkonu, kroku, přístupu apod., přičemž někdo souhlas/oprávnění uděluje, a to podle předem stanovených pravidel. Jedná se o proces ověření přístupových oprávnění uživatele vstupujícího do informačního systému. Tento proces ve většině případů navazuje na proces autentizace. Podstatou autorizace je ověřit, zda daný uživatel má oprávnění provést příslušnou akci, například vložení nového záznamu nebo modifikace stávajícího.

Elektronická identifikace není nic nového, známe ji však spíš pod pojmem *digitální identita*. Je obdobou fyzické identity, nezbytnou ve světě informačních systémů a internetu. Jestliže prokazujeme totožnost například dnes běžným občanským průkazem, předkládáme určitý soubor informací o své osobě, který je na tomto průkazu uveden. Stejně tak činíme ve světě IT, opět předkládáme souhrn informací o své osobě, tentokrát v digitální podobě. Každý uživatel internetu má zpravidla více svých elektronických identit, které používá při identifikaci pro přihlášení do systému nebo pro určitou transakci z počítače, tabletu nebo chytrého telefonu.

Poskytovatel služby, vůči které se prokazuje elektronická identita, vždy sám zváží – pokud není vázán právním nebo jiným předpisem – zda k přístupu k dané službě postačí jednoduchá forma digitální identity, často přihlašovací/uživatelské jméno a heslo, kde každý ručí sám za svoji digi-

tální identitu. Poskytovatel v těchto případech neřeší, zda se skutečně jmenujete James Bond, nebo je to vaše přezdívka. Nás však zajímají především situace, kdy musí být zajištěno, že elektronická identita odpovídá skutečné identitě, resp. skutečné osobě. Je zřejmé, že se jedná o systémy bank, podnikové informační systémy a v neposlední řadě informační systémy veřejné správy. V těchto případech nutně musí nastoupit prvek ověření skutečné totožnosti dané osoby s využitím takových procesů, které zaručí vydání digitální identity správné osobě a následně ručí za proces řádného ověřování.

Ve velké míře se jako nástroj elektronické identity pro přístup do informačního systému používá *autentizační certifikát;* čeští kvalifikovaní poskytovatelé služeb vytvářejících důvěru tyto certifikáty vydávají shodně pod obchodním názvem *komerční certifikát*. Je možné vydat tento certifikát, aniž by bylo nutné „face to face" ověřit totožnost žadatele o tento typ certifikátu? Teoreticky ano a řada certifikačních autorit tak činí, ovšem čeští kvalifikovaní poskytovatelé vždy trvají na ověření totožnosti žadatele na místě. Někteří poskytovatelé v případě, kdy žadatel o komerční certifikát má už platný kvalifikovaný certifikát pro elektronický podpis, umožňují na základě žádosti elektronicky podepsané s využitím tohoto kvalifikovaného certifikátu vydat i komerční certifikát. Neboť totožnost žadatele už byla ověřena pro vydání komerčního certifikátu dostačujícím způsobem.

Aby byl uživatelům poskytnut větší komfort, První certifikační autorita, a.s. (I.CA), vydává pod obchodním názvem *Twins* oba typy certifikátů najednou – kvalifikovaný pro vytváření podpisu a komerční pro autentizaci a případně pro šifrování. Majitel Twins má tedy oba kdykoliv k dispozici s možností každoroční obnovy (vydání následných certifikátů), která probíhá online. Fyzická osoba, která si Twins pořídí, navštíví registrační autoritu poskytovatele pouze jednou, při vydání první dvojice certifikátů, a následně už veškerá komunikace probíhá jen po síti.

Nejvyšší míru komfortu a zároveň nejvyšší míru bezpečnosti představuje spojení certifikátu a příslušného soukromého klíče na hardwarovém prostředku; je výhodné, a především bezpečné volit ty prostředky, v jejichž čipu se soukromý klíč generuje a není exportovatelný.

