Masarykova univerzita v Brně
Filozofická fakulta
Ústav české literatury a knihovnictví
Kabinet informační studií a knihovnictví

Bezpečnost informací eGovernmentu v cloudu

Seminární práce do předmětu Informační průmysl

Autor: Bc. Radek Mezuláník, DiS.
UČO: 398472
Typ studia: Mgr. navazující / kombinované

Praha
20. 11. 2012

Obsah

1 eGovernment v cloudu

eGovernment je „možnost komunikace s institucemi státní a veřejné správy v elektronické podobě a další procesy s tím související, zejména tvorba příslušné legislativy a přechod úřadů na elektronickou verzi vedení agendy“[1]. Cílem eGovernmentu je usnadnění styku veřejnosti s úřady. Jedná se hlavně o úsporu času občanů, posílení efektivity fungování úřadů a úspora financí jak na straně nás občanů, tak na straně státní správy. To vše díky elektronizaci agendy.

1.1 Legislativa

Elektronizaci státní správy však nešlo provést jen tak. Bylo potřeba pro ni vytvořit optimální podmínky a pravidla, proto byly ustanoveny některé nové zákony, kterými se mimo jiné eGovernment řídí:

- Zákon o svobodném přístupu k informacím č.106/1999 Sb.
- Zákon č.111/2009 Sb., o základních registrech
  Upravuje základní procesy při elektronizaci státní správy. *Zákonem č.227/2009 Sb. se změnily některé jeho zákony.*
- Zákon o veřejných zakázkách č.137/2006 Sb.
  Využití elektronických nástrojů při zadávání veřejných zakázek.[2]
- Zákon č.300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů.
  Tento zákon je známý také jako eGovernment Act
- Zákon č.301/2008 Sb., doprovodný zákon k zákonu č.300/2008 Sb, kterým se mění některé zákony v souvislosti s přijetím zákona o elektronických úkonech a autorizované konverzi dokumentů.
- Zákon o občanských průkazech č.328/1999 Sb.
  Využití e-občanky v elektronické komunikaci.

[1] *Ministerstvo vnitra České republiky* [online]. 2012 [cit. 2012-11-26]. Dostupné z: http://www.mvcr.cz/clanek/cesty-k-egovernmentu.aspx

[2] *Moravské hospodářství* [online]. [cit. 2012-11-15]. Dostupné z: http://www.moravskehospodarstvi.cz/clanky/legislativa/prehled-zakonu-v-oblasti-egovernmentu/

- Zákon č.365/2000 Sb., o informačních systémech veřejné správy.
  Tento zákon rámcově vymezuje například vydávání výpisů na kontaktních místech veřejné správy Czech POINTech.

1.2 Co je to cloud?

Bavíme se tu o eGovernmentu v cloudu, ale mnohým pojem „cloud" nemusí nic říkat.
Je to technologické uspořádání počítačové infrastruktury, kterou zákazník (v našem případě tedy státní správa) nevlastní, ale pouze si ji pronajímá. V praxi to znamená, že informační systém je uložen na serverech poskytovatele v datovém centru poskytovatele a zákazník ke svému systému přistupuje pouze přes internet.

Jaké jsou výhody cloudu?

- Aktualizace firmwaru a všech aplikací probíhá v cloudu denně (na vlastní infrastruktuře v měsíční až roční periodě)
- Platba jen za využité prostředky
- Úspora energie
- Dlouhodobé snížení celkových nákladů
- Možnost kdykoliv zvýšit nebo naopak snížit HW nároky podle potřeby
- Bezpečnost?

Proč se tedy soukromý sektor zdráhá přejít na cloud? Důvody jsou více než jasné.

- Přechod na cloudové řešení je jednorázově velká investice
- Bezpečnost dat není zaručena, protože jsou uložena na „cizím" úložišti mimo kontrolu zákazníka
- Zákazník je odkázán na internetