Egovernment
elektronizace veřejné správy

Kyberbezpečnost

www.egovernment.cz

č. 2/2015

Úvodní slovo

Kyberbezpečnost nade vše

Kyberbezpečnost se stává zásadním pojmem a současně nadnárodní aktivitou. V rámci ochrany ekonomických, politických a dalších aktivit realizovaných prostřednictvím kyberprostoru jdou stranou i zcela odlišné ideologické cíle a postoje. Dokládá to skutečnost, že americký ministr zahraničí G. Kerry ve svém nedávném prohlášení uvádí, že USA a Čína se shodují na potřebě vytvořit pravidla pro chování států v kyberprostoru a zavázaly se na nich společně pracovat. Přitom problematika kyberbezpečnosti byla jedním ze zcela zásadních bodů společného jednání, jehož výsledkem prohlášení bylo.

Kyberbezpečnost je zcela neoddělitelnou součástí našeho přemýšlení o IT systémech, to je realita, kterou přinesl rozvoj a rozmach dostupnosti těchto systémů a jejich služeb. Ta neoddělitelnost je, jak vyplývá z diskuze našeho semináře popisovaného uvnitř magazínu, tak těsná, že se týká i systémů, o kterých si myslíme, že jsou od vnějšího světa oddělené.

Byť to jde proti duchu kyberprostoru, jednou z cest, jak čelit kyberútokům, je odstranění, či snížení anonymity pohybu v něm. Získat identitu těch, kteří zde realizují konkrétní úkony, lze (alespoň v tom úředním směru) zavedením jakéhosi elektronického občanského průkazu, určité elektronické identity. Právě o ní je druhá část magazínu.

Zvyšená kyberobrana a prokazatelná identita, spolu s kvalitní legislativou, mohou přispět k většímu bezpečí kyberprostoru. Toto bezpečí nebude nikdy úplné, neboť jak bylo řečeno na semináři, legislativa i náš zásah je vždy o krok pozadu za těmi, kteří chtějí útočit, ale jistou naději a uklidnění dávají. Své o tom věděly i čínská a americká vyjednávací delegace.

Ing. Michal Jirkovský
šéfredaktor

Nová adresa:

info◆com
komunikace informací

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

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: Bc. Klára Šmídová

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.

ISSS 2015

18. ROČNÍK KONFERENCE JE MINULOSTÍ

V kongresovém centru Aldis v Hradci Králové v úterý 14. dubna úspěšně skončil 18. ročník konference ISSS. Tuto prestižní akci, na níž se každoročně scházejí politické špičky, šéfové a výkonní úředníci státních i samosprávných orgánů, odborníci na informatizaci veřejné správy i vrcholní manažeři renomovaných firem, již podvanácté doprovodila mezinárodní konference V4DIS. Program začal již v neděli odpoledne diskusním setkáním v královéhradeckém planetáriu a pokračoval tradičním VIP večerem v Klicperově divadle. Během dvou dnů konference se uskutečnilo přes dvě stě přednášek, diskusí a jednání, ve výstavní části se představilo více než 100 dodavatelských firem a organizací a registrační listiny zaznamenaly 2365 účastníků.

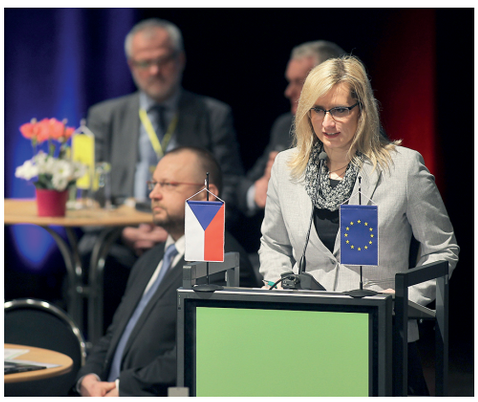
Záštitu konferenci letos poskytlo několik členů vlády včetně premiéra Bohuslava Sobotky, místopředsedy Pavla Bělobrádka, ministra vnitra Milana Chovance, ministryně pro místní rozvoj Karly Šlechtové a ministra zemědělství Mariana Jurečky, místopředsedové obou komor Parlamentu ČR – Přemysl Sobotka, místopředseda Senátu, který již řadu let zaštiťuje visegrádské setkání V4DIS, a Jan Bartošek, místopředseda Poslanecké sněmovny. Další záštity poskytli hejtman Královéhradeckého kraje Lubomír Franc a Asociace krajů ČR. Řada ze jmenovaných politiků se konference osobně zúčastnila, stejně jako desítky dalších zástupců státních institucí, poslanců a senátorů či zahraničních hostů.

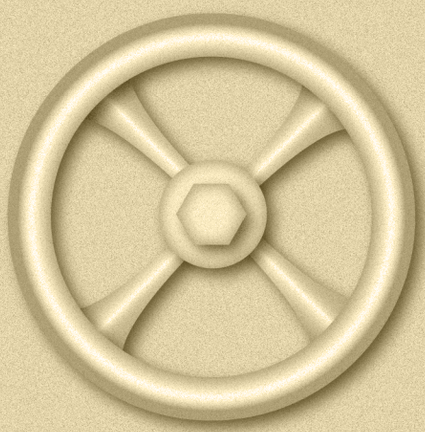
Přednášky a diskuse, které se během dvoudenního programu odehrály, se zaměřily nejen na hodnocení současného stavu e-governmentu a plánů do budoucnosti, ale i na veřejné investování v oblasti ICT, kybernetickou bezpečnost, rozšiřování internetové infrastruktury, elektronizaci zdravotnictví a řadu dalších oblastí. Důležitou součástí programu byly doprovodné akce, jako například zasedání Rady vlády pro informační společnost, setkání poslaneckých klubů, zasedání komisí Asociace krajů ČR, jednání zástupců akademické obce, poslanecké sněmovny, Technologické agentury ČR, Svazu průmyslu a odborníků zaměřené na podporu technického vzdělávání či setkání Sdružení tajemníků obecních a městských úřadů.

V programu konference jako obvykle nechybělo populární vyhlašování výsledků – ocenění Český zavináč, soutěže JuniorErb, Eurocrest, Zlatý erb, Biblioweb a Ceny ministra vnitra za přínos k rozvoji informační společnosti.

Více informací včetně kompletního archivu minulých ročníků, aktualit, audio- a videozáznamů z konference ISSS/V4DIS 2015 je k dispozici na stránkách:

www.isss.cz





Kyberbezpečnost – víc než zákon II

Magazín Egovernment navázal na svůj loňský seminář v Poslanecké sněmovně PČR, který se věnoval, tehdy připravovanému, zákonu o kyberbezpečnosti. Protože i nadále zákon o kyberbezpečnosti a případné "vyladění" jak samotného zákona, tak především jeho vnímání a plnění povinností, které z něj plynou, považujeme za zásadní téma, uspořádali jsme volné pokračování pod názvem KYBERBEZPEČNOST – VÍC NEŽ ZÁKON II. Na začátku června se tak v Poslanecké sněmovně PČR diskutovalo o tom, kdo jsou osoby dotčené tímto zákonem a jak přesně mají postupovat, aby byly v souladu nejen se samotným zákonem, ale i s příslušnými vyhláškami a nařízeními vlády, jak probíhá implementace zákona atp.

Celý seminář byl pořádán pod záštitou Ing. **Jana Bartoška**, místopředsedy PS PČR, Ing. **Dušana Navrátila**, ředitele NBÚ, a JUDr. **Jaroslava Strouhala**, náměstka ministra vnitra, kteří také obstarali úvodní prezentace k tématu.

Úvodním slovem Dušan Navrátil připomněl, jak se NBÚ stalo garantem kyberbezpečnosti, s jakými úkoly svoji práci začínalo a s jakými problémy se při jejich realizaci potýkalo.

Jaroslav Strouhal v rámci své prezentace podrobněji prezentoval dohledové centrum MV ČR pro provoz ICT systémů a kybernetickou bezpečnost, které má za cíl centralizovat a sjednotit provozní a bezpečnostní dohledy. V této souvislosti apeloval na vnímání kyberbezpečnosti jako zásadní téma. Uvedl: *„Státní instituce mají vazbu nejen mezi sebou navzájem, ale i na další, například evropské orgány. Proto MV ČR chápe kybernetický zákon v širším měřítku."*

Náměstek ředitele NBÚ Jaroslav Šmíd se věnoval problematice implementace zákona o kyberbezpečnosti. Přibližoval proces implementace zákona o kybernetické bezpečnosti, aktivity GovCERT.CZ, některé doposud identifikované kybernetické incidenty a samozřejmě se věnoval problematice kritické informační infrastruktury a významných informačních systémů.

Další část semináře pak byl postavena především na diskuzi, která na uvedené prezentace navazovala a které se krom vystupujících účastnili Ing. Jaroslav Šmíd, náměstek ředitele NBÚ, Ing. Miroslav Tůma, Ph.D., ředitel odboru kybernetické bezpečnosti a koordinace ICT, MV ČR, Bc. Dalibor Tatýrek, ředitel Elektrotechnického zkušebního ústavu, a Ondřej Šťáhlavský ze společnosti Fortinet.

Prezentace ze semináře jsou k dispozici na www.egovernment.cz/kyber. Na následujících stránkách si můžete přečíst podrobnější informace k jednotlivým prezentacím i průřez následnou diskuzí. Tato zpráva ze semináře v PS PČR je doplněna některými návaznými články, které téma kyberbezpečnosti kompletují.

Dušan Navrátil, NBÚ

Ředitel Národního bezpečnostního úřadu v úvodu svého vystoupení upozornil, že nediskutujeme o nějakých nahodilých útocích. Kyberbezpečnost je podle jeho slov souboj s plně organizovaným zločinem, který útočí na kontrétní instituce zcela záměrně a promyšleně. V této souvislosti uvedl, že zdaleka nesouhlasí s vyjádřením, které zaznělo v úvodu semináře, že nejsme, jako Česká republika, připraveni čelit takovýmto hrozbám. Podle jeho mínění jsme za čtyři roky, kdy NBÚ je garantem kyberbezpečnosti, výrazně pokročili a Česká republika je dnes ve fázi, kterou ji mohou závidět i vyspělé západní země. Dušan Navrátil upozornil, že ani v rámci EU, ale dokonce ani v rámci USA není nikde jinde k dispozici střechový zákon, který by se zabýval kritickou infrastrukturou. O této problematice se podle jeho slov všude jinde teprve diskutuje, a proto je možné tvrdit, že jsme pro ostatní státy inspirací.

Jak ředitel NBÚ dále zopakoval, jeho úřad se stal před čtyřmi lety garantem kyberbezpečnosti v ČR a zároveň dostal dva základní úkoly:

1. vybudovat Národní centrum kybernetické bezpečnosti v Brně, což se podařilo. NCKB má nyní 30 zaměstnanců a nyní probíhají jednání o navýšení rozpočtu i kapacit;

2. připravit zákon o kyberbezpečnosti. I když snahy o jeho realizaci byly velmi často označovány jako snahy o zavedení velkého bratra, podařilo se podle slov Dušana Navrátila tyto názory osvětou postupně vyvrátit. Zákon nakonec Parlamentem ČR prošel až nečekaně hladce, a to patrně i díky konsensu politické i odborné veřejnosti. V rámci jednání Parlamentu se tak nejednalo o politické, ale odborné téma a zákon bylo skutečně relativně snadno schválen. Pokud jde o samotné počátky, považuje Dušan Navrátil za určitou výhodu, že se začínalo tak říkajíc na zelené louce a nedošlo k žádným kompetenčním sporům. V tom byla naše velká výhoda oproti řadě ostatních států, kde se s nutností řešit kompetence v této oblasti potýkali.

Důležitým mezníkem byl, dle ředitele NBÚ rok 2012, kdy došlo k několika DDoS útokům. Nebyly ani tolik nebezpečné, jako spíše výrazně medializované, což přineslo tématu kyberbezpečnosti určitou publicitu. Zároveň se jednalo o velice dobrou příležitost k procvičení spolupráce státního, soukromého sektoru a akademické sféry, která je pro zajištění kyberbezpečnosti naprosto nezbytná. Postupem doby podle slov Dušana Navrátila útoků přibývalo, k čemuž přispělo i zhoršení bezpečnostní situace v Evropě. Typickým příkladem byla situace na Ukrajině, kde došlo ke kombinaci klasické formy války a kyberválky.

V současné době dle ředitele NBÚ evidujeme útoky, které je již možné považovat skutečně za vážné. Jedná se o různé formy SCADA útoků, tedy útoků na systémy, které řídí technologie a které nejsou vždy nutně propojené internetem, ale velice často „izolovanými" uzavřenými sítěmi. Jako příklad uvedl útok na ocelárnu v Německu, který zde vyřadil její výrobu z provozu.

V rámci ČR byla dle slov Dušana Navrátila letos přijata nová Národní strategie kybernetické bezpečnosti na roky 2015–20 a zároveň byl zpracován akční plán, který tuto strategii podrobněji rozpracovává. Jako velice důležité v této souvislosti hodnotí skutečnost, že pro Ministerstvo obrany vyvstal úkol, na němž se již pracuje, a to zřídit Národní síly kyberbezpečnosti.

IMPLEMENTACE ZKB
Jaroslav Šmíd, náměstek ředitele NBÚ

Náměstek ředitele NBÚ Jaroslav Šmíd se ve svém vystoupení věnoval především implementaci zákona o kybernetické bezpečnosti a základním časovým milníkům této implementace.

Uvedl, že zákon vstoupil v účinnost 1. 1. 2015 pod číslem 181/2014 Sb., přičemž je velice důležité, že vláda již schválila 45 prvních prvků kritické informační infrastruktury. Zároveň upozornil, že koncem roku 2014 vyšly ve Sbírce zákonů tři související prováděcí předpisy, a to:

- **č. 315 – novela nařízení vlády č. 432**, která stanovuje kritéria určování prvků kritické infrastruktury;
- **č. 316 – vyhláška o bezpečnostních opatřeních, tzv. standardizační vyhlášk**a, která popisuje, jakým způsobem mají být jednotlivé systémy zabezpečeny;
- **č. 317 – vyhláška o významných informačních systémech**, která obsahuje jako přílohu seznam 92 IS, které jsou považovány za významné ve smyslu zákona.

V další části svého vystoupení se Jaroslav Šmíd věnoval současnému dění v GovCERT. Jak řekl, je to technická část Národního centra kybernetické bezpečnosti (NCKB) a pracuje už od roku 2014 na vybudování svého technického zázemí, kterým je například databáze, která zahrnuje data od potencionálních uživatelů služeb GovCERT (kontaktní osoby, informace o jednotlivých incidentech atp.). Zároveň GovCERT zabezpečuje osvětovou a vzdělávací činnost a samozřejmě spolupráci a kontakty se zahraničními subjekty v oblasti výměny informací o potencionálních hrozbách kyberútoků. Spolupráce je rovněž navázána se společností Microsoft, jedná se především o monitoring IP adres z našeho adresního prostoru, které jsou potencionálně zahrnuty do bootnetů a útoků. Jak náměstek Šmíd uvedl, jsou tato data analyzována a provozovatelé příslušných počítačů jsou následně informováni o patrně špatném zabezpečení na jejich straně.

Jaroslav Šmíd dále uvedl přehled nejvýznamnějších incidentů, které proběhly v tomto roce:

1. Český statistický úřad

DDoS – dne 30. 1. 2015 NCKB obdrželo od Českého statistického úřadu (ČSÚ) informace týkající se probíhajících a opakovaných DDoS útoků na webový server czso.cz. První útok na server byl zaznamenán 15. 1. 2015 a trval přibližně dvě hodiny. Další útoky následovaly 19. 1., 23. 1., 24. 1. a 27. 1. Na základě obdržených informací bylo zjištěno, že se pravděpodobně nejednalo o cílený útok, který měl za úkol jakkoliv poškodit volby probíhající v nadcházejícím víkendu (31. 1.–1. 2. 2015), ale jednalo se o chybu v nastavení čínského DNS serveru. Pravděpodobně se jednalo o chybný překlad seznamu předem definovaných domén (torrenty, facebook, twitter) na náhodné IP adresy. Tyto dotazy následně provozem zahlcovaly server czso.cz. Na základě těchto zjištění NCKB doporučilo určitá řešení. Ta pracovníci ČSÚ konzultovali se správci dotčených serverů, ale vzhledem ke krátké době nezasahovali do nastavení těchto serverů. V současnosti probíhají zátěžové a penetrační testy na novém webu.