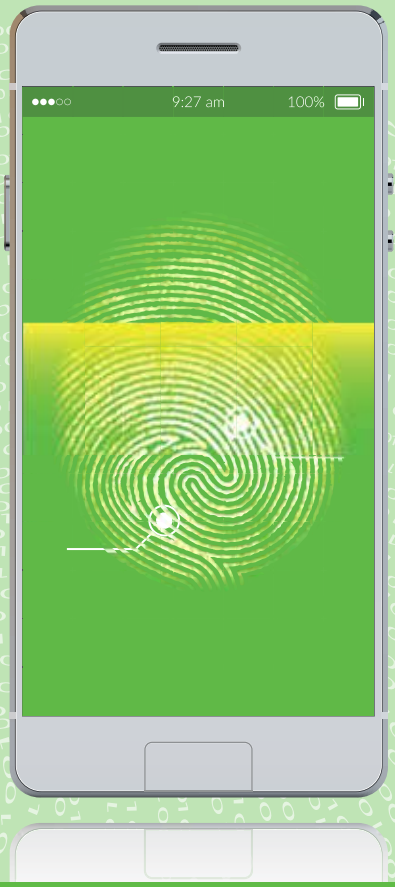
Typicky jsou takovými nástroji *kvalifikované prostředky pro vytváření elektronických podpisů* (QSigCD), které splňují požadavky eIDAS. Tyto prostředky poskytují všichni kvalifikovaní poskytovatelé, v případě I.CA se už tradičně jedná o čipové karty Starcos, v současné době řady 3.5. Nabízeny jsou buď ve standardní velikosti pro použití se čtečkou čipových karet, nebo opatřená výřezem (plug-in formát) pro vylomení čipu a jeho vložení do tzv. USB tokenu.

Uživatel Twins má tedy možnost vytvářet *kvalifikovaný elektronický podpis* podle eIDAS a zároveň má k dispozici komerční certifikát s potenciálem autentizačního nástroje. V této souvislosti je vhodné připomenout, že funkce elektronické identifikace a elektronického podpisu, případně elektronické pečetě nelze zaměňovat - podpisy a pečetě slouží k vyjádření projevu vůle podepisující nebo pečetící osoby, například učinit konkrétní podání, elektronická identifikace slouží k identifikaci osoby.

Pokud se jedná o řešení autentizačních procesů, I.CA nejen vydává příslušné certifikáty, ale v řadě případů se u svých klientů podílí i na celém řešení autentizace.

Aby byla aktuálně používaná terminologie úplná, je nutné zmínit *identifikační certifikát*, který bude součástí kontaktního čipu občanského průkazu a bude sloužit k elektronické identifikaci zejména při přístupu občana, držitele konkrétního občanského průkazu, k informačním systémům veřejné správy.

Ing. Petr Budiš, Ph.D., MBA
ředitel a předseda představenstva
První certifikační autorita, a.s.



Autentizace otiskem prstu do mobilního zařízení

Tento příspěvek se zamýšlí nad přínosy a riziky využití autentizace pomocí otisku prstu do mobilních zařízení a porovnává tento způsob autentizace s běžnou autentizací pomocí PINu.

Autentizace otiskem prstu

Autentizace otiskem prstu není obecně považována za bezpečný způsob přihlašování, a to i při porovnání s běžně používanými metodami, jako je přihlašování jménem a heslem.

Autentizaci otiskem prstu je zejména vytýkáno:

- běžné snímače, a to zejména integrované do mobilních zařízení, je možné zmást vytvořeným duplikátem otisku prstu (sejmutým z mobilního zařízení, sklenice, vytvořené z velice kvalitní fotografie) - těmto snímačům chybí test živosti;
- otisk prstu není možné zneplatnit nebo změnit (maximálně přestat používat a vyřadit ze seznamu povolených otisků), přičemž je člověk nechává po celou dobu svého života na všech předmětech, kterých se dotkne;
- otisky prstu mohou být sejmuty i bez spolupráce uživatele (donucení, spánek, bezvědomí, ...);
- rozpoznání otisku prstu není 100% přesné – vyhodnocování vždy operuje s definovanou úrovní nejistoty.

Vše výše uvedené je pravdivé a používat otisk prstu jako jediný faktor autentizace není za běžné situace možné doporučit.

Porovnání otisku prstu vs. PINu

Je však otázkou, zdali použití otisku prstu pro autentizaci do mobilního zařízení přináší výrazné snížení bezpečnosti při porovnání s běžně používaným přihlašováním pomocí PINu.

Přihlašování pomocí gesta není uvažováno, neboť jeho úroveň zabezpečení je ještě nižší než použití otisku prstu, a není ani uvažováno zabezpečení heslem, které je sice technicky možné, ale uživatele extrémně obtěžující.