2. Turla (Uroburos, Snake, Carbon)

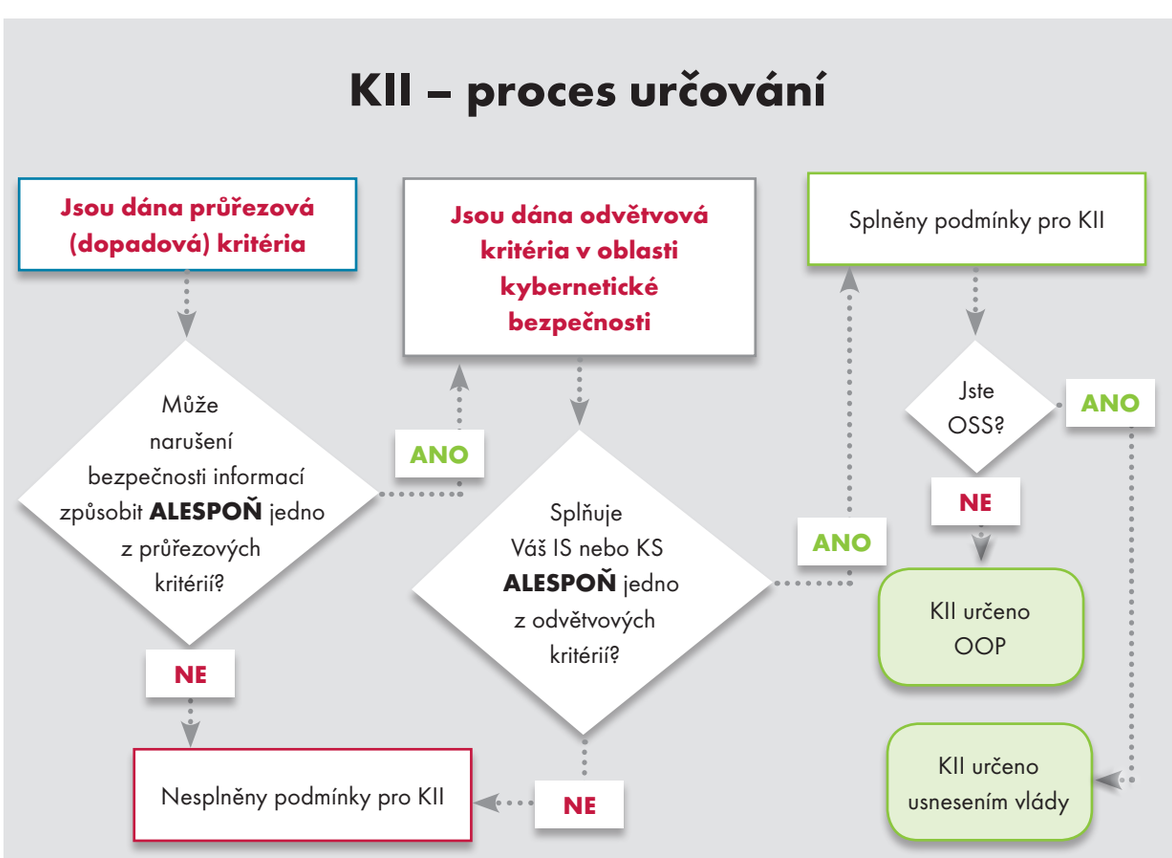
Od CERT-EU a bezpečnostní společnosti BAE Systems obdrželo NCKB dokument týkající se kompromitovaných IP adres a domén. Mezi nimi byla i česká doména hostovaná v Rusku. Dne 3. 3. NCKB získalo od BAE Systems doplňující informace, že incident Shortener-Bug attack je ve skutečnosti další instancí špionážního malware Turla (Uroburos, Snake, Carbon). Na základě tohoto zjištění došlo ke sloučení s incidentem #1657. V průběhu řešení incidentu požádalo jednotlivá ministerstva o kontrolu síťových logů, zda některá ze stanic v jejich rozsahu nekomunikovala se škodlivými webovými stránkami. Ze 14-ti oslovených ministerstev (23. 2.) NCKB doposud obdrželo vyjádření od 8 z nich. Z osmi konečných výsledků hledání bylo nalezeno 9 potenciálně infikovaných stanic. Náměstek Šmíd považuje za nutné upozornit na skutečnost, že tři ministerstva ze 14-ti doposud nikdy nereagovala na výzvy NCKB.

3. Zranitelnost FREAK

Po zveřejnění informací o zranitelnosti FREAK v protokolu TLS/SSL zahájilo NCKB ve spolupráci s národním CSIRT týmem skenování serverů státních institucí, které jsou vůči této chybě v zabezpečení zranitelné. V mezidobí obdrželo anonymní e-mail, který na tuto skutečnost upozorňoval. Poté byl rozšířen sken o další zranitelnosti. V souvislosti se zranitelností FREAK bylo nalezeno 107 potenciálně zranitelných serverů a varováno 73 státních institucí.

KRITICKÁ INFORMAČNÍ INFRASTRUKTURA

Jaroslav Šmíd se dále podrobněji věnoval problematice kritické informační infrastruktury (KII). Jak uvedl, jedná se o komplex informačních a komunikačních systémů, které naplňují stanovená průřezová kritéria a odvětvová kritéria v oblasti kybernetické bezpečnosti a jejich nefunkčnost by mohla způsobit závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.



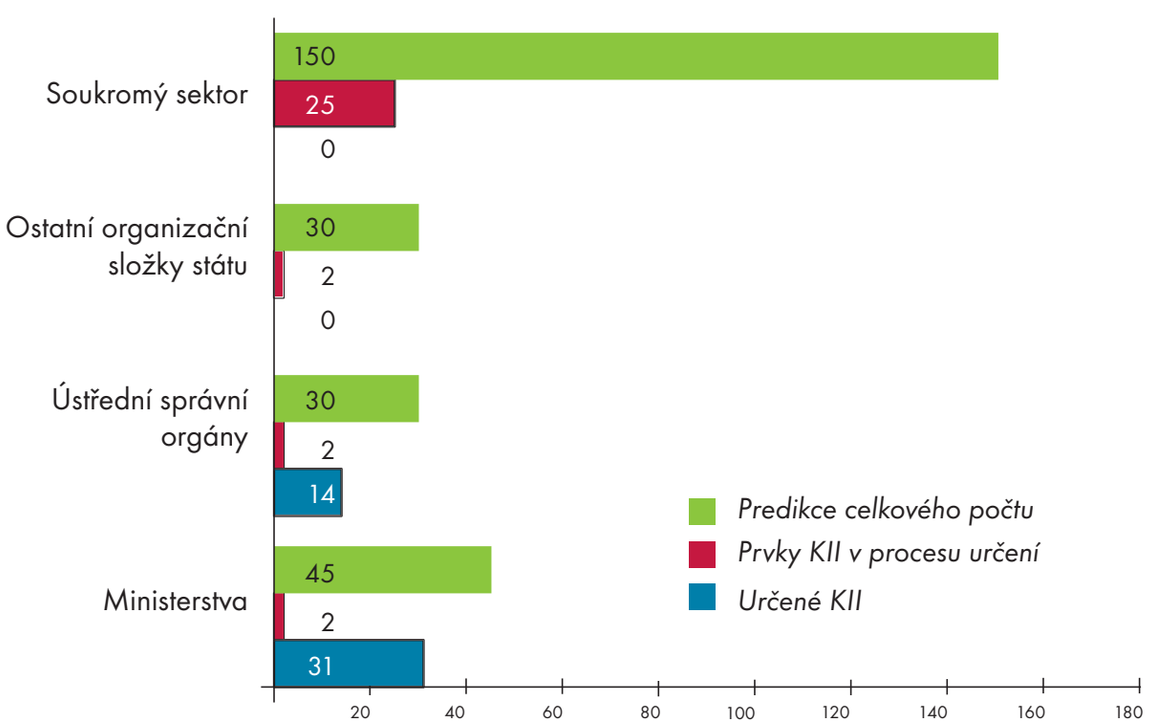
V této souvislosti Jaroslav Šmíd ukázal návod, jak určit, zda konkrétní IS patří do systému kritické informační infrastruktury či nikoli.

Proces určování prvků KII probíhá podle jeho slov ve třech vlnách. První vlna již proběhla. Týkala se ministertev a ústředních orgánů a jejím výstupem bylo určení 45 prvků KII. Druhá a třetí vlna probíhají nyní. Zatímco druhá se věnuje organizačním složkám státu, ta třetí je zaměřena na soukromé subjekty.

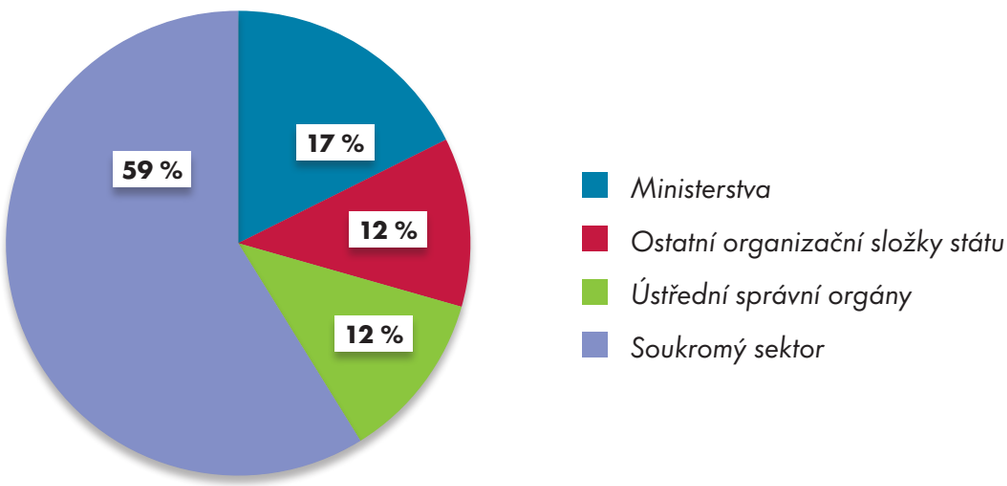
Představu o tom, kolik, respektive jaké poměry prvků KII by měly být mezi soukromými subjekty a státním sektorem, ukazují následující grafy.

Jak Jaroslav Šmíd upozornil, určení prvků KII nemusí jednotliví správci naplňovat okamžitě, neboť pro tuto povinnost platí roční lhůta.

Predikce a současný stav určování KII prvků v daných oblastech



Předpokládaný poměr prvků KII v daných oblastech (predikce)



VÝZNAMNÉ INFORMAČNÍ SYTÉMY (VIS)

Jsou podle slov náměstka Šmída systémy, které mohou být provozovány veřejnou správou, nikoli soukromým sektorem. Tyto systémy sice nesplňují kritéria krizového zákona (tzv. průřezová a odvětvová kritéria), ale jedná se přitom o systémy, jejichž nečinnost by mohla mít pro fungování státu katastrofální důsledky. VIS naplňují kritéria, která jsou dána vyhláškou č. 317/2014 Sb. a její součástí je rovněž seznam těchto IS. Proces doplňování tohoto seznamu je stále živý, další systémy tedy do něj mohou být zahrnuty, naopak některé z těchto systémů budou patrně přesunuty do KII. I v případě VIS náměstek Šmíd prezentoval schéma, dle kterého je možné určit, zda konkrétní IS je možné zařadit mezi významné.

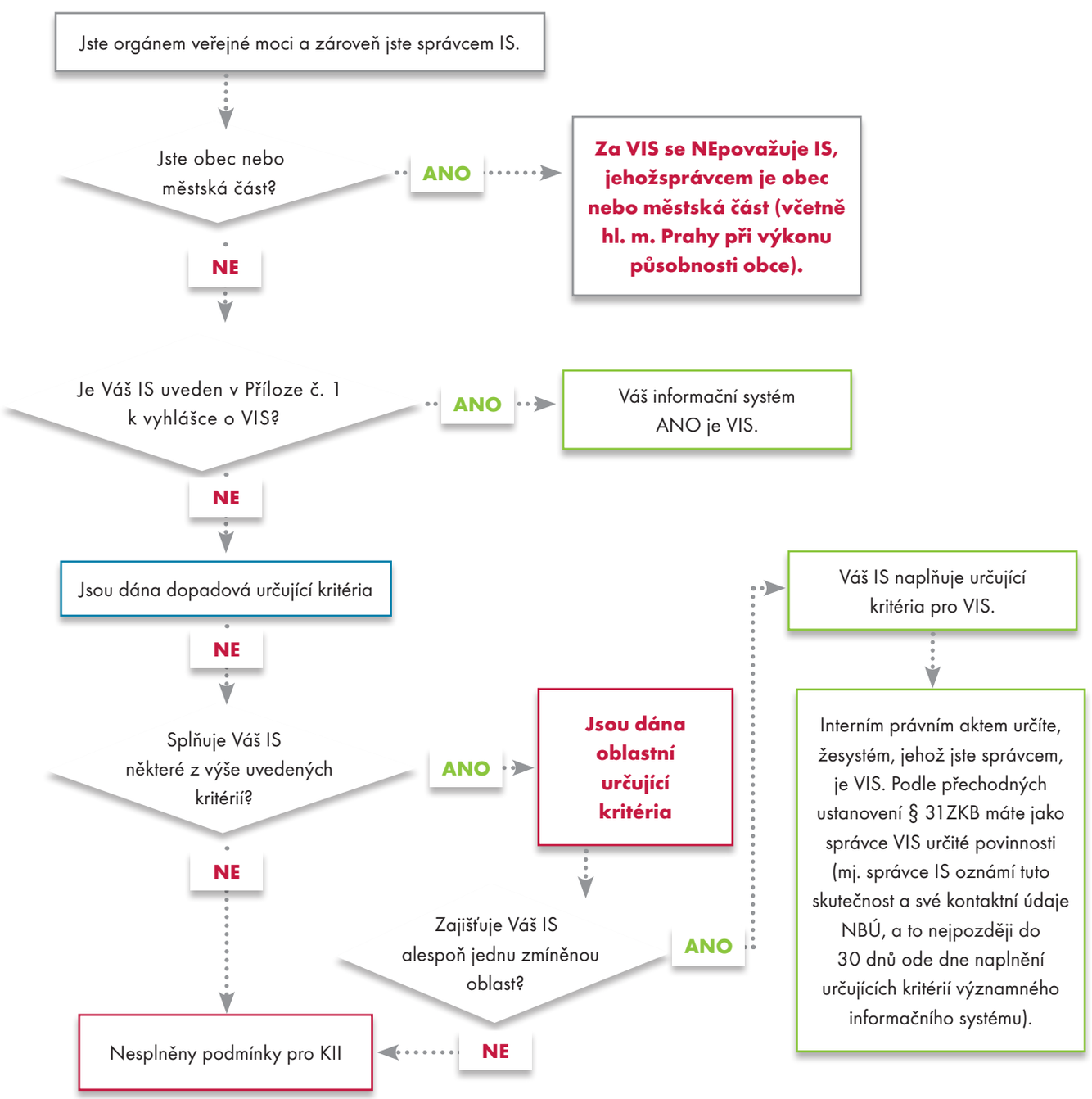
Jak dále náměstek Šmíd zdůraznil, NCKB poskytuje podporu při posuzování IS, a to buď na pracovišti NCKB nebo u žadatele. Společně projdou popis konkrétního systému a podle něj se posuzuje zařazení na příslušný seznam. Jak uvedl, v současné době je 113 systémů v kategorii VIS, tedy včetně nově identifikovaných. Jaroslav Šmíd upozornil, že většina těchto systémů je v případě krajů obdobná, bylo by tedy vhodné, aby se zde postupovalo koordinovaně. Nyní podle jeho slov probíhá s kraji debata, a to především na úrovni AKČR.

Bude vytvořena příloha „Informační koncepce", která bude obsahovat tabulku ISVS totožnou s „Informační koncepcí", kde bude u vybraných ISVS označeno, že je VIS, a ke všem ISVS bude přiložen výstup z excelu (vytvořeného NBÚ), kterým se určuje, zda ISVS je, či není VIS. Tímto bude možné doložit, že se zástupci krajů posuzováním zabývali. Případné rozpory v názoru kontrolního orgánu (státní dozor NBÚ) budou řešeny jako změna. Od okamžiku zjištění, že je provozovaný informační systém VIS, je třeba do 30 dnů nahlásit na NBÚ správce tohoto VIS.

V závěru svého vystoupení náměstek Šmíd shrnul, jaké jsou základní služby NBÚ/NCKB v oblasti KII a VIS. Jedná se především o určování prvků kritické informační infrastruktury, podporu při posuzování významných informačních systémů, metodickou podporu související s problematikou kybernetické bezpečnosti, a to v legislativně-právní oblasti, v oblasti managementu kybernetické bezpečnosti a v technické oblasti. V neposlední řadě se pak jedná o provádění auditů kybernetické bezpečnosti v rámci kontrol dodržování zákona.

Kromě toho NCKB spolupracuje s dalšími institucemi i firmami na mezinárodní i národní úrovni, a to především za účelem vzdělávání v oblasti problematiky zákona o kybernetické bezpečnosti, přípravě podpůrných materiálů, pořádání osvětových akcí atp.

Schéma určování VIS



Egovernment

elektronizace veřejné správy

Vše o elektronizaci veřejné správy - srozumitelně a zdarma:

www.egovernment.cz

LEX UNO ORE OMNES ALLOQUITUR

Jaroslav Strouhal, náměstek ministra vnitra pro řízení sekce informačních a komunikačních technologií

Náměstek Strouhal v úvodu svého vystoupení řekl, že by skutečně chtěl, aby zákon hovořil ke všem stejně, jak říká název jeho příspěvku. Tedy abychom si zákon o kyberbezpečnosti všichni, kterých se týká, vykládali stejně. Jak řekl, on sám jej čte jako normu, která vychází z toho nejlepšího, co bylo k dispozici, a to i proto, že základem pro úvahy o kyberbezpečnosti byly britské standardy. Protože v rámci semináře bylo úvodními vystoupeními na adresu kyberbezpečnosti řečeno téměř vše, chtěl by svou prezentací pouze rozptýlit určité obavy, které ve vztahu k MV ČR vnímá.

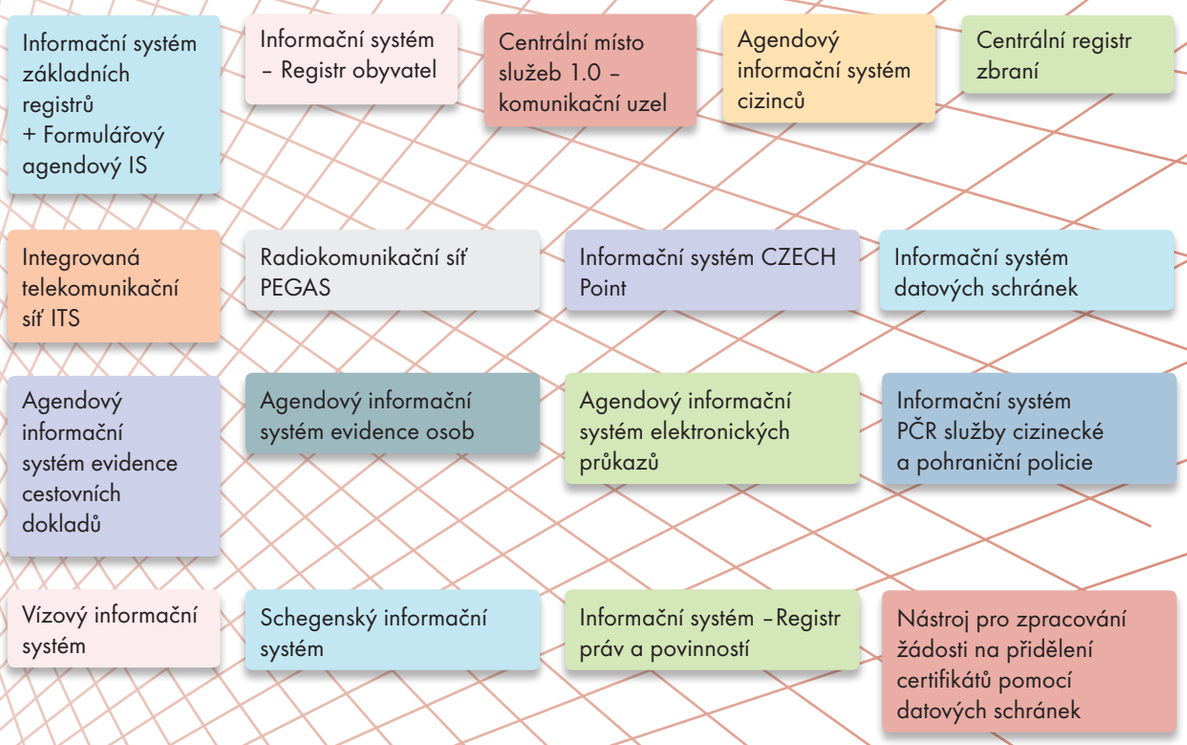
Náměstek Strouhal připomněl, že nikoli software, nikoli hardware, ale naše data jsou tím nejcennějším v oblasti IT. Pokud ta ztratíme, většinou je téměř nemožné je plně nahradit. Proto se je musíme naučit skutečně účinně chránit.

Jak řekl, žijeme zatím v klidu, přičemž by chtěl zdůraznit ono ZATÍM. Rozhodně se totiž nejedná o setrvalý stav. Například MV již zaznamenalo kybernetický útok proti jednomu z archivů. Tento útok sice nebyl dokonán, neboť systémy jej včas zaregistrovaly a zastavily, ale je zřejmé, že takových útoků bude rozhodně přibývat.

Podle náměstka Strouhala je rozhodně škoda zániku Ministerstva informatiky. Toto ministerstvo mělo totiž dobrou filozofii – zastřešovat ICT v rámci státního sektrou, což bylo něco, co nám do jisté míry v zahraničí záviděli. Nyní je tedy gestorem v oblasti informatiky MV ČR, které se podle jeho slov snaží naplňovat očekávání a potřeby. Ministr vnitra je zároveň předsedou RVIS, což je v současné době podle Jaroslava Strouhala velice reprezentativní orgán a důležité fórum pro diskuzi.

Většina systémů e-governmentu je v současné chvíli zařazena do kategorie kritické infrastruktury, případně do kategorie významných informačních systémů. Před námi je budování a rozvíjení elektronické identity a ISZR. Přitom je podstatné, že státní instituce nemají vazbu jen mezi sebou navzájem, ale jsou dnes provázány i se zahraničními subjekty, a tak kyberbezpečnost není pouze lokální záležitostí, ale skutečně mezinárodní spoluprací. MV ČR šlo v tomto směru, podle mínění Jaroslava Strouhala, příkladem při přípravě svých systémů na aplikaci zákona o kyberbezpečnosti. V této souvislosti prezentoval náměstek Strouhal kritickou informační infrastrukturu v rámci MV ČR.

Kritická informační infrastruktura v rámci MV



Významnými informačními systémy v rámci MV ČR jsou:

- informační systém Policie ČR;
- rejstřík politických stran;
- Portál veřejné správy;
- Ústřední evidence nabytí (pozbytí) státního občanství ČR.

Významnými IS určenými MV ČR (nejdříve k 1. 7. 2015) jsou: GINIS; EKIS.

V závěru svého vystoupení uvedl Jaroslav Strouhal, že MV ČR nyní buduje tzv. dohledové centrum pro provoz ICT systémů a kybernetickou bezpečnost (SOCCR – Security Operation Center for Continuous Reliability). Jak řekl, cílem MV ČR je centralizovat a sjednotit provozní a bezpečnostní dohledy prostřednictvím vybudování bezpečnostního dohledového centra SOCCR (Security Operational Centre for Cyber Reliability) a provozního dohledového centra NOC (Network Operation Centre).

Diskuze

Na prezentaci ředitele NBÚ Dušana Navrátila, jeho náměstka Jaroslava Šmída a náměstka ministra vnitra Jaroslava Strouhala navazovala diskuze. Do té se dále zapojili Jan Binder, zastupující místopředsedu Poslanecké sněmovny Parlamentu ČR Jana Bartoška, Miroslav Tůma, ředitel odboru kybernetické bezpečnosti a koordinace informačních a komunikačních technologií MV ČR, Dalibor Tatýrek, ředitel Elektrotechnického zkušebního ústavu, a Ondřej Šťáhlavský ze společnosti Fortinet.

Ondřej Šťáhlavský

Právě Ondřej Šťáhlavský rozproudil diskuzi. Řekl, že na základě svých více než 15 tiletých zkušeností má určité připomínky k tomu, co zaznělo v úvodu. Především podle něj působily přednášky ukolébavě a mohly vyvolat dojem, že situace v ČR je ideální.

Určitě je podle jeho mínění velice dobré, že máme zákon o kybernetické bezpečnosti (ZKB), protože řada zemí okolo nás jej vůbec nemá. Problém však spatřuje v tom, že zákon, nebo jeho výkon není kvalitně podpořen v rámci rozpočtu. Zároveň má pocit, že vyhláška, která má definovat kritické systémy, je psána tak, že do ní řada systémů, které by zde měly být, nebyla vůbec zařazena. a to pravděpodobně právě z finančního důvodu. Ondřej Šťáhlavský upozornil, že naší výhodou je to, že doposud nejsme zemí, která by byla primárním cílem útoků. To ssebou ale nese nebezpečí absence tlaku na kvalitní zabezpečení. Proto je velice důležité věnovat se v této oblasti osvětě a propagaci, protože situace v oblasti kyberbezpečnosti je docela kritická a dynamika vývoje je taková, že legislativa jí skutečně nemůže stačit.

Dušan Navrátil

Na vystoupení O. Šťáhlavského samozřejmě reagoval předseda NBÚ Dušan Navrátil. Podle jeho mínění nehrály v přípravách jak samotného zákona, tak souvisejících vyhlášek roli peníze. Chápe, že firmy, které se této problematice věnují, jsou nespokojeny třeba právě proto, že zatím byly vynechány obce. Jak ale upozornil, při definování kritické infrastruktury vychází NBÚ z krizového zákona, který je dán, a z nařízení vlády, které určuje kritickou infrastrukturu. Na základě konkrétních kritérií pak hledá kritickou informační infrastrukturu, tedy informační systémy, které tato kritéria splňují a jsou pro tuto infrastrukturu stěžejní. Zatím bylo ve veřejné a státní správě identifikováno 45 systémů, ale počítá se s tím, že se bude posuzovat další balík systémů.

Jak Dušan Navrátil upozornil, identifikace se týkala veřejné správy. V oblasti soukromé sféry, jsme dle jeho slov teprve na začátku. První opatření veřejné povahy budou realizována v červenci a bude se jednat o ČEZ, ČEPS, banky a providery.

Obce byly z posuzování KII zatím vyjmuty záměrně, neboť jak Dušan Navrátil upozornil, bylo cílem začínat s menším počtem prvků a KII se bude dále postupně rozšiřovat. Pravděpodobně tedy dojde k novelizaci, která by zahrnovala i větší obce, ale to není tématem tohoto roku.

Z pohledu kritérií KII se tedy nehovoří o penězích. Ty jsou záležitostí jednotlivých rezortů, které nyní mají jeden rok Dušan Navrátil zároveň připustil, že jsou určitá bílá místa. Tím zásadním je podle něj zdravotnictví, v němž by do KII měla být například zahrnuta až nemocnice s počtem lůžek nad 2500, ale taková skutečně v ČR není. Ptá se tedy, proč v KII byla právě tato definice. Druhé bílé místo jsou chemičky. Ty v kritické infrastruktuře vůbec nejsou, což je dle jeho mínění hodně zvláštní, protože většinou se jedná o továrny, které jsou přímo ve středu města a jejich provoz znamená určité ohrožení. Třetí krizovou oblastí je plyn, který je sice zahrnut v evropské kritické infrastruktuře, ale ne v české. Ředitel NBÚ v této souvislosti uvedl, že bude připraven doporučující materiál pro bezpečnostní radu státu, respektive pro vládu tak, aby v této oblasti došlo k potřebným změnám.

Miroslav Tůma

Další diskuze se týkala především toho, jak moc se problematika KII týká či netýká obcí. Miroslav Tůma za MV ČR uvedl, že systémy EG, které spadají do kritické infrastruktury, budou letos postupně upravovány tak, aby byly v souladu se zákonem a zabezpečeny proti kyberútokům. Na základě těchto kroků budou vznikat jednotlivé příručky pro dané uživatele, tedy i pro obce tak, aby se chovaly kyberbezpečně. To znamená, že MV ČR bude podle jeho slov ovlivňovat obce z hlediska uživatelského a bude je proškolovat, aby nedocházelo k bezpečnostním problémům. Upozornil ale, že MV nebude ovlivňovat obce v rámci jejich systémů, tento tlak se bude týkat pouze systémů EG,tj. datových schránek, Czech POINTů, základních registrů.

Zároveň Miroslav Tůma uvedl, že se připravují komplexní projekty, které nezahrnují pouze kyberbezpečnost, ale i rozvoj a zabezpečení systémů. Konkrétně se jedná o okruhovou výzvu ve strategickém rámci rozvoje veřejné správy v implementačním cíli 3, kde je jasně definován okruh kyberbezpečnosti. Miroslav Tůma předpokládá, že právě pod tímto okruhem vznikne výzva umožňující podat projekt na úpravu systémů v souvislosti s kyberbezpečností. Tato úprava by podle něj ale měla být širšího charakteru.

Dalibor Tatýrek

Do diskuze se zapojil rovněž ředitel EZÚ Dalibor Tatýrek, který osvětlil, proč se vlastně EZÚ tohoto semináře účastní. Jak řekl, nejen chytré telefony, ale i naše domácnosti se díky elektronickým přístrojům stávají chytřejší a chytřejší, a i když nás to možná překvapí, řada domácí elektroniky (televize, lednice,...) se dá zneužít v rámci kyberútoků. Aby představil EZÚ, uvedl, že ke kyberbezpečnosti se dostali přes produktovou bezpečnost. Úřad zároveň testuje zdravotnické prostředky i oblast energetiky. Kromě zkoušení výrobků se EZÚ věnuje i systémům kvality. Jak Dalibor Tatýrek uvedl, do kyberbezpečnosti tedy nahlíží jak z produktové strany, tak z pohledu osobních dat i kvality procesů. EZÚ rovněž nabízí určitý preaudit, tedy kontrolu, jak je daná organizace připravena na ZKB i související normy.

Jan V. Binder

Asistent Jana Bartoška, Jan V. Binder, do debaty přispěl svojí zkušeností ze semináře Českého institutu manažerů bezpečnostní úseků, na němž byla prezentována zkušenost z německé obce, která si

pro zjištění stavu svého zabezpečení cíleně najala hackerský útok. Protože k napadení a ovládnutí zdánlivě zabezpečených systémů došlo velice snadno, je tato zkušenost pomocí prezentací předávána ostatním. Jan Binder upozornil, že považuje za velice důležitý postoj oné německé obce, která se výsledek testu nesnažila ututlat, ale naopak z něj vytěžit poučení pro ostatní.

Ondřej Štáhlavský z Fortinetu takovou aktivitu rozhodně přivítal a uvedl, že právě v tomto směru by viděl potřebu větší aktivity NBÚ. Medializace těchto problémů je v ČR podle jeho mínění velice špatná a kvůli tomu si ti, kteří tvoří zákony a normy, vůbec neuvědomují, jaká je realita. V této souvislosti uvedl, že zatímco v osobních počítačích systém Windows XP pravděpodobně byl už vyměněn za novější, naprostá většina průmyslových systémů běží na Windows XP ve verzi první bez service packů. Ti, kteří jsou zodpovědní za bezpečnost, mají podle Ondřeje Šťáhlavského mylný pocit bezpečí jenom proto, že se jedná o „odříznuté" systémy, které nejsou přímo připojeny k internetu. To podle něj ale není žádnou překážkou a není možné spoléhat na to, že se díky přenosu dat pomocí USB klíčů nějaký vir do systému nevnese.

Zdá se, že u nás skutečně neřešíme problémy kyberbezpečnosti, protože jsme se zatím skutečně nestali cílem útoků, ale kdy k nim dojede, je pouze otázkou času.

Ředitel NBÚ Dušan Navrátil v reakci na slova O. Šťáhlavského upozornil, že mluvíme-li nyní o ZKB, hovoříme o ochraně kritické infrastruktury. Jak již bylo řečeno, postupujeme cestou pomalého rozšiřování prvků, které do této infrastruktury patří. Pokud jde o odpovědnost státu, je samozřejmě otázkou, jak má být velká, a i zákon v této souvislosti hovoří o tzv. individuální zodpovědnosti jednotlivých správců systémů. Stát podle Dušana Navrátila pouze pomáhá a koordinuje.

Ředitele NBÚ v jeho názorech podpořil i Dalibor Tatýrek, ředitel EZÚ, když potvrdil, že problematika kyberbezpečnosti neleží výhradně na státu, ale ten by jí měl vlastně jen pomáhat. EZÚ se podle jeho slov účastní řady pracovních skupin na úrovni Evropy i celého světa. Zde probíhají diskuze o těch největších rizicích a o tom, jak je minimalizovat. Ale je pak na každé organizaci a v jejím komerčním zájmu, aby ji nikdo nenapadl, a to je podle Dalibora Tatýrka riziko i zájem každého podnikatele. Motivem pro řádnou ochranu není represe, ale úspěšnost podnikání.

Miroslav Tůma z MV ČR v této souvislosti uvedl, že dnes není problém technicky realizovat jakákoliv opatření, pokud máme dostatek finančních prostředků. Reálně se podle něj jedná vždy o kompromis mezi možností investovat do bezpečnostního systému a procesní realizací, jde tedy o jakousi kombinaci. Když jsou k dispozici prostředky provést technické řešení, umíme to, když nejsou prostředky, musíme realizovat procesní věci,zde se však naráží velice často na diskuze, jak a s jakou kapacitou.

Používání vlastních zařízení – situace ve státní a veřejné správě

To bylo otázka, která rozproudila velice protichůdné názory. Na jedné straně byly argumety, které hovoří o tom, že nemůžeme zakazovat pracovníkům používání jejich vlastních zařízení. Proti tomu byly názory, které říkaly, že nelze spoléhat na to, že by byla síť tak dobře zabezpečena, aby jí při pravidelném používání jiných zařízení nepořízených organizací (míněno tablet, chytrý telefon ...) nehrozilo narušení. Nicméně ve výsledku se obě skupiny shodly v tom, že je to trend současnosti a že především nastupující generace zaměstnanců považuje využívání vlastního zařízení i v pracovním procesu za naprosto samozřejmé.

V další části se diskutující věnovali tomu, jak na pozadí ZKB vypadá otázka bezpečnostních incidentů v realitě. Miroslav Tůma popsal, že ze strany NBÚ přicházejí jednotlivá hlášení. MV ČR na jejich základě prověřuje své systémy a hlásí zpět NBÚ, na co narazilo. Tato komunikace je podle jeho slov poměrně intenzivní. Stejně tak, když MV ČR zaznamenalo kyberútok na své systémy, okamžitě podalo NCKB hlášení. NCKB velmi rychle žádalo další informace a podklady tak, aby mohlo situaci analyzovat a informovat další subjekty.

Jaroslav Šmíd

Náměstek ředitele NBÚ Jaroslav Šmíd doplnil, že NCKB má už svoji databázi incidentů. Bezprostředně po nahlášení napadení dojde k porovnání, zda se jedná o záležitost, kterou již známe a existuje na ni nějaké konkrétní řešení. Pokud ne, dochází k dalšímu dotazování, analýze incidentu a informaci ostatním potencionálním obětem takového útoku. To je preventivní část. Na ni navazuje hledání minimalizace dopadů případného útoku.

Ředitel NBÚ Dušan Navrátil upřesnil, že zatím je převážná část těchto informací tzv. zvenku. Naše kritická infrastruktura je čerstvě definována a subjekty mají nyní rok lhůty, aby tuto reportační povinnost plnily, proto je předpoklad, že domácích hlášení bude postupně přibývat. KCNB připravuje veřejný a neveřejný web. Veřejný web bude uvádět obecně známé informace o útocích a varování, které je možné zveřejnit. Na neveřejný web bude zaheslovaný vstup prioritně pro KII a VIS tak, aby dostaly aktuální informace o čerstvých varováních.

V závěru semináře se diskutovalo především o penězích. Jak vyplynulo z dotazů, řada vedoucích odborů IT na úřadech má velice často potíže prosadit u vedení úřadu vyšší investice do zabezpečení. Především pak ve chvíli, kdy například obce nejsou do KII zahrnuty. Představitelé NBÚ v této souvislosti uvedli, že úřad nemůže nikomu nařizovat více, než je dáno zákonem. Zároveň ale je nutno si uvědomit, že ze zákona je v podstatě povinností statutárního zástupce zajistit kvalitní zabezpečení. Každý musí zajistit naplňování zákona a nelze říci, že nejsou prostředky, a měl by zvážit, zda místo části cyklostezky neprovede řádné zabezpečení. Nicméně obě strany se v závěru shodly v tom, že by bylo velice vhodné zpracovat nějaké případové studie a že by tomuto tématu měla být vytvořena větší míra propagace.