Z tabulky možných scénářů útoku vyplývá, že u většiny scénářů útoků nabízí otisk prstu přibližně stejnou (u některých scénářů nižší, u jiných vyšší) úroveň ochrany.

Popis scénáře útoku	Ochrana poskytovaná PIN	Ochrana poskytovaná otiskem prstu	Porovnání
Náhodné odcizení nehlídaného mobilního zařízení	**Základní ochrana** Zloděj vyzkouší základní PINy, potom telefon spíše smaže	**Základní ochrana** Otisk se dá sejmout z povrchu telefonu, ale je možné předpokládat, že otisky budou poškozeny/překryty otisky zloděje; scénář útoku je příliš komplikovaný, zloděj telefon spíše smaže	Srovnatelná úroveň záruk
Ztráta telefonu	**Základní ochrana** Zloděj vyzkouší základní PINy, potom telefon spíše smaže	**Základní ochrana** Otisk se dá sejmout z povrchu telefonu, ale je možné předpokládat, že otisky budou poškozeny/překryty otisky zloděje; scénář útoku je příliš komplikovaný, zloděj telefon spíše smaže	Srovnatelná úroveň záruk
Náhodné odcizení telefonu při používání	**Minimální ochrana** Zařízení je odemčené nebo zloděj může odpozorovat zadávaný PIN (např. v tramvaji, zastávce ...)	**Minimální ochrana** Zařízení je odemčené, ale otisk prstu zloděj neodpozoruje	Srovnatelná úroveň záruk, otisk lehce lepší
Přístup do telefonu ze strany spolupracovníků	**Minimální – základní ochrana** Spolupracovník může odpozorovat často zadávaný PIN (např. v autě)	**Základní ochrana** Spolupracovník má přístup k otiskům prstů vlastníka, ale daný útok spočívající ve vytvoření duplikátu vyžaduje jisté úsilí	Otisk poskytuje lepší úroveň záruk
Přístup do telefonu ze strany členů rodiny	**Minimální – základní ochrana** Členové rodiny PIN většinou znají (i třeba jenom odpozorováním při odemykání telefonu v autě při navigaci)	**Základní ochrana** Členové rodiny mají přístup k otiskům prstů vlastníka, ale daný útok vyžaduje jisté úsilí spočívající ve vytvoření duplikátu nebo drzost (přiložení prstu k ruce spící osoby)	Srovnatelná úroveň záruk, otisk lehce lepší
Cílený přístup do telefonu (cílený útok)	**Žádná ochrana** Útočník PIN odpozoruje	**Žádná ochrana** Útočník si vytvoří duplikát otisku	Srovnatelná úroveň záruk
Násilný cílený útok (donucení k odemčení telefonu)	Teoreticky základní ochrana, ale prakticky většina osob ustoupí	**Žádná ochrana**	Srovnatelná úroveň záruk, PIN lehce lepší

Je možné, že s vyšším podílem používání otisku prstu už budou útočníci lépe vybaveni ke snímání a vytváření duplikátů falešných otisků a následně bude nutné úroveň rizika a poskytované ochrany přehodnotit. Zároveň je ale možné předpokládat, že technologie pro snímání otisků prstů se bude vyvíjet a zlepšovat, případně že bude tento způsob autentizace nahrazen kvalitnějšími biometrickými snímači.

Omezení použití PINu

V prostředí Android je PIN zadávaný pro odemčení mobilního zařízení používaný i pro získání klíče, kterým je zařízení případně šifrováno. Bohužel obecné požadavky na PIN použitý pro získání šifrovacího klíče jsou v naprostém nesouladu s požadavky na PIN, který má být pravidelně a jednoduše zadáván. Většina uživatelů potom z důvodu jednoduché použitelnosti vybere krátký PIN, který je pro účel získání šifrovacího klíče naprosto nedostačující.

Z tohoto pohledu může použití otisku prstu bezpečnost mobilního zařízení zvýšit, neboť znalým uživatelům umožní použít pro základní přihlášení a šifrování mobilního zařízení delší heslo/PIN, protože tento zadávají pouze ve výjimečných případech (při spuštění mobilního zařízení).

Závěr

Autentizace pomocí otisku prstu nabízí pouze základní úroveň ochrany přístupu k mobilnímu zařízení, tato úroveň ochrany však není výrazně nižší než při autentizaci s využitím PINu.