-MJ-

Kybernetická bezpečnost se týká nás všech

Pojmy, jako kyberbezpečnost, kyberkriminalita a kybernetické útoky, stále ještě mnozí vnímají spíše jako ze scénáře amerických filmů. Hrozba narušení bezpečnosti je ale stále reálnější. S rychlým rozvojem IT technologií vznikají i stále důmyslnější způsoby kyberzločinu a frekvence útoku hackerů se zvyšuje.

V České republice začal od první ledna letošního roku nově platit zákon o kybernetické bezpečnosti, jehož cílem je zajistit bezpečnost kritické informační infrastruktury státu a systémů, které zpracovávají a uchovávají osobní data občanů. Na to, jakým reálným hrozbám jsou tyto instituce vystaveny a v čem může pomoci zákon o kybernetické bezpečnosti, jsme se ptali **Ondřeje Šťáhlavského, regionálního ředitele pro oblast střední a východní Evropy ve společnosti Fortinet**, která je předním světovým dodavatelem výkonných síťových bezpečnostních řešení.

O kybernetické bezpečnosti a kyberprostoru vůbec se hovoří poměrně často, přesto je to pro mnohé stále dost abstraktní pojem. Mohl byste na úvod trochu přiblížit, co se pod tímto označením skrývá?

Kybernetický prostor můžeme úplně nejjednodušeji označit jako prostor vytvářený počítači a digitálními technologiemi. Pro mnoho lidí je kyberprostor synonymem pro internet a vzniká pak mylná představa, že pokud nemám svůj systém připojený k internetu, nemohu se stát obětí kyberzločinu. To ale rozhodně neplatí. Do kyberprostoru spadají všechna zařízení kontrolovaná počítačovým programem, tedy například tiskárny, průmyslové stroje, lékařské přístroje či domácí elektronika, a stejně tak i řídicí systémy ve všech odvětvích. Hrozby se napříč těmito systémy mohou šířit prakticky jakkoli, například prostřednictvím fyzických nosičů, jako jsou flashdisky, SD karty a podobně.

V čem spočívá největší riziko kybernetického zločinu a proč dochází k tak masovému rozvoji této oblasti?

S pokračujícím rozvojem informačních technologií se stále větší část našeho života přesouvá do kyberprostoru. S cílem zefektivnit jednotlivé činnosti vznikají stále propojenější systémy, a to nejen v rámci firem a velkých institucí, ale i v našich domácnostech. Trend inteligentních zařízení a automatizovaných systémů nám na jednu stranu usnadňuje život, na stranu druhou potenciálně zvyšuje riziko úniku a ztráty dat. Zatímco dříve představovala nejvyšší hrozbu pro únik informací e-mailová komunikace a USB nosiče zaměstnanců a dostatečnou ochranu proti škod-

livým kódům představoval firewall, dnes se musí IT specialisté potýkat s daleko sofistikovanějšími hrozbami, které navíc není snadné na první pohled identifikovat. Kyberprostor odstraňuje bariéry v podobě času a vzdálenosti, navíc zajišťuje anonymitu, z čehož kriminální skupiny ve velké míře těží.

Organizace již dnes používají poměrně pokročilé systémy ochrany, protože jsou si vědomy rizik souvisejících s únikem či ztrátou dat. Je tedy skutečně nutné ukotvovat zajištění bezpečnostních opatření zákonem?

To, že bezpečnostní opatření existují, bohužel ještě neznamená, že firmy dělají vše pro to, aby jich využily k ochraně svých systémů. Problém vidím v nedostatečné informovanosti, celá řada osob v řídících funkcích si v plné míře neuvědomuje potenciální bezpečnostní rizika a především jejich dopady. 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, ještě závažnější jsou pak možnosti škod fyzických, způsobených potenciálním útokem na průmyslové a řídicí systémy. Rozumný zákon vymezující podmínky pro zajištění kritické informační infrastruktury státu může nejen pomoci organizacím uvědomit si své nedostatky v oblasti bezpečnosti a adekvátně na ně reagovat, ale zároveň zvýšit ochranu samotných občanů, kteří nemají možnost ovlivnit, jak jsou informační a řídicí systémy řízeny a spravovány.

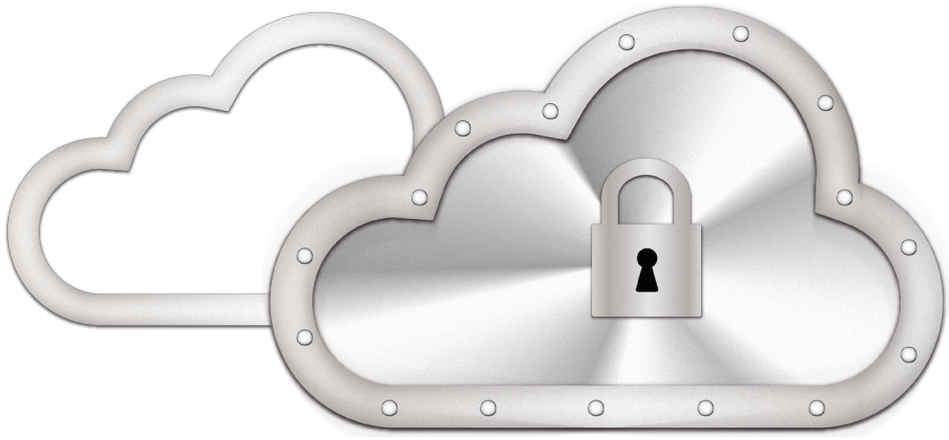
Častým argumentem kritiků je v souvislosti se zákonem o kybernetické bezpečnosti nadměrná administrativní zátěž...

Tyto a další argumenty jen dokládají zcela chybný přístup řady vedoucích osob k zajištění bezpečnosti vlastní organizace. Bezpečnost by měla být standardem, samozřejmostí. V případě, že jsem zodpovědný za systém, který řídí například distribuci energetických médií, musím v plné míře zodpovídat za jeho funkčnost a s tím samozřejmě zabezpečení úzce souvisí. Organizace by měly zajistit bezpečnost ne proto, že jim to nařizuje zákon, ale protože je to v jejich vlastním zájmu a v zájmu jejich zákazníků. Odpovědné osoby by tedy k zákonu o kybernetické bezpečnosti neměly přistupovat jako k nevyhnutelné administrativní zátěži, ale ve spolupráci s odborníky by měly aktivně přemýšlet nad tím, jak zajistit, aby systém, za který jsou zodpovědné, byl co nejbezpečnější.

Kde by měly organizace při zavádění bezpečnostních opatření začít?

Základním kamenem informační bezpečnosti kterékoliv firmy, nejen těch, kterých se kybernetický zákon týká, by měla být kvalitně zpracovaná bezpečnostní politika. To znamená, že osoba, případně tým zodpovědný za řízení bezpečnosti, by měl mít úplné informace o všech systémech a datech, kterými daná firma či organizace disponuje. Na základě těchto informací pak lze posoudit relevantní rizika, určit, jakou formou je eliminovat, ať už procesně či technologicky, a také stanovit cílový stav systémů, respektive úroveň jejich zabezpečení. Ta by měla zohledňovat veškerá kritéria vyplývající z již zmíněné bezpečnostní politiky. Bohužel takto systémový přístup je vidět ve velmi málo firmách či organizacích. Většinou bývá zabezpečení řešeno ad hoc, buď v rámci rozpočtu, který zbyl po vybudování ostatní informační infrastruktury, nebo v reakci na konkrétní bezpečnostní incident. Takové řešení může sice organizaci krátkodobě vytrhnout trn z paty, ale za cenu komplikovanější infrastruktury, jejíž správa je složitější a ve výsledku i finančně náročnější. Samotný nákup technologie, byť pokročilé, totiž neznamená automaticky vyšší bezpečnost. Ta přichází až se správnou implementací a schopností takovou technologii řídit a především vyhodnocovat informace, které poskytuje. Tím se dostáváme zpět k tomu, že pokud firma či organizace pochopí bezpečnostní rizika spojená s kybernetickým prostorem a jejich reálné dopady, může již od začátku postupovat při implementaci bezpečnostních řešení systémově, v souladu s bezpečnostní politikou šitou na míru vlastní organizaci, a ve výsledku tak získat spolehlivou zabezpečenou infrastrukturu, která bude oporou pro veškerou činnost organizace, nikoli bariérou.

FORTINET®



V cloudu od Microsoftu jsou i informační systémy veřejné správy v bezpečí

Cybersecurity je téma tohoto čísla magazínu Egovernment. V našem článku shrneme, co znamená provozovat informační systémy, včetně ISVS a AISů, v cloudovém prostředí Microsoft tak, aby to bylo v souladu s bezpečnostními požadavky stanovenými legislativou. Porovnáme výhodnost multitenantních cloudových služeb s provozem aplikací ve vlastním datovém centru a zkusíme se zamyslet nad dalšími kroky vlády v oblasti sdílených služeb.

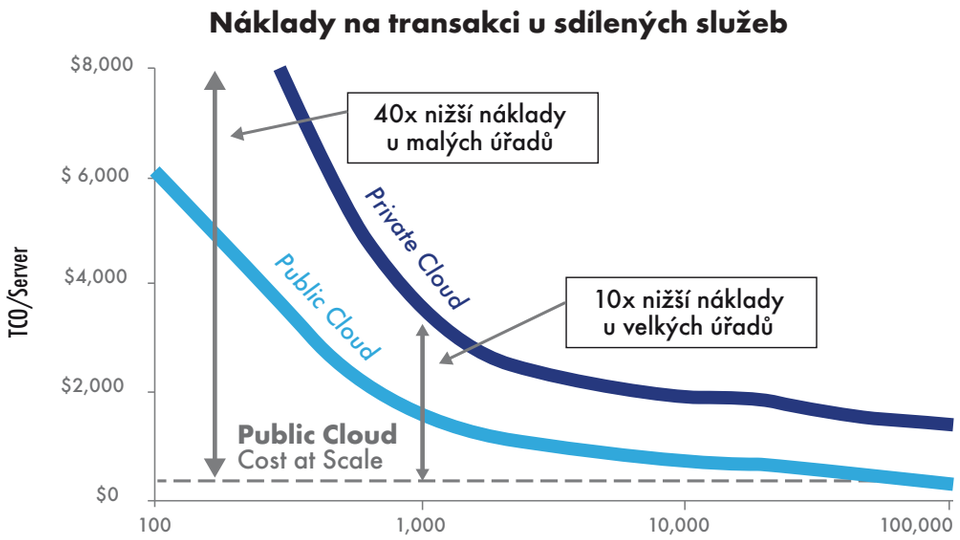
VÝHODNOST MULTITENANTNÍCH SLUŽEB

V čem vlastně spočívá základní podstata ekonomické výhodnosti multitenantních cloudových služeb oproti individuálně provozovaným aplikacím? Většina z vás určitě ví, co to je multitenantní aplikace, ale malé zopakování nám neuškodí. Zkusme si pojem vysvětlit na příkladu poštovního serveru. Pokud si provozujete poštovní server sami, jsou s jeho pořízením, implementací a provozem spojeny náklady. Jeho zakoupení, včetně hardware, je první náklad.

Jaké jsou náklady na jeho implementaci? Server musíte někde umístit, potřebujete tedy alokovat část datového centra (pokud jej máte), ve kterém server připojíte k elektřině, kterou spotřebovává. Datové centrum musíte chladit, což je opět náklad. Software poštovního serveru musí někdo na server instalovat – opět náklad. Instalovaný server musí splňovat bezpečnostní požadavky, které jej chrání před internetovými útoky, jako je např. zneužití neoprávněným uživatelem k rozesílání nevyžádané pošty – opět náklad. O poštovní server se někdo musí pravidelně starat, provádět instalaci nových verzí, reagovat na aktuální hrozby a útoky a provádět i zálohování celého systému poštovního serveru. Výpadek poštovního serveru bude ošetřen jeho „zdvojením" a bude provozován redundantně – opět náklad. Na konci životního cyklu serveru je nutné jej nechat ekologicky zlikvidovat – tedy opět náklady. **Jak to vypadá, pokud poštovní server využíváte jako službu z cloudového prostředí Microsoft Office 365?** Velmi jednoduše, prostě jen platíte určitou částku za jednoho uživatele měsíčně a žádné z výše uvedených nákladů na provoz poštovního serveru neřešíte. Jedinou výjimkou je implementace, protože poštovní server jako službu z Office 365 musíte integrovat do svého interního prostředí tak, že uživatelé vůbec nepoznají, zda je poštovní server ve Vašem datovém centru, nebo ho využíváte z Office 365.

A jak je to s multitenantností? Poštovní server poskytovaný jako služba je multitenantní aplikace. To znamená, že z jedné instalace je poskytován více organizacím současně. Microsoft jako provozovatel takového multitenantního poštovního serveru má samozřejmě s jeho implementací, provozem atd. stejné typy nákladů jako Vy, když si poštovní server provozujete sami – také musíme nakoupit „železo", platit zaměstnance, kteří se o něj starají, elektřinu atd. Zásadní rozdíl ale je v tom, že Microsoft provozuje multitenantně statisíce serverů a variabilní náklady se tím pádem rozpouštějí ne u jedné organizace, ale právě u řádově statisíců organizací. Proto je provoz multitenantní služby obvykle levnější, než když provozuji sám pro sebe jeden poštovní server.

Názorně je rozdíl v nákladech mezi lokálně provozovaným datovým centrem (Private Cloud) a komerčním cloudem (Public Cloud) vidět na následujícím grafu.



Zdroj: „Cloud Economics" - Dokument pro IT ne-profesionály, Studie Univerzity Milán / Benátky, Prof. Federico Etro

CLOUD A ZÁKON O KYBERNETICKÉ BEZPEČNOSTI (ZKB)

V případě zahrnutí cloudových služeb do svého systému řízení bezpečnosti informací (tzv. ISMS) musí povinné osoby zohlednit požadavky §7 vyhlášky o kybernetické bezpečnosti č. 316/2014 Sb. To se může zdát na první pohled obtížné, ačkoliv skutečnost může přinést naopak zjednodušení: otázkou je, zda cloudový dodavatel zavedl ISO 27001:2013 a má k dispozici příslušnou dokumentaci zahrnující řízení rizik a auditní zprávy. Vyjasníli jsme dotazem u Národního bezpečnostního úřadu, jaký rozsah dokumentace je nutné předat povinné osobě a zahrnout v rámci smluvních podmínek. Poskytnutá dokumentace pak povinné osobě fakticky zjednoduší úsilí vypracovat celkovou bezpečnostní dokumentaci dle přílohy č. 4 k uvedené vyhlášce, případně zjednoduší získání vlastní certifikace ISO 27001, viz následující schéma.

Soulad cloudových služeb dle ZKB a vyhl. č. 316/2014 Sb. § 7 – Stanovení bezpečnostních požadavků pro dodavatele (povinných osob)

Významné informační systémy (VIS) – § 7 odst. (1)

Zavedení pravidel pro dodavatele pro potřeby řízení bezpečnosti informací
Dokumentace smlouvou, jejíž součástí je ustanovení o bezpečnosti informací

Microsoft splňuje „Podmínkami pro služby online" (Online Services Terms), oddíl „Podmínky ochrany osobních údajů a zabezpečení" – součást písemné smlouvy.

Kritická informační infrastruktura (KII) – § 7 odst. (2) b

Smlouva zahrnuje způsoby a úrovně bezp. opatření a vztah odpovědnosti za jejich zavedení a kontrolu

Microsoft: „OST" obsahuje seznam opatření a závazek cert. ISO 27001

Microsoft dá k dispozici povinné osobě:
1. Svoji „Bezpečnostní politiku"
2. ISO 27001 certifikát (online výpis)
3. ISO 27001 prohlášení o aplikovatelnosti (výčet opatření)
4. ISO 27001 auditní zprávu, a na vyžádání SOC 1 & 2 auditní zprávy

Povinná osoba zapracuje do svoji bezpečnostní politiky.

Kritická informační infrastruktura (KII) – § 7 odst. (2) a, c

Pravidelné hodnocení rizik služeb (příp. i před uzavřením smlouvy); Kontroly zavedených bezp. opatření

Microsoft:
1. Poskytne dokumentaci řízení rizik v rozsahu schváleném Národním bezpečnostním úřadem
2. Hodnocení nezávislého auditora metodiky řízení rizik cloudu Microsoftu
3. Kontrola zavedených bezpečnostních opatření auditními zprávami ISO 27001 a dále SOC 1 & 2 Type II

Povinná osoba zapracuje do svojí dokumentace dle Přílohy č. 4 vyhlášky.

TRAGÉDIE OBECNÍ PASTVINY VE STÁTNÍM CLOUDU

Zatím jsme se věnovali pohledu na cloudové služby. Vzhledem ke stávajícím strategiím veřejné správy (např. Strategický rámec rozvoje veřejné správy) je jisté, že stát bude využívání sdílených služeb subjekty veřejné správy koordinovat (iniciativa „G-Cloud“) a některé sdílené služby bude i sám pro sebe provozovat (např. Státní pokladna, Centrum sdílených služeb, ČP OZ atd.). Problematika G-Cloudu je velmi široké a komplexní téma a rozsah tohoto článku nám neumožní věnovat se mu dostatečně detailně. Podívejme se trochu z nadhledu na poskytování sdílených služeb v datových centrech, které si provozuje stát sám, případně prostřednictvím některé své organizace nebo státního podniku. **Co je možným rizikem neefektivního poskytování sdílených služeb v datových centrech provozovaných státem?** Zkusme se podívat za hranice. V některých státech plánují poskytovat sdílené služby ze státem provozovaného datového centra pro subjekty státní správy zdarma. Zdarma, protože bylo vybudováno za evropské dotace. Současně proto, že není jednoduché, aby stát sám sobě nabízel datové centrum a chtěl za něj sám od sebe platit za jeho užívání tak, aby to bylo v souladu se zákonem o veřejných zakázkách. Jak takové poskytování „zdarma“ obvykle končí? Abychom nevymýšleli vymyšlené, podívejme se na „tragédii obecní pastviny“, kterou budete možná znát ze studia ekonomie. Jedná se o to, že sdílená obecní pastvina, jejíž spotřebovávání je pro členy obce zdarma, je postupně přeplněna ovcemi. Každý občan obce je motivován k tomu, aby si pořídil více ovcí, vždyť přece pastva pro ně je zdarma, tak proč toho nevyužít. Co se ale stane? Ovce nakonec nemají co spásat, protože kapacita pastviny tak velké množství ovcí neuživí. Pokud to převedeme do podoby „tragédie sdíleného datového centra“, je to velmi podobné. Pokud budu jeho služby dávat zdarma, jen na základě schváleného projektu, brzo výkon a kapacitu datového centra rozdám a neefektivně spotřebuji. Každý úřad si raději alokuje o (pro jistotu) pár serverů více (když je to zdarma) – aniž by je reálně potřeboval. Za co se neplatí přímým spotřebitelem, bývá obvykle spotřebováno nehospodárně. Postup státu, kdy takto „zdarma rozdá“ služby datového centra, způsobuje i nesystémový zásah do tržního prostředí v této oblasti.

JAKÝ JE ZÁVĚR? V CLOUDU OD MICROSOFTU LZE PROVOZOVAT I ISVS

Cloudové služby společnosti Microsoft lze implementovat v souladu s požadavky legislativy, zejména z hlediska ochrany osobních údajů, provozu ISVS a souladu se ZKB. Z hlediska celkových nákladů za pětileté období (TCO) je výhodné přejít na multitenantní cloudovou verzi dnes využívaných informačních systémů.

Václav Koudele a Zdeněk Jiříček,
Microsoft s.r.o.

Microsoft

Kdo má plnit zákon?

V dnešní informační společnosti jsou informace považovány za hlavní zdroj ekonomického, sociálního a kulturního pokroku. Měřítkem úrovně informační společnosti není úroveň hardwaru, ale rozsah, kvalita, relevance a dostupnost informací a informačních služeb. Narůstající užití informačních a komunikačních technologií v činnostech organizací, firem i jednotlivců pak vyžaduje, aby při zpracování, přenosu, ukládání a opětovném využití objemů dat nedocházelo ke ztrátě životně důležitých údajů, ke vzniku chyb, kompromitaci nebo neoprávněné modifikaci dat. To vše a mnohem více má za úkol řešit kybernetická bezpečnost.

Svět kybernetické bezpečnosti se vyvíjí velmi dynamicky, pořád je to ale ještě svět, který nesmírně ovlivňují lidé, a právě u nich je potřeba začít. Rizika úniku a zneužití informací hrozí zejména zevnitř organizace. Podle výzkumů jsou lidé nejrizikovějším faktorem kompromitace, modifikace, vyzrazení, úniku a zničení citlivých dat a informací v organizaci (způsobují až 80 % kybernetických incidentů). Rizikovost tohoto faktoru ještě více umocňuje například rozmach BYOD. Většina nezabezpečených míst není zřejmá, o to užitečnější jsou pak rady profesionálů s bohatými zkušenostmi.

Problémem jsou ale také bezpečnostní chyby (zranitelnosti) v samotných zařízeních a jejich SW. Mezi ty nejaktuálnější lze zařadit například:

- kritickou zranitelnost v operačním systému iOS a Mac OS X dovolující útočníkům snadno získat přístup k citlivým uživatelským datům, např. k uloženým heslům pro jednotlivé služby;
- snadné zneužití mobilních telefonů z produkce společnosti Samsung – ovládání některých funkcí smartphonu na dálku a sledování jeho majitele;
- kritickou bezpečnostní chybu v programu Flash Player od společnosti Adobe;
- zadní vrátka do operačního systému Windows a webový prohlížeč Internet Explorer (v reakci na ně uvolněny aktualizace s označním kritické).

To vše se potom samozřejmě odráží také v průzkumech. Jeden z nich byl realizován agenturou Ponemon Institute, která oslovila téměř dva tisíce vedoucích manažerů a IT pracovníků s otázkami, které se týkaly toho, jaké hrozby pro IT vnímají jako největší. Výsledky ukázaly, že podle manažerů jsou největší hrozbou pro IT bezpečnost třetí strany, například dodavatelé cloudových služeb (49 %). IT pracovníci nejčastěji uváděli nezabezpečené webové aplikace (57 %) a nezodpovědné interní uživatele (56 %).

Jaké má taková situace řešení?

Když si v lepším případě vedení organizací uvědomí všechna hrozící rizika, často je jejich reakcí nákup různých zařízení a SW nástrojů a řešení renomovaných firem, které jim jsou prezentovány jako„všelék" na kybernetickou bezpečnost. Nelze říci, že tyto kroky nenapomáhají zlepšovat kybernetickou bezpečnost, naopak – jedná se o nezbytnou součást celkového řešení. V první řadě je ale nutné provést audit vlastních digitálních aktiv,

jehož výsledkem by měla být důkladná analýza rizik, která mohou nastat, a soubor opatření, jak na ně reagovat. K pořízení kvalitních technologií a nástrojů řešících kybernetickou bezpečnost a jejich správnému zapojení a provozování je v celkovém řešení naprosto nezbytné vytvoření a především dodržování systematické bezpečnostní strategie a kvalifikace a připravenost bezpečnostního týmu. Jakékoliv jednorázové investice nevedou k systematické bezpečnostní strategii, jen vyčerpávají rozpočet a způsobují provozní komplikace.

Další část řešení představuje implementace požadavků nového zákona č. 181/2014 Sb. (zákona o kybernetické bezpečnosti) a s ním souvisejících právních prováděcích předpisů (převážně vyhlášky č. 316/2014 Sb.) a platného mezinárodního standardu ISO/IEC 27001:2013. Ty do svých požadavků zapracovaly best practices v oblasti kybernetické bezpečnosti a jsou průběžně aktualizovány, což je především v této oblasti naprostou nezbytností.

Co se týče zákona o kybernetické bezpečnosti, jistě se nabízí otázka – kdo má plnit?

Na ni odpovídá samotný zákon, a to v § 3. Související a zajímavější otázkou je – měl by plnit jen ten, kdo má plnit? Vždyť nejen stát, ale i organizace samotné mohou čelit a také čelí problémům spojeným se ztrátou životně důležitých údajů, vznikem chyb, kompromitací nebo neoprávněnou modifikací dat. Ani u subjektů spadajících pod zákon o kybernetické bezpečnosti navíc nejde ani tak o to, že nesoulad může být potrestán pokutou, ale hlavně o skutečnost, že se tím značně minimalizuje riziko samotného kybernetického incidentu. A ten může být v důsledku mnohem horší než stotisícová pokuta. Pro organizaci by mohl být zcela likvidační a nejen v případě správců významných informačních systémů mít navíc také nedozírné následky pro všechny osoby, s jejichž daty se nakládá. Mimo to k samotným požadavkům zákona patří také povinnost v nezbytné míře zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatelů pro uvedené systémy. Správci tak musí promítnout požadavky ZKB do výběrových řízení jak na dodavatele služeb, tak i zboží. A který dodavatel splní tyto požadavky lépe než ten, jenž sám plní požadavky zákona?

Mezinárodní standard ISO/IEC 27001:2013, pro který je vypracován i jeho český ekvivalent ČSN ISO/IEC 27001:2014 a jehož propojení se zákonem o kybernetické bezpečnosti zmiňuje v § 29 samotný zákon, lze vnímat jako výchozí bod jak pro naplnění požadavků zákona, tak i pro kybernetickou bezpečnost jako takovou. Normu tvoří požadavky na ISMS, nebo-li systém řízení bezpečnosti informací. Do těla normy je včleněn dobře známý PDCA cyklus, protože ISMS je potřeba nejen zavést a provozovat, ale i monitorovat, průběžně vyhodnocovat jeho účinnost a neustále zlepšovat. Standard evokuje těchto pět funkcí:

- identifikace (řízení aktiv, posouzení rizik, navázání na cíle, zúčastněné strany, vedení a aktivity organizace, definice procesů, postupů a politik);
- ochrana (kontrola přístupu, povědomí a školení, bezpečnost dat, údržba a opravy komponent, dodržování procesů a postupů k ochraně informací, řízení technických bezpečnostních prvků);
- detekce (neustálé sledování bezpečnosti, nastavení detekčních procesů);
- reakce (plánování reakcí, řízení komunikace, provádění analýzy, případná zmírnění dopadu incidentu a jeho eliminace, zlepšování reakčních činností);
- obnova (provádění a udržování obnovovacích procesů a postupů).

Důležitou součástí jak požadavků normy, tak vyhlášky o kybernetické bezpečnosti jsou požadavky na bezpečnostní role. Bezpečnostní role garant aktiva znamená totéž, co v mezinárodním standardu vlastník aktiva, odpovědnosti jsou pro ně definovány stejně – odpovídají za rozvoj, použití a bezpečnost aktiva.

- **Roli manažera** kybernetické bezpečnosti, tedy osoby odpovědné za systém řízení bezpečnosti informací, by měl zastávat interní zaměstnanec organizace, protože jinak si lze velmi těžko představit správné nastavení a řízení ISMS, navázání na vrcholové vedení organizace, na její cíle a strategie. A bez toho bude systém nefunkční a spíše než přínos bude znamenat přítěž.
- **Role architekta**, tedy osoby zajišťující návrh a implementaci bezpečnostních opatření, by mohla být zajištěna i externě, ale pouze při úzce navázané spolupráci s manažerem kybernetické bezpečnosti a garanty (vlastníky) aktiv.
- **Roli auditora**, tedy osoby provádějící audit kybernetické bezpečnosti, by měla vykonávat osoba odborně způsobilá (praxe s prováděním auditů kybernetické bezpečnosti po dobu nejméně tří let) a výkon této role by měl být nestranný a striktně oddělený od výkonu všech ostatních bezpečnostních rolí. To vše evokuje jediné – tato role by měla být zajištěna externě.

ezú elektrotechnický zkušební ústav

Konečné řešení

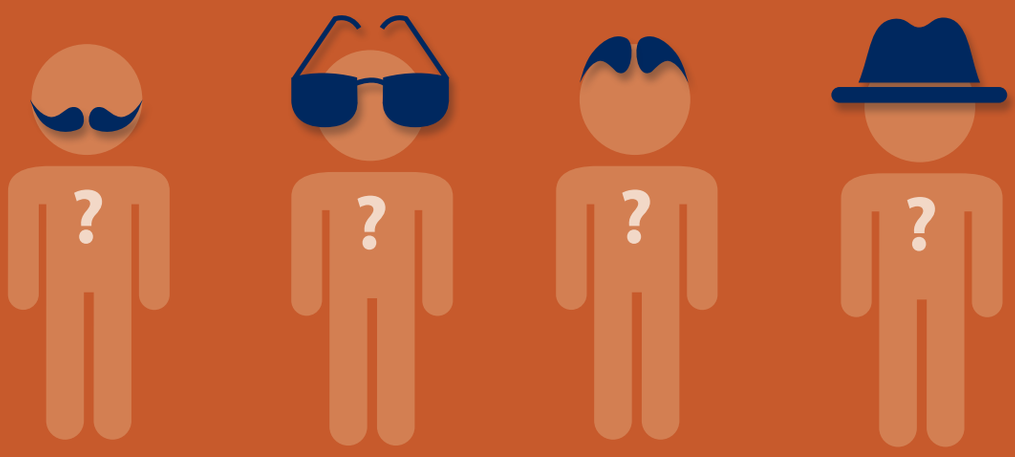
Cesta k co možná nejvyšší úrovni kybernetického zabezpečení je cestou složitou. Je nutné dívat se na kybernetickou bezpečnost z mnoha různých úhlů pohledu a řešit ji komplexně. K tomu samotné pořízení a instalování technologií nestačí. Pro účinnou ochranu je důležité pochopit, jaké informace organizace má a jakou hodnotu pro ni znamenají. Je také zásadní uvědomit si cíle a reálné fungování organizace. Jen tak lze navrhnout opravdu účinné a efektivní řešení kybernetické bezpečnosti. Cílem není pouze jeho zavedení, ale také zaručená dlouhodobá funkčnost a rozvoj. Právě proto musí být v pravidelných intervalech ověřováno a certifikováno. Mělo by být schopné reagovat na změny organizace i jejího okolí. Jediným způsobem, kterým lze takového stavu dosáhnout, je zapojení vrcholového managementu organizace a pravidelné školení zaměstnanců o kybernetické bezpečnosti. Vedlejším důsledkem je pak snížení nákladů ICT a celkově vyšší efektivita procesů.

My nabízíme řešení a pomocnou ruku ve vaší snaze vydat se touto cestou.

Bc. Michal Hager

NAŠE ŘEŠENÍ

- Situační analýza kybernetické bezpečnosti
- Certifikace kybernetické bezpečnosti
  - Základní certifikát kybernetické bezpečnosti (Essential Certificate of Cybersecurity)
  - Rozšířený certifikát kybernetické bezpečnosti (Enhanced Certificate of Cybersecurity)
  - Certifikát nejvyšší úrovně kybernetické bezpečnosti (Top-level Certificate of Cybersecurity)
- Školení kybernetické bezpečnosti
- Osobní certifikace
  - Manažer kybernetické bezpečnosti
  - Architekt kybernetické bezpečnosti
  - Auditor kybernetické bezpečnosti
- Zajištění role auditora kybernetické bezpečnosti podle zákona č. 181/2014 Sb.
- Implementace, zajištění a instalace potřebných technologií ve spolupráci s partnery



Elektronická identita občana aneb Nestačí jen datovky?

Píše se rok 2015, už nechodíme do banky, nechodíme si předem koupit do pokladny lístky do kina, divadla, stejně tak letenky, jízdenky. To vše zvládáme po internetu. Chodíme však dál na úřady, k volbám, napoprvé i do té banky jsme museli zajít. Na vše nestačí naše datová schránka, tedy pokud ji vůbec máme zřízenu. Zkrátka, naše identita v kyberprostoru není plnohodnotná. To vše se má změnit, mimo jiné i díky nařízení Evropského parlamentu a Rady EU č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu. Všimněme si, že se jedná o nařízení, tj. státy musí konat.

Toto pochopili i někteří zákonodárci, a tak dne 22. dubna 2015 v Poslanecké sněmovně Parlamentu České republiky proběhl seminář iniciovaný, svolaný a zaštítěný místopředsedou Poslanecké sněmovny panem Janem Bartoškem. Ve své úvodní řeči uvedl, že již více než rok spolupracuje s hlavním architektem e-governmentu Ondřejem Felixem a že se shodli, že je třeba dát občanovi univerzální a uznatelný nástroj na prokazování totožnosti v kyberprostoru. Uvedl několik příkladů, kde je třeba takové identity, a to například hráčská karta, kvůli regulaci hazardu, přístupy do informačních portálů státní správy a cílově i distanční volby, tj. volby občanů po internetu.

Dalšími diskutujícími byli Robert Piffl z Ministerstva vnitra ČR, Vilém Kahoun z České správy sociálního zabezpečení, Zdeněk Jiříček z Microsoftu, Pavel Kolář z ČSOB, Tomáš Hebelka z ATOS IT, Richard Gürlich, právník, Richard Kaucký z ICT Unie, Jakub Pacanda z VirPR, Jiří Peterka, nezávislý novinář, Jan Vojtěch Binder, asistent Jana Bartoška, a moderátor semináře. Zapojili se i hosté z publika. Byl také citován pan Tomáš Svoboda, předseda ICT komise KDU-ČSL, který sice nakonec nedorazil, ale již v roce 1996 na Invexu prohlásil: „Stát by měl pro rozvoj digitální ekonomiky udělat totéž, co dělá v tradičním světě – zprostředkovat obchodním partnerům vzájemnou důvěryhodnou identifikaci." A tomu se přesně věnuje eIDAS.

Dle eIDAS má vzniknout státem garantovaná identita občana, která bude mít široké užití, a to nejen vůči orgánům státní moci, ale i vůči komerční subjektům a dle nařízení EU má platnost a důvěryhodnost napříč všemi členskými státy EU. Takže občan ČR může důvěryhodně komunikovat se systémem v Belgii. Může si půjčit vozidlo nebo se přihlásit pojišťovně apod. To, že užití takové identity je široké a že od ní každý očekává trochu něco jiného, bylo zřejmé už v úvodu.

Vyzvali jsme totiž každého účastníka, aby se dopředu krátce zamyslel, čím je pro něj eIDAS. Získali jsme tyto názory:

Jan Bartošek:
„Žijeme v době kartové a internetové. Stát by měl dát občanovi jeden jediný doklad, který v sobě sloučí všechny potřebné funkce pro identifikaci v reálném i kybernetickém prostoru."

Vilém Kahoun:
„Bude-li existovat plošně zavedená a vládou podporovaná e-identifikace občana, můžeme získat ve státě tolik kontrolorů „černých mezd", kolik je pojištěnců v registrech ČSSZ."

Jaroslav Strouhal:
„eIDAS? Už aby to bylo."

Pavel Kolář:
„Spolupráce bankovního sektoru s veřejnou správou na rozvoji e-governmentu při naplňování konceptu bezhotovostní ekonomiky přináší dlouhodobě pozitivní výsledky. Proto se přímo nabízí ji nyní zaměřit i na oblast elektronické identity občana v návaznosti na naplňování nařízení Rady a Parlamentu EU č. 910/2014."