Oba dva způsoby zabezpečení je však možné akceptovat pouze pro osoby, u kterých není předpokládán cílený útok. U osob, kde je možné očekávat vyšší pravděpodobnost cíleného útoku, je nutné doporučit použití delšího PINu nebo hesla (zadávaný PIN/heslo slouží pro získání klíče pro šifrování mobilního zařízení).

Zde se jeví jako výhodné použít kontejnerizaci a pro přístup do mobilního zařízení používat PIN/otisk a pro přístup k informacím organizace v kontejneru jiný (komplexnější) PIN nebo heslo.

Tým konzultantů společnosti S. ICZ, a.s.

ROK INFORMATIKY 2018

Magazín Egovernment uspořádal ve spolupráci s KÚ Libereckého kraje na přelomu května a června letošní ročník konference ROK INFORMATIKY. Všichni, pro které je zajímavá a důležitá elektronizace veřejné správy na úrovni obcí, měst a krajů, se sešli v příjemném prostředí rezortu Malevil. Díky až tropickému počasí a kulisám rezortu se podařilo navodit téměř dovolenkovou atmosféru, kterou jsme proložili diskuzemi a prezentacemi zajímavých projektů, strategií a záměrů.

Tématem, které se skloňovalo minimálně dva ze tří konferenčních dní, byl Portál občana. **Jiří Kárník, koordinátor projektů za MV ČR**, toto téma představil jak v diskuzi prvního odpoledne, tak především prezentací v rámci hlavního dne. Upozornil, že Portál občana je z pohledu veřejné správy velice důležitý projekt, který je určitou možností, jak plně využít infrastrukturu veřejné správy, a to případně i pro služby třetích stran. Doslova uvedl, že se jedná o zcela novou platformu, kde by nové služby mohly získat zcela nové publikum.

Pro projekt Portálu občana je zásadním datem 1. 7. 2018, kdy nejen dojde k jeho spuštění, ale zároveň odstartuje vydávání nových elektronických občanských průkazů s čipem. Ty budou umožňovat využívání služeb Portálem nabízených. Jiří Kárník nepředpokládá, že by hned počínaje datem spuštění došlo k jeho zahlcení. Návštěvnost a využití bude, podle jeho mínění, plynule narůstat, adekvátně tomu, jak bude Portál naplňován obsahem. V současné době je k dispozici agenda Czech POINT, ČSSZ, některé další formuláře, některé typy trestního oznámení. Rovněž Magistrát hl. m. Prahy připravuje nabídku služeb, k dispozici je e-recept

a pravděpodobně, díky Kraji Vysočina, i vstup do Národního kontaktního bodu českého zdravotnictví.

Souběžně s přípravami Portálu byl podle slov Jiřího Kárníka zpracován manuál pro obce, jak vytvořit vlastní dlaždici, umístit ji v Portálu a jejím prostřednictvím nabízet služby obce.

V rámci druhého dne konference Jiří Kárník ukázal právě vytváření takové dlaždice. Zároveň upozornil, že MV ČR připravuje informační kampaň jak pro občany, tak rovněž pro pracovníky veřejné správy.

Informace MV ČR k Portálu pak ještě doplnil **ředitel SZR Michal Pešek**, který se věnoval problematice elektronické identity. Upřesnil, že služby Portálu budou vyžadovat buď identifikaci prostřednictvím datové schránky, nebo právě zmiňované eOP.

V rámci odpoledních prezentací druhého dne konference byly představeny jednotlivé realizované projekty a vlastní část programu byla pak věnována **Microsoft woknu** – tedy konkrétním ukázkám využití a nasazení řešení společnosti Microsoft. Protože v rámci této části byla bezpochyby nejpoutavější ukázka rozšířené virtuální reality, byla následně druhý den k dispozici v rámci workshopu, kde si jednotliví účastníci mohli prezentované možnosti „na živo" vyzkoušet.

Jednotlivé konferenční dny byly propojeny společenským večerem, který byl rovněž z části sportovní, a byla tak navozena dostatečně přívětivá atmosféra pro neformální diskuze k programu.

Prezentace a fotogalerii naleznete na:
www.egovernment.cz v sekci ROK INFORMATIKY.