Zdeněk Jiříček:
„Potřebujeme elektronickou identitu fyzické osoby snadno využitelnou pro elektronické transakce ve veřejném i soukromém sektoru, s výběrem rolí, v níž osoba vystupuje, uznávanou v ČR i v zahraničí, a s ochranou soukromí proti neoprávněnému profilování."

Tomáš Hebelka:
„Pevně věřím, že i v ČR jako v jiných zemích EU se podaří prosadit čip na občanském průkazu jako hlavní nosič elektronické identity občana. Bude to průlom v dalším rozvoji e-governmentu a také širší propojení veřejné správy a komerčního sektoru."

Richard Kaucký:
„Elektronická identita pro občany, ne pro stát!"

Jakub Pacanda:
„Práce a povinnosti na net, zábava do reálu!"

Robert Piffl:
„Digitální Evropa realitou."

Jan Vojtěch Binder:
„Až bude i-EDA „at home", tak to bude teprve pravý Home Office."

Diskuse musela být nakonec ukončena kvůli vypršení času a stále bylo o čem diskutovat. Proto se již dnes připravuje na září pokračování této akce. Jsme zvědavi zejména na pokrok, který za tu dobu udělá Ministerstvo vnitra ČR a Poslanecká sněmovna.

-JVB-

Univerzální zaklínadlo jménem „eIDAS“

Dne 23. července 2014 bylo vydáno nařízení Evropského parlamentu a Evropské rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. Ač průběžné pracovní verze nařízení eIDAS byly známy již několik měsíců a byly živě diskutovány, až finálním schválením se nařízení stalo závazným, a tudíž mu nikdo nemůže uniknout. O to víc se spustila živá debata o dopadech tohoto nařízení na české právní prostředí, resp. o příležitostech, které nařízení vytváří v každodenním životě. Pojďme si na úvod alespoň stručně zrekapitulovat, o čem ono nařízení eIDAS vlastně je.

Oblasti působnosti, negativní působnost a cíle

Nařízení eIDAS pokrývá ve stručnosti následující oblasti působnosti:

- podmínky uznávání prostředků pro elektronickou identifikaci v rámci oznámeného (či „notifikovaného“) systému elektronické identifikace jiného členského státu;
- pravidla pro služby vytvářející důvěru (či tzv. „trust services“);
- právní rámec pro elektronické podpisy, elektronické pečetě, elektronická časová razítka, elektronické dokumenty, služby elektronického doporučeného doručování a certifikační služby pro autentizaci internetových stránek.

Z hlediska jeho cílů pak můžeme identifikovat následující klíčová slova:

- **interoperabilita** a usnadnění přeshraničního využívání on-line služeb v oblasti elektronické identifikace;
- **harmonizace** v oblasti služeb vytvářejících důvěru;
- technologická **neutralita**.

Mimo výše uvedené oblasti regulace se nařízení vymezuje i negativně tím, že definuje oblasti, které jeho úprava nemá zasáhnout. Obecně lze říct, že nařízení směřuje svoji působnost jen na „vztahy s mezinárodním prvkem“: ačkoli není normou mezinárodního práva soukromého, všechny oblasti uvedené výše jsou dotčeny jeho úpravou zejména tehdy, pokud probíhá přeshraniční styk – tj. obvykle mezi provozovatelem nějaké služby a jejím uživatelem.

Nařízení tedy nedopadá na privátní systémy autentizace a vnitrostátní „proprietární“ systémy; podle článku 2 se nařízení eIDAS nevztahuje na poskytování trust services používaných výhradně v rámci uzavřených systémů vyplývajících z vnitrostátního práva nebo z dohod mezi určeným okruhem účastníků. Stejně tak, poměrně logicky, není dotčeno ani vnitrostátní právo týkající se uzavírání a platnosti smluv ani obdobné normy stanovující kontraktační proces a formu dohod, jakkoliv reálný dopad na tyto právní vztahy mít nařízení bude, a to zejména prostřednictvím změn právní úpravy elektronického právního jednání, které nařízení vyvolá.

Časový harmonogram nařízení

Nařízení vstoupilo v platnost 7. září 2014. Mezi první úkoly, které si komise stanovila, bylo přijmout nezbytná procesní opatření pro usnadnění spolupráce mezi členskými státy týkající se mimo jiné interoperability, bezpečnosti, výměny informací a zkušeností v oblasti systémů elektronické identifikace a opatření týkající se rámce interoperability obecně vymezeného v článku 12, odst. 4 nařízení eIDAS. Do 1. července 2015 komise prostřednictvím prováděcích aktů stanoví specifikace týkající se podoby, zejména formátu, uspořádání, velikosti a vzhledu značky důvěry EU pro kvalifikované služby vytvářející důvěru.

Pro konkrétní implementaci nařízení v národních právních řádech je zcela zásadní září 2015, kdy má komise za úkol přijmout prováděcí akty podle článků 8(3), 22, 27(5) a 37(5), tedy:

stanovení minimální technické specifikace, norem a postupů, jejichž pomocí je vymezena nízká, značná a vysoká úroveň záruky prostředků pro elektronickou identifikaci;

- upřesnění informací ohledně důvěryhodných seznamů obsahujících informace týkající se kvalifikovaných poskytovatelů služeb vytvářejících důvěru, včetně stanovení technických specifikací a formátů těchto seznamů;
- referenční formáty zaručených elektronických podpisů nebo referenční metody, jsou-li používány alternativní formáty;
- referenční formáty zaručených elektronických pečetí nebo referenční metody, jsou-li používány alternativní formáty.

Počínaje datem publikace těchto prováděcích aktů je možné volitelně ze strany států začít uznávat prostředky pro elektronickou identifikaci, nejpozději však tři roky po tomto datu se pak tato volitelnost stává povinností a členské státy tedy budou muset vzájemně uznávat prostředky pro elektronickou identifikaci, které se budou kvalifikovat dle struktury uvedené v nařízení.

Konečně 1. července 2016 je okamžik, kdy vstoupí v účinnost nařízení jako takové, tudíž od tohoto data bude přímo aplikovatelné i pro právní vztahy založené českým právním řádem. Na rozdíl od směrnic tak nařízení nevyžaduje, aby byla právní úprava přenesena do jednotlivých národních právních řádů samostatnými zákony, ale je účinné bez dalšího. Nicméně vzhledem k rozsáhlé stávající právní úpravě v našich zákonech se dá očekávat legislativní smršť novelizací (hovoří se až o 120 dotčených zákonech) tak, aby naše zákony nebyly v rozporu s právní úpravou nařízení eIDAS.

Elektronická identifikace

Nařízení se snaží integrovat vše, co nějakým způsobem souvisí s elektronickou identifikací a autentizací. Za tímto účelem vystavělo poměrně složitou strukturu nástrojů různých úrovní co do požadavků na ně kladených.

Úrovně záruky prostředků pro elektronickou identifikaci a autentizaci:

- nízká – „omezená míra spolehlivosti u deklarované totožnosti osoby“ (např. klasické jméno/heslo);
- značná – „značná míra spolehlivosti u deklarované totožnosti osoby“ (např. certifikát pro autentizaci);
- vysoká – „vyšší míra spolehlivosti u prokazované totožnosti osoby, než nabízí prostředek pro elektronickou identifikaci se značnou úrovní záruky“ (př. „certifikát pro autentizaci uložený na eOP“).

Do 18. září 2015 komise stanoví minimální technické specifikace, normy a postupy pro určení obsahu výše zmíněných úrovní záruky, tudíž do tohoto okamžiku lze jen rámcově předpokládat, které systémy splní jednotlivé úrovně, když např. náš ISDS v tuto chvíli splňuje jen úroveň nízkou.

Služby vytvářející důvěru

Dle nařízení můžeme rozlišit následující služby vytvářející důvěru:

- elektronický podpis, elektronická pečeť, elektronické časové razítko a spojené služby;
- služby elektronického doporučeného doručování;
- certifikáty pro autentizaci internetových stránek;
- uchovávání elektronických podpisů & spol.

Je vhodné připomenout, že elektronický podpis bude určen pouze pro fyzické osoby, zatímco elektronická pečeť naopak pouze pro osoby právnické. Zároveň dojde k dalšímu terminologickému zmatení uživatelů, když uznávaný elektronický podpis dle našeho Zákona č. 227/2000 Sb., o elektronickém podpisu, se stane kvalifikovaným elektronickým podpisem.

Lze předpokládat, že nařízení bude mít pozitivní efekt na trh poskytovatelů služeb vytvářejících důvěru. Rozlišuje tzv. nekvalifikované a kvalifikované poskytovatele a na základě smyslu a koncepce nařízení můžeme očekávat růst počtu těchto poskytovatelů a celkové otevření podmínek. Jak uvádí recitál 36, „[n]ekvalifikovaní poskytovatelé služeb vytvářejících důvěru by měli podléhat nezatěžujícím a pružným činnostem následného dohledu, odůvodněným povahou jejich služeb a činností. Orgán dohledu by proto neměl mít obecnou povinnost vykonávat nad nekvalifikovanými poskytovateli služeb dohled.“

Příležitosti pro soukromý i veřejný sektor?

Nařízení eIDAS není zásadní revolucí, ale spíše příležitostí pro harmonizaci elektronické identifikace a elektronického právního jednání v rámci EU. Bez detailní znalosti prováděcích dokumentů je poněkud předčasné hovořit o konkrétních způsobech využití, ale na první pohled se naskýtají široké možnosti snazšího využití elektronických nástrojů v každodenním životě - banky či operátoři mohou fungovat jako poskytovatelé služeb ověření elektronické identity (server signing) a významně tím zjednodušit elektronizaci právního jednání. Stát konečně možná začne lépe využívat možností elektronických občanských průkazů a prostý občan doufejme ušetří čas tím, že v elektronickém světě zvýší důvěryhodnost svého právního jednání.

JUDr. Josef Donát, LLM, Partner

eIDAS – Brave New World

Aldous Leonard Huxley byl anglický spisovatel. Napsal mimo jiné knihu Brave New World (vyšla roku 1932), česky pod názvem Konec civilisace (L. Mazáč, 1933). Tento antiutopický román je často srovnáván s jinými díly (například 1984, G. Orwell). Pozoruhodnost rozdílu názvu knihy v původním českém překladu mě připadla vhodná při hledání myšlenky jak čtenářům eGovernmentu přiblížit NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (známé též a ne zcela přesně jako eIDAS (Electronic Identification and Trust Services). Velmi vulgárně řečeno ve zmíněné knize vedou dobré úmysly (Brave New World) k tragickým koncům (Konec civilisace). eIDAS je dobrým úmyslem. Může dopadnout dobře, může vést i k tragickým koncům. V tomto článku popíši, jak to bude krásné, pokud to dopadne dobře.

eIDAS má odstranit bariéry

eIDAS má odstranit bariéry elektronického trhu na území Evropské unie. Primárním cílem odstranit „...odstranit hlavní problémy, které občanům Unie brání ve využívání výhod jednotného digitálního trhu a přeshraničních digitálních služeb". (EN: „... to solve the main problems that prevent Union citizens from enjoying the benefits of a digital single market and cross-border digital services"; DE: „...die Hauptprobleme zu lösen, die Unionsbürger davon abhalten, die Vorteile eines digitalen Binnenmarktes und grenzüberschreitender digitaler Dienste zu nutzen"). Dovolte, abych některé bariéry popsal z osobní zkušenosti a naznačil, jak krásné to bude až eIDAS.

Bariéra 1 – PayPal mi nevěří, kdo jsem

Používám PayPal. K placení u mnoha malých obchodníků je to ideální nástroj. Jednoduše ho nabijete a platíte. Zkušenost jako obchodník nemám, ale jako milý platící jsem si nemohl ztěžovat. Až pojednou... Nabil jsem větší částku, konkrétně asi 50 000 Kč. Odjížděl jsem do zahraničí, chtěl jsem si tam něco případně koupit a už jsem zažil situaci, kdy mi moje platební karty u amerických obchodníků nefungovaly, protože neměly uvedenu americkou doručovací adresu. (Naše krásná země není jediná, která kvůli pár profesionálním zločincům zprudí všechny občany.) A najednou mi PayPal poslal email, že pokud jim nepošlu kopii pasu a kopii účtu například za elektřinu nebo plyn, kde bude moje (rezidenční, doručovací) adresa, omezí mi funkcionalitu. Těmi padesáti tisíci jsem jim vyběhl z profilu, na který kašlou a chtěli po mě další identifikaci. Přitom jistě mají identifikaci z mého bankovního účtu, ze kterého jsem PayPal nabil. Takže jsem oskenoval pas a účet za telefon a poslal jsem jim to. Ani nepřemýšlím, jak je to legální ale udělal jsem to, protože jsem to potřeboval. O pár dní později mi milostivě sdělili, že je to OK. Protože to byly prosté skeny, zjevně to přečetl člověk, nikoli robot. Otrava na všech stranách. Náklady na všech stranách.

Bariéra 1 s eIDASem padá

Bude-li fungovat eIDAS, zaregistruji se jako uživatel PayPalu svoi eIDASovou (eIDASu vyhovující) identitou. PayPal, jako spoléhající strana se spolehne na tuto státem garantovanou identitní informaci a nebude mě obtěžovat prokazováním údajů o mé totožnosti. Krásný nový svět. (Pro šťouraly podotýkám, že strana se kterou jsem jednal je: PayPal (Europe) S.à r.l. & Cie, S.C.A., Société en Commandite par Actions, Registered Office: 5th Floor 22-24 Boulevard Royal L-2449, Luxembourg, RCS Luxembourg B 118 349). Tedy lucemburskou právnickou osobou.

Bariéra 2 – Kdo prodává na aukro.cz?

Aukro.cz je asi nejznámější elektronickou burzou na .cz doméně. Pozoruhodné je, že většina nabízeného zboží je nového a prodejci jsou většinou firmy. Část zboží na aukro.cz nabízená je prodávané v dražbě. Nejprve jsem se rozhodl (v rámci testu) něco koupit. Zaregistroval jsem se, v rámci tohoto procesu byl ověřen můj email. Dále jsem vyplnil další přístupové údaje. Nijak jsem to „netúroval" a uvedl své skutečné osobní údaje. Předpokládám, že se tak chová většina klientů a (bohužel) si nelámou hlavu s jejich zneužitím. Vše proběhlo v pořádku, až na to, že se mi ten ošklivý obraz s kočkou z oleje na plátně nepovedlo koupit, protože mě někdo o deset korun přehodil.

Potom jsem zkusil něco prodat. Proces mi trochu vyrazil dech. V procesu aktivace mých osobních údajů jsem byl požádán o převedení 3 Kč z mého účtu na účet aukro.cz. Bylo mi nabídnuto pět bankovních ústavů nebo převod z jiné, výhradně české banky. Pokud bych měl zahraniční účet, mám zvolit aktivaci dopisem. Bum!!!

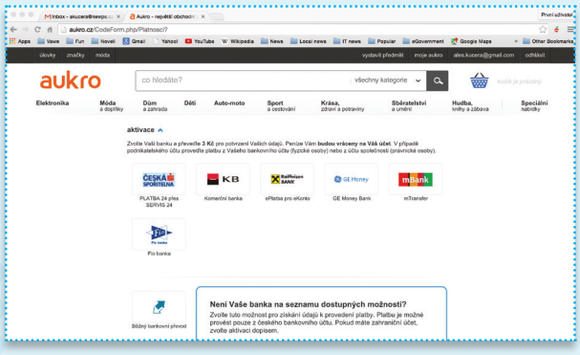
Toto je shrnutím lesku a bídy internetového obchodování, lesku a bídy povídaček o volném pohybu zboží, osob a kapitálu. Ještě se k tomu vrátím.

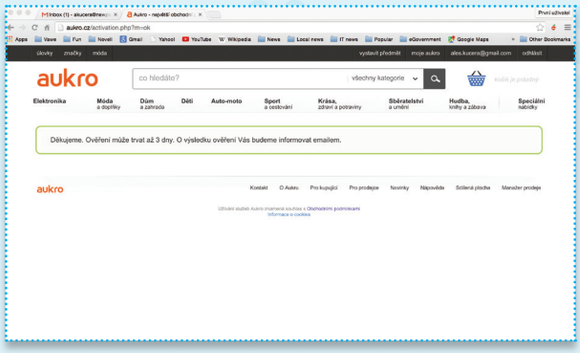
Provedl jsem platbu z jedné z vyjmenovaných bank a dozvěděl jsem se že „...ověření může trvat až 3 dny. O výsledku ověření Vás budeme informovat emailem." Email skutečně přišel, konkrétně asi za 27 hodin. Jednak jsem už neměl náladu něco prodávat, navíc mi ho podle mailu poslal polský server.

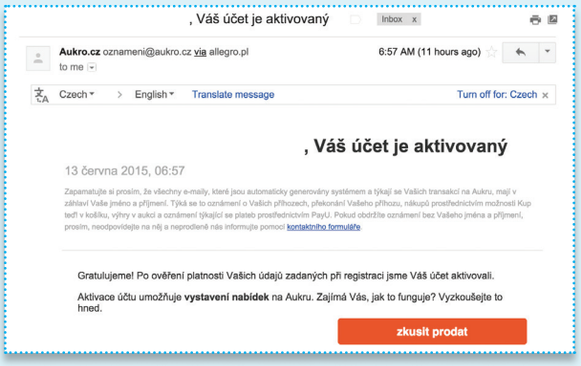
Co k tomu říct? Aukro.cz je asi těžké z něčeho vinit. Identitu prodávajícího potřebují znát a na žádný lepší způsob nepřišli, on asi ani neexistuje.

Bariéra 2 s eIDASem padá

Lépe by se žilo jak Aukru tak mě, kdyby moje identita byla ověřena třetí, autoritativní stranou. V tomto případě státem. eIDAS v tomto okamžiku reálně odstraní překážku v obchodování. Nebudete muset nikam převádět peníze, nikdo vám je nebude vracet a nebudete přemýšlet, proč jste ten email dostali z Polska. (I když ono je to asi







jedno. Celý proces ověření je plný děr otevřených sociálním hackerům.)

Máme tedy dva případy z byznysu. V jednom případě je obtěžován platící nebo placený, v druhém případě prodávající. Pojďme si teď ukázat, jak to už funguje, i když spoléhající se stranou na státem garantovanou identitu je jiný orgán veřejné moci.

Spolehnutí se na státem garantovanou identitu – vzor pro eIDAS

Asi před půldruhým rokem v tichosti ČSSZ zprovoznilo na svém portále (eportal.css.z.cz) přihlášení údaji do datové schránky. Máte-li zřízenu datovou schránku fyzické osoby nebo máte-li přístupové údaje k datové schránce právnické osoby, můžete si to sami vyzkoušet. V tomto případě zde pouze popíšu, co uvidíte, protože ta věc není hračka a prostě jsou to moje údaje. Z hlavní stránky portálu ČSSZ jste přesměrováni na přihlašovací dialog Informačního systému datových schránek, po zadání přístupových údajů ještě odsouhlasíte, že ISDS předá vaše osobní údaje ČSSZ a jste přihlášeni. Na to vám portál ČSSZ nabídne řadu služeb, kterou byste jinak získali pouze na pracovišti ČSSZ. Výpis takových údajů si můžete nechat poslat právě do té datové schránky, jejímiž údaji jste se přihlásili nebo dopisem. V řadě případů vám ovšem stačí na údaje nahlédnout. Jako fyzická osoba si tak například ověříte, jak jste na tom se započtenými odpracovanými lety pro výpočet důchodu.

Jak je to uděláno technicky je nepodstatné, jak je to procesně? Spoléhající se strana (zde ČSSZ) se spolehla na to, že podle zákona 300/2008Sb. (o elektronických úkonech a autorizované konverzi dokumentů) byl přihlašující se ověřen oprávněnou úřední osobou. Tedy, pokud jste žádali o zřízení datové schránky fyzické osoby, ověřil vás úředník na Czech POINTu, pokud jste jednatelem právnické osoby, ověřil vás notář. Zcela jistě zde chybí to, aby byly ověřovány všechny osoby mající identitu v datových schránkách. Potom by třeba k účtu právnické osoby v databázi ČSSZ mohla přistoupit i pověřená osoba, například pracovník, který má tuto agendu v podniku na starosti. Dnes se přihlašovacími údaji pověřené osoby k portálu ČSSZ nepřihlásíte. Což je správně. Věřme, že zákonodárci tuto díru brzy zalátají.

Konce dobrý, všechno dobré. Na vlastním malém pískovišti máme vyzkoušen princip spolehnutí se na státem garantovanou identitu. Máme něco jako trakař. Vzhůru k postavení dvoukoláku. Jen varuji před přílišným optimismem. Nemalujme hned auto s ABS a airbagy. O možných haváriích při implementaci eIDASu si povíme někdy jindy.

Ing. Aleš Kučera
Předseda představenstva
NEWPS HOLDING SE

NEWPS.CZ

Lokální JIP – koncept centrální správy uživatelů

Uživatel informačního systému a jeho oprávnění je pořád aktuální téma. Dotažení správy uživatelů až do úrovně opravdové centrální správy se povedlo dosud pouze několika orgánům veřejné moci (OVM). Zatímco u většiny OVM se jedná o řízení uživatelů na úrovni aplikací, pouze některé sdílejí identitu alespoň prostřednictvím Active Directory. Tento stav představuje velké bezpečnostní riziko. Uživatel je nucen si pamatovat několik uživatelských účtů a hesel, dokonce dochází ke sdílení účtů mezi více uživateli. Nelze tak hovořit o nepopiratelné odpovědnosti uživatele za provedený úkon. Nyní i s nástupem zákona o kybernetické bezpečnosti už skutečně nezbývá nic jiného, než se do projektu centrální správy uživatelů skutečně pustit.

Cílovým stavem by měla být správa uživatelů OVM a zřizovaných organizací, kdy každý uživatel bude používat pro autentizaci jeden unikátní uživatelský účet, nejlépe včetně vícefaktorové autentizace, čímž bude zajištěna nepopiratelná odpovědnost za jím provedené úkony.

Jak toho stavu dosáhnout? Variant je několik, zde se pokusím popsat tu, která se již osvědčila v praxi, vyzkoušel ji prakticky každý úřad a přináší víc než jenom správu uživatelů. Je to koncept Lokální jednotný identitní prostor (LJIP), klon řešení JIP CzechPOINT.

Lokální JIP

Koncept jde za hranici klasického pojetí Identity Managementu, vychází ze zkušeností získaných při realizaci JIP Czech POINT a integrací IDM systémů orgánů veřejné moci (OVM) pro zajištění autentizace a autorizace uživatelů prostřednictvím jednoho univerzálního uživatelského účtu. Zahrnuje vybudování centrálního adresáře uživatelů v prostředí úřadu a lokálních adresářů uživatelů zřizovaných organizací. V centrálním adresáři budou uloženy uživatelské účty všech uživatelů OVM, v lokálních pak uživatelské účty jednotlivých zřizovaných organizací.

Centrální adresář může být postaven na technologii NetIQ eDirectory nebo Microsoft Active Directory. Stane se základem konceptu nového Identity Management Systému - lokálního JIP. Rozšiřuje tak současné řešení správy uživatelských účtů v ICT prostředí OVM.

Centrální adresář bude dále propojen s Identity Management Systémem (IDM), který zajistí správu všech uživatelů po celou dobu životního cyklu uživatelského účtu. Bude navázán na autoritativní zdroj dat – personální systém, který je jediným spolehlivým zdrojem o stavu uživatele – úředníka/zaměstnance OVM. V krajním případě lze použít i mzdový systém. Uživatelské identity budou následně propagovány do všech připojených agendových informačních systémů a aplikací OVM.

Součástí řešení IDM jsou rovněž postupy (workflow) pro schvalování přístupových oprávnění. Důležitou součástí je uživatelská samoobsluha, prostřednictvím které mohou uživatelé sami provádět změnu hesla či vybraných údajů svých uživatelských účtů. Přece nechcete celou pracovní dobu strávit resetováním hesel vašich uživatelů.

Výsledkem je sjednocení uživatelských účtů ve všech integrovaných systémech pro každého uživatele, čímž budou mimo jiné sníženy náklady na provoz a údržbu jednoúčelových uživatelských účtů v mnoha agendových informačních systémech a aplikacích při současném zvýšení bezpečnosti těchto IT systémů.

Externí uživatelé

Koncept se věnuje rovněž kontrole přístupu externích uživatelů (zaměstnanců zřizovaných organizací, případně externích spolupracovníků, konzultantů apod.). Pro kontrolu jejich přístupu slouží komponenta Access Gateway (AGW, přístupová brána), která umožní další rozvoj systému v případě zajištění přístupu uživatelů z řad zřizovaných organizací, či dalších externích subjektů. AGW zajistí ověření přístupových údajů uživatele vůči centrálnímu adresáři uživatelů, po úspěšném ověření pak pouští uživatele k systémům a aplikacím na základě přidělených oprávnění (uživatelských rolí).

AGW umožňuje autentizaci uživatele klasickým postupem (jménem a heslem), ale i použití vícefaktorové autentizace, a to pomocí certifikátu nebo jednorázového hesla (OTP – One Time Password).

AGW slouží primárně pro autentizaci externích uživatelů, lze ji však využít jako centrální přístupovou bránu, přes kterou pak k systémům a aplikacím přistupují rovněž inter-

ní uživatelé. Komponenta AGW prokázala svou spolehlivost v systémech, jako Czech POINT a Informační systém datových schránek.

Synchronizace LJIP – JIP Czech POINT

Koncept nabízí možnost využití synchronizace uživatelských účtů mezi centrálním adresářem uživatelů OVM (LJIP) s jednotným identitním prostorem Czech POINT. Synchronizaci účtů zajistí komponenta LDAP2JIP, případně AD2JIP (podle typu adresáře OVM). Díky tomu pak mohou uživatelé OVM, případně také vybraných zřizovaných organizací přistupovat prostřednictvím jednoho unikátního uživatelského účtu k ISVS, jako např. Czech POINT, CzechPOINT@office, ISUI, IAIS, AIS RPP působnostní apod., stejně jako k AIS a lokálním systémům vlastního úřadu.

Nezanedbatelnou výhodou synchronizace s JIP Czech POINT je ztotožnění uživatelů vůči registru obyvatel (ROB). To zajistí, že uživatelský účet používá skutečná osoba, jejíž data jsou vedena správně jak v základních registrech, tak v personálním systému OVM, resp. zřizované organizace. Opačnou synchronizací může OVM z JIP Czech POINT získat aktuální seznam agend a činnostních rolí, k nimž se přihlásil v základních registrech.

Díky synchronizaci adresářů dochází například po změně statusu v personálním systému OVM automaticky k zablokování uživatelského účtu zaměstnance, který ukončil pracovní poměr v lokálním JIP. Současně je tato informace propagována do všech připojených systémů, tedy samozřejmě i do JIP Czech POINT. Odpadá tak nebezpečí vytváření mrtvých duší.

Zřizované organizace

V každé zřizované organizaci bude vytvořen lokální adresář uživatelů. V nich budou uloženy uživatelské účty uživatelů příslušné zřizované organizace. Tyto účty budou primárně používány pro přihlašování uživatelů do lokálních agendových informačních systémů a aplikací zřizované organizace.

Prostřednictvím synchronizačního modulu budou uživatelské účty zřizované organizace synchronizovány do centrálního adresáře uživatelů OVM. To umožní, aby se uživatelé z jednotlivých organizací s oprávněním přístupu mohli přihlásit pomocí svých unikátních uživatelských účtů do AIS a aplikací provozovaných OVM.

Volitelně lze řešení doplnit o synchronizační komponentu LDAP2JIP (AD2JIP), prostřednictvím které budou uživatelské účty uživatelů zřizovaných organizací synchronizovány do JIP Czech POINT.

Zřizované organizace, které nemají kapacity ani kompetence na provoz vlastního IT prostředí, pak mohou využít dedikovaného prostoru LJIP pro potřeby správy vlastních uživatelů a jejich uživatelských oprávnění.

Správa uživatelů

Vlastní správa uživatelů vychází ze zkušeností správy uživatelů JIP Czech POINT. Každý subjekt (OVM, zřizované organizace) má pověřeného administrátora/y. Lze aplikovat obdobný způsob jejich autorizace jako pro lokální administrátory JIP Czech POINT.

Administrátor OVM je odpovědný za správu uživatelů OVM, kterou provádí primárně v lokálním JIP. Současně může uživatelské účty spravovat rovněž v prostředí Czech POINT v aplikaci Správa dat (toto prostředí zná v současnosti zhruba 8 000 lokálních administrátorů OVM). Provedené změny jsou následně automaticky propagovány do centrálního adresáře uživatelů lokálního JIP nebo naopak do JIP Czech POINT.

Obdobně spravuje uživatele lokální administrátor ve zřizované organizaci.

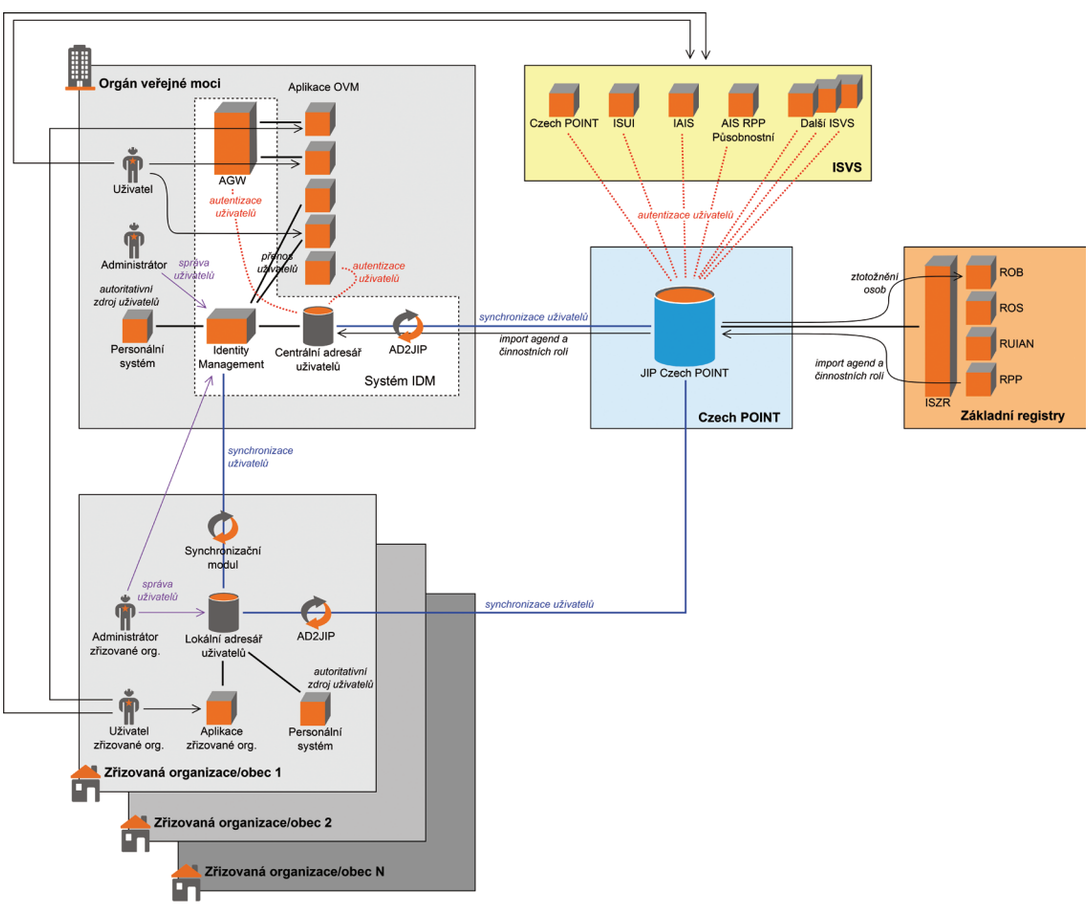
Součástí konceptu LJIP je samozřejmě správa certifikátů, případně dalších autentizačních prostředků uživatelů. Správa certifikátů zahrnuje registraci nových certifikátů uživatele do systému IDM, případně obnovených certifikátů, přičemž certifikáty mohou být vydány některou z akreditovaných certifikačních autorit. Lze použít i interní certifikáty, přesto preferovanou variantou je použití certifikátů vydávaných některou z akreditovaných certifikačních autorit.

Správa jiných autentizačních prostředků zahrnuje registraci (či zrušení registrace) OTP zařízení pro generování jednorázových hesel, nebo třeba i reset zapomenutého hesla.

Varianty řešení lokálního JIP

Koncept LJIP má tu výhodu, že si zákazník může vybrat variantu HW a SW řešení, která nejlépe vyhovuje jeho

Základní schéma konceptu IDM pro OVM a zřizované organizace



možnostem. K dispozici je standardní on-prem řešení s implementací v datovém centru zákazníka. LJIP lze stejně tak provozovat v cloudu, například v Azure.com, který splňuje všechny požadavky bezpečnosti pro provozování takového systému. Vždyť také JIP Czech POINT je de facto provozován v cloudu, uživatelé přistupují k jeho autentizačním a autorizačním službám vzdáleně prostřednictvím webových služeb. Případně lze zvolit kombinovanou variantu, kdy vlastní LJIP je provozován v datovém centru zákazníka a cloud je využit pro backup a disaster recovery řešení.

Přínosy řešení

Těch zde byla uvedena celá řada. Koncept LJIP je aplikovatelný pro ORP, kraje i ministerstva, včetně všech jimi zřizovaných organizací. Ale především administrátoři orgánů veřejné moci již dnes pracují s účty uživatelů v JIP Czech POINT, jsou tedy připraveni spravovat uživatele i v lokálním JIP svého úřadu. Nebudou se muset učit nic nového.

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

NEWPS.CZ

eIDAS: Česká příležitost, nebo ohrožení?

Ve světě stále se zjednodušujících sdělení (aby náhodou příjemce informace nebyl obtěžován tím, že musí používat vlastní rozum) jaksi zaniká, že NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A EVROPSKÉ RADY (EU) č. 910/2014 ze dne 23. července 2014 „O elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu", známé též jako eIDAS, není zaměřeno jen na elektronickou identitu, ale je nástrojem pro zpřístupnění evropského „Digital Single Market", tedy jakéhosi Schengenského prostoru pro konzumaci on-line služeb nabízených napříč veřejnou správou a podnikatelskými subjekty členských zemí EU svým zákazníkům. Zkrátka, tak jako přejíždíte hranice z Česka do Německa, aniž by Vás kdokoliv obtěžoval kontrolou, zda máte právo vstupu, neboť Německo se spoléhá na fakt, že na našem území se pohybují jen osoby, které mají právo pobytu v Česku, a tedy i po celé EU, tak stejným způsobem se bude moci spolehnout německý dodavatel na digitální formu totožnosti, dokumentů, zásilek a informací na webu, které mu poskytne český obchodní partner nebo klient.