Liberecký kraj

Poslední předprázdninová akce magazínu Egovernment se odehrála na výstavišti v Litoměřicích. Spolu s Ústeckým krajem a městem Litoměřice jsme zde připravili dvoudenní setkání zaměřené na geografické informační systémy. Názvem GIS OUTDOOR – Fórum Ústeckého kraje jsme chtěli dát najevo, že forma setkání nebude zcela tradiční konferencí.

Ve dvou dnech jsme zde měli možnost vyslechnout řadu prezentací, tak jako na jiných konferencích. Vedle toho však byly bloky věnované praktickým ukázkám na venkovních plochách výstaviště. Prolínal se zde tedy prezentační, diskuzní i praktický duch.

Význam konference podtrhoval hned triumvirát zahajujících – hejtman Ústeckého kraje Oldřich Bubeníček, ředitel krajského úřadu Milan Zemaník a starosta města Litoměřice Ladislav Chlupáč, kteří nás přivítali a odstartovali dvoudenní jednání. Duchovním otcem myšlenky na uspořádání konference byl vedoucí odboru informatiky Ústeckého kraje Jan Jelínek, který byl rovněž prvním prezentátorem konference. Představil nám pohledem z venku úlohu krajského úřadu v jednotlivých agendách a jejich řešení pomocí informačních technologií a GIS. Až futuristicky pak zněla


Oldřich Bubeníček


Milan Zemaník


Ladislav Chlupáč

prezentace tajemníka města Litoměřic Milana Čigáše, který představoval jejich MÚ jako vysoce moderní nejen v nasazení technologií, především ale v nastavení procesů uvnitř úřadu a přístupu samotných úředníků. Úvodní část konference uzavíral ředitel Inovačního centra Ústeckého kraje Tomáš Siviček, představující současnost, ale především budoucnost a cesty, kterými by se podle něj měla veřejná správa ve svém přístupu ubírat.

Velkou pozornost vzbudilo vystoupení doc. Ing. Jana Paciny, PhD., z ÚJEP, který představil práci svoji a svých kolegů v rámci univerzitního GIS. Praktické ukázky konkrétních výstupů, např. modelování krajiny na základě pozemního laserového skenování, ukázky fotogrammetrie, 3D rekonstrukce zaniklých sídel nebo archeologický výzkum v Súdánu, byly rozhodně oživením programu. V další části jsme se spolu s partnery konference, kterými byly společnosti ARCDATA PRAHA, HRDLIČKA spol. s r.o. nebo T-MAPY, věnovali mobilnímu GIS, chytrým řešením a DTM.

Následně měli účastníci možnost diskutovat s vystavujícími u jejich stánků jak uvnitř konferenčního pavilonu, tak na venkovní ploše. Zde, krom Hasičského záchranného sboru či autonomních vozidel, vzbudilo největší pozornost seskupení dronů a ukázka jejich možností.

Večerní program se nesl v duchu koncertu pod širým nebem, rovněž v prostorách výstaviště.

Druhý konferenční den jsme vyslechli prezentaci využití GIS v rámci HZS ČR, novinky v oblasti open source software QGIS, poskytování dat a služeb ČÚZK, možnostech prostorového řízení vozidel i díky GIS. Závěrečná prezentace byla pak věnována bezpilotnímu létání, tedy otázce dronů, a to z pohledu pravidel, která stanovuje Úřad civilního letectví.

Další informace, prezentace a fotogalerii naleznete na **www.egovernment.cz** v sekci Fórum GIS.

Jak vypadá pohled na Ústecký kraj z ptačí perspektivy, že MÚ Litoměřice patří mezi nejmodernější a nejpokrokovější, že univerzitní GIS není hračka, jak využít mobilní GIS, co očekávat o DTM, že v přírodě i ve městě naleznete trauma body, že open source není anarchie, nebo že bezpilotní letoun má pilota, to jsou jen některé postřehy z letošního GIS OUTDOOR FÓRA ÚSTECKÉHO KRAJE.

e-government 20:10

aneb žijem si jak na zámku, ať to trvá věčně

MIKULOV • 4. - 5. 9. 2018

ODBORNÝ PARTNER

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

SPCSS
Státní pokladna
Centrum sdílených služeb

PLATINOVÝ PARTNER

CISCO

GENERÁLNÍ PARTNER

GORDIC®

... vše podstatné o eGovernmentu najdete v Mikulově.

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