Štěstí, že jsme členskou zemí EU

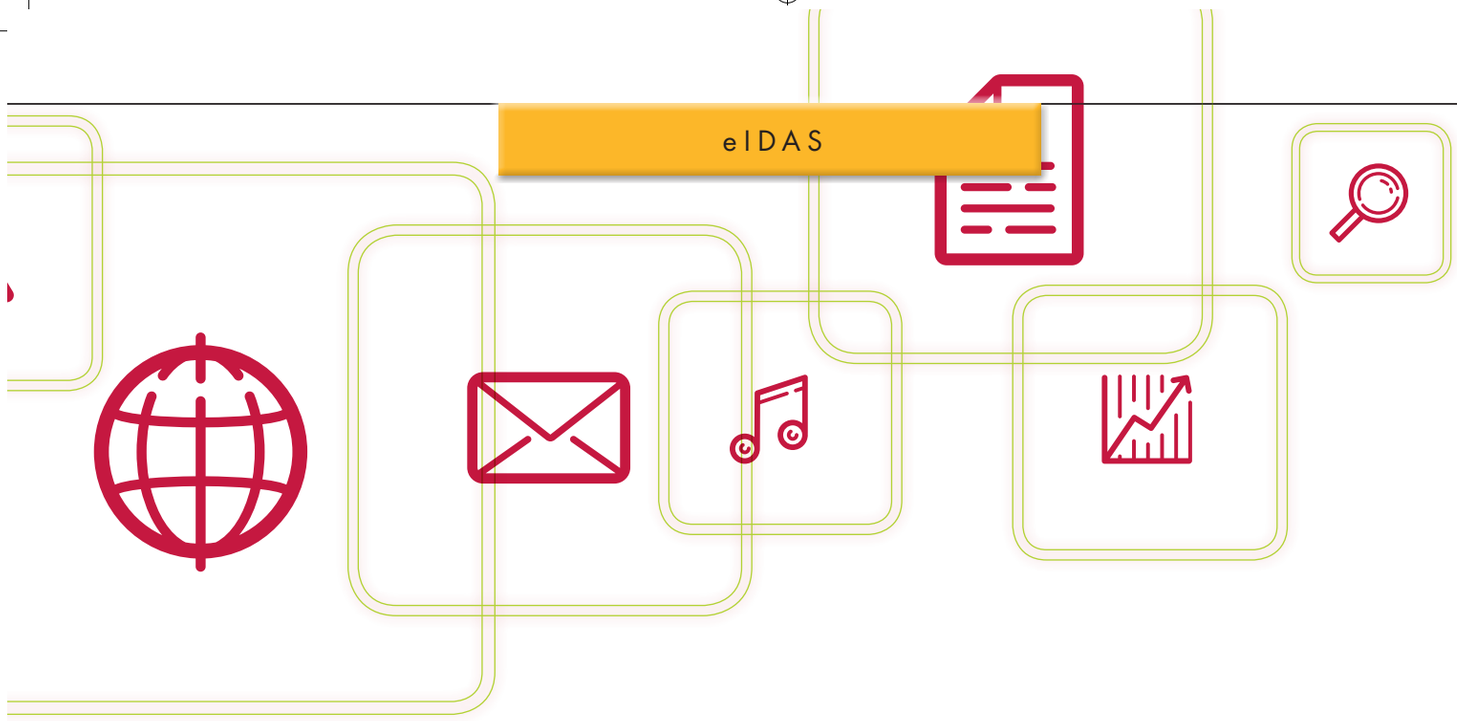
Pro většinu „účastníků zájezdu", kteří mají zkušenosti s tím, kolik chce český dodavatel služeb (z veřejnoprávního i soukromoprávního sektoru) po českém zákazníkovi papírů a potvrzení, to zní jako těžko uvěřitelné sci-fi. Nicméně je zde jakési světlo v tunelu, protože jsme členským státem EU se závazky z toho vyplývajícími – u eIDAS se jedná nikoliv o směrnici, která má většinou doporučující charakter, ale o evropské nařízení, které je platné napříč EU. Proto je soudně vymahatelné např. u Evropského soudního dvora a česká exekutiva bude muset konat (a nikoliv jen deklarovat, že „se bude snažit"), aby se vyhnula rizikům soudních sporů. Netvrdím, že výše popsaný mechanismus bude v roce 2020 běžnou rutinou, ale určitě nám EU v tomto směru pomůže udělat si pořádek na vlastním dvorku.

Elektronická identita občana nejsou elektronické identifikační průkazy

Zavedení elektronické identity je bohužel médii (a následně i širokou veřejností) mylně spojováno výhradně s projektem elektronických občanek. V kontextu nařízení eIDAS je elektronická občanka pouze jedním z (mnoha) alternativních nosičů pro důvěryhodné přihlašování k on-line službám poskytovaných nejen veřejnou správou, ale zejména komerčním sektorem. V ČR díky funkčnímu systému základních registrů by měl být po technické stránce onou elektronickou identitou fyzické osoby záznam (referenční údaj) v registru obyvatel, který umožňuje spojit elektronickou identitu při přihlášení do on-line služeb s důvěryhodně ověřenou identitou fyzické osoby. Pro masivní rozvoj využití elektronické identity v ČR je klíčové, aby její výhody mohli využívat občané s mobilním zařízením a účtem v bance nejen pro komunikaci s úřady (podám a zaplatím správní poplatek), ale především v běžném životě. Tedy rychle objednám a zaplatím za zboží nebo službu v libovolném členském státu EU pod jednou elektronickou identitou na jakémkoliv zařízení, ať je to PC/notebook, tablet nebo chytrý telefon.

Elektronické doporučené doručování

Právní účinek služby elektronického doporučeného doručování v eIDAS říká: „Datům odeslaným a přijatým prostřednictvím služby elektronického doporučeného doručování nesmějí být upírány právní účinky a nesmějí být odmítána jako důkaz v soudním a správním řízení pouze z toho důvodu, že mají elektronickou podobu nebo že nesplňují



požadavky na kvalifikovanou službu elektronického doporučeného doručování.“ Jednoduché sdělení, na které jsme díky rutinnímu provozu datových schránek (v dikci eIDAS formou kvalifikované služby) připraveni po úpravách systému, které nejsou koncepčního charakteru, jak technicky, tak zejména procesně pro veřejnoprávní i soukromoprávní sektor. Na rozdíl od členských zemí, kde tento typ služby není ani v pilotním provozu, bychom neměli mít s plněním tohoto bodu eIDAS problémy.

Elektronický dokument

Elektronickému dokumentu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu – tolik jediný odstavec, který v eIDAS definuje právní účinek elektronických dokumentů a který bude mít fatální dopad na fungování moderní informační společnosti. I zde máme vybudovanou infrastrukturu a procesy (zatím jen v komunikaci se státem) navazující na zákon o elektronickém podpisu, kterému je věnována velká část eIDAS, navíc máme k dispozici propracovaný systém autorizovaných konverzí z listiny do elektronické podoby (a naopak). Klíčové bude, jak se podaří promítnout tyto zkušenosti do soukromoprávního sektoru u elektronické formy právního jednání, kterému jde vstříc i nový občanský zákoník („Písemná forma je zachována i při právním jednání učiněném elektronickými nebo jinými technickými prostředky umožňujícími zachycení jeho obsahu a určení jednající osoby.“).

Příležitost, nebo ohrožení?

Zdánlivě by nařízení mělo být příležitostí, jak by se mohlo Česko posunout v EU na přední pozice, protože při pohledu na eIDAS jako na stavebnici máme řadu „prefabrikovaných“ modulů funkčních a v rutinním provozu a neměl by být problém je sladit do zážitku, který CHCE uživatel zažít. Pozice a priority vlády jsou bohužel nastavené jiným směrem – sice ve svém programovém prohlášení tvrdí, že bude usilovat o „efektivní využití informačních a komunikačních technologií (ICT) ve veřejné správě a současně podporu internetové ekonomiky“, ale pod efektivním využitím ICT si představuje pouze snížení nákladů na ICT nebo zavedení dalších povinných elektronických výkazů. Zcela chybí představa využití a rozvoje ICT ve prospěch uživatelských služeb poskytovaných státem pro podporu vize Digital Single Market.

Co na to ICT UNIE

Pracovní tým ICT UNIE zaměřený na problematiku eIDAS se ve svých aktivitách hodlá soustředit zejména na spotřebitele (tedy daňové poplatníky v různých rolích) a jejich uživatelský zážitek, které naplňuje poslání ICT UNIE: „Posláním ICT UNIE je být respektovanou profesní organizací ICT průmyslu odstraňující bariéry brzdící rozvoj informačních a komunikačních technologií ve prospěch spotřebitelů. Chceme být partnerem i oponentem vládě České republiky v projektech podporujících směřování k evropské informační společnosti a modernímu výkonu státní a veřejné správy pracující efektivně pro občany i podnikatelský sektor.“

Richard Kaucký
člen představenstva ICT UNIE
odpovědný za problematiku eIDAS

Budoucnost elektronické identifikace i dokumentů leží ve spolupráci napříč Evropou

Na konci srpna loňského roku bylo v Úředním věstníku Evropské unie publikováno Nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu, které je odborné veřejnosti více známo pod zkráceným názvem eIDAS.

Toto nařízení se zaměřuje jak na elektronický podpis a s ním spojené kvalifikované certifikáty či časová razítka, tj. oblasti částečně upravené Směrnicí 1999/93/ES, o zásadách Společenství pro elektronické podpisy, ale též nové a dosud neregulované oblasti, jako je elektronické doručování (tzv. e-Delivery), webové (SSL) certifikáty nebo vzájemné uznávání elektronické identifikace (eID).

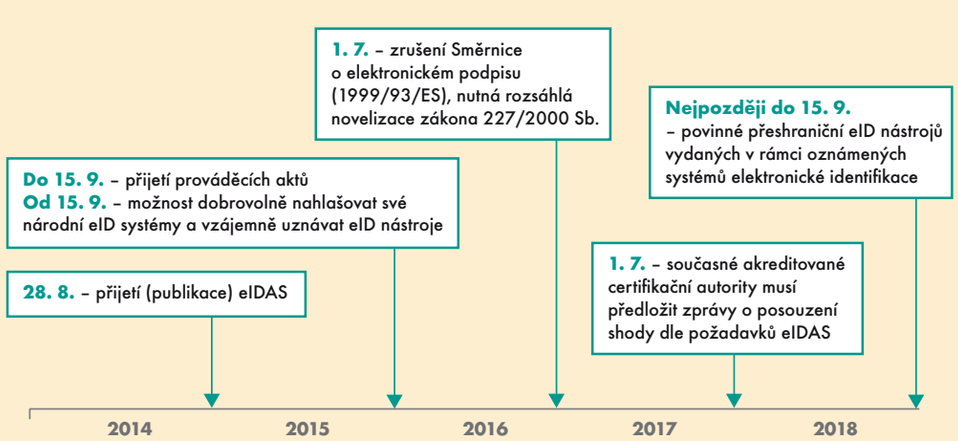
Co změní eIDAS?

Přesto, že eIDAS byl publikován již téměř před rokem, jeho jednotlivé části budou nabývat účinnost postupně až prakticky do konce roku 2018. Rozsáhlé změny jsou očekávány především v oblasti elektronické identifikace. Zde tato přímo účinná evropská legislativa počítá s možností vzájemného uznávání eID nástrojů. Těmi ale nemusí být jen elektronické občanské průkazy (eOP), ale i nástroje soukromého sektoru, jako např. bankovní karty, které jsou dnes pro přihlašování ke službám e-Governmentu využívány především ve Skandinávii. Zkušenosti z ostatních zemí Evropy přitom ukazují, že šanci na úspěch mají především řešení umožňující přihlašování jak ke službám e-Governmentu, tak ke službám soukromého sektoru jako jsou např. elektronické obchody či banky, které využíváme mnohem častěji.

Na to pamatuje i eIDAS, který zahrnuje i možnost zapojení nestátních eID nástrojů.

V rámci vzájemného uznávání pak eIDAS počítá nejdříve s dobrovolnou fází, která by měla být teoreticky zahájena již na podzim letošního roku, a o tři roky později i s fází povinnou. Do toho vstoupí již v průběhu roku 2016 nutnost významně přepracovat současný český zákon č. 227/2000 Sb., o elektronickém podpisu, neboť dojde ke zrušení platnosti již zmíněné Směrnice 1999/93/ES a tuzemská legislativa se tak bude muset vypořádat především s tím, že nařízení je na rozdíl od směrnice přímo účinné a tuzemský zákon tak může upravit jen ty části, u kterých k tomu mají členské státy výslovné zmocnění, případně jdou nad rámec eIDASu.

Dopad eIDAS na oblast eID v čase



Elektronická identifikace jako součást jednotného trhu

Na možnosti vzájemného uznávání elektronických občanských průkazů a dalších nástrojů se však vEvropě začalo pracovat již dávno před přijetím eIDAS a jeho projednáváním vbruselských institucích. Cílem Evropské komise bylo navázat na dosavadní integrační úsilí v oblasti vnitřního trhu a jeho čtyři základní svobody (pohybu osob, zboží, kapitálu a služeb) a vytvořit tzv. jednotný digitální trh. Jeho součástí by pak měly být vzájemně propojené elektronické služby (zejména e- Governmentu), kde elektronická identifikace představuje jeden ze základních pilířů.

Zatímco „klasický" elektronický průkaz je bez problémů uznáván na evropských letištích, hotelích či autopůjčovnách, sfunkcemi elektronického průkazu a jeho možnostmi např. při přihlášení ksystémům elektronického doručování (v ČR datové schránky) nebo portálům veřejné správy s možností volit, je to o poznání horší.

Již v roce 2008 se proto Evropská komise rozhodla podpořit rozsáhlý pilotní projekt STORK (Secure idenTity acrOss boRders linKed), jehož cílem mělo být na vybraných případech (use case) v oblasti veřejné správy vyzkoušet možnosti elektronické identifikace a autentizace ke službám e- Governmentu v jiné zemi. Na tento projekt pak navázal od dubna 2012 projekt STORK 2.0, který se zabývá též zapojením nestátních subjektů a využitím jejich atributů nezanesených v základních registrech. Do řešení tohoto projektu se za Českou republiku zapojilo rovněž sdružení CZ.NIC, jehož služba jednotných identit mojeID byla v loňském roce jako jediná v ČR ohodnocena stupněm důvěryhodnosti QAA3 (tj. stejně jako např. švýcarské elektronické občanské průkazy) odpovídající „značné úrovni záruky" dle eIDAS.

eID nejsou jen elektronické občanské průkazy

Důvěryhodný autentizační nástroj však představuje jen jednu zčástí vzájemného uznávání elektronických identifikačních nástrojů. Tou další částí je vystavění systému, ve kterém si jednotlivé národní nástroje (tj. elektronické občanské průkazy, ale i bankovní či studentské karty) budou vzájemně rozumět. Vzhledem ke značné rozdílnosti jednotlivých národních systémů se jako řešení ověřené již v rámci projektu STORK ukazuje možnost vybudování vzájemně propojených rozhraní, tzv. PEPS (Pan-European Proxy Services), na které se tyto nástroje napojí.

Na základě Nařízení Evropského parlamentu a Rady (EU) č. 283/2014 o hlavních směrech transevropských sítí v oblasti telekomunikační infrastruktury následně Evropská komise v rámci programu Connecting Europe Facility (CEF) podpořila vývoj a následnou implementaci těchto bran, které představují jeden z pěti tzv. základních stavebních kamenů infrastruktury pro digitální služby (DSI). Těmi dalšími částmi je elektronický podpis, elektronické doručování (tzv. e-Delivery), elektronická fakturace a to zejména ve vztahu ke Směrnici o elektronické fakturaci při zadávání veřejných zakázek a oblast automatických překladů.

Právě těchto pět základních kamenů představuje jeden z budoucích trendů vzájemně propojených služeb e-Governmentu a pokud se Česká republika nechce v hodnocení e-Governmentu propadnout až na poslední příčku, měla by na tento trend reagovat a jednotlivé základní stavební bloky představující nedílnou součást telekomunikační infrastruktury integrovat do Národního architektonického plánu eGovernmentu ČR a jednotlivých projektů e-Governmentu.

Jiří Průša

Autor se dlouhodobě věnuje problematice evropského eGovernmentu a ve sdružení CZ.NIC má na starost právě realizaci a zapojování do evropských projektů.

e-government 20:10

aneb žijem si jak na zámku, ať to trvá věčně

MIKULOV • 8. - 9. 9. 2015

ODBORNÝ PARTNER

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

PLATINOVÝ PARTNER

CISCO

GENERÁLNÍ PARTNER

Česká pošta

GORDIC®

Check Point SOFTWARE TECHNOLOGIES LTD.

ZLATÝ PARTNER

Atos · ČSOB · CZ.NIC · FORTINET · FUJITSU · hp · ICZ · Microsoft · NEWPS.CZ · ROWAN LEGAL · software602 · T · · · vmware

PARTNER

COMSYS · dns · elinkx · HELIOS · ictunie · information and records management society CZECH REPUBLIC GROUP · MARBES CONSULTING · OKI · SZR SPRÁVA ZÁKLADNÍCH REGISTRŮ · AVERA

TECHNOLOGICKÝ PARTNER

AV MEDIA komunikace obrazem · intel

... vše podstatné o eGovernmentu najdete v Mikulově.

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



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 **8. - 9. 9. 2015**.

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. 2015 ..... 500 Kč
registrace do 25. 6. 2015 ..... 600 Kč
registrace do 25. 7. 2015 ..... 1 000 Kč
registrace do 25. 8. 2015 ..... 1 200 Kč
registrace do 7. 9. 2015 ..... 1 500 Kč

KOMERČNÍ SFÉRA (uvedené ceny jsou bez DPH):

registrace do 25. 5. 2015 ..... 2 700 Kč
registrace do 25. 6. 2015 ..... 3 600 Kč
registrace do 25. 7. 2015 ..... 4 500 Kč
registrace do 25. 8. 2015 ..... 4 900 Kč
registrace do 7. 9. 2015 ..... 8 000 Kč







... vše podstatné o eGovernmentu najdete v Mikulově.

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

e-government 20:10

aneb žijem si jak na zámku, ať to trvá věčně

MIKULOV • 8. - 9. 9. 2015

REGISTRACE STÁLE MOŽNÁ

ODBORNÝ PARTNER

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

PLATINOVÝ PARTNER

CISCO

GENERÁLNÍ PARTNER

Česká pošta

GORDIC®

Check Point SOFTWARE TECHNOLOGIES LTD.

... vše podstatné o eGovernmentu najdete v Mikulově.

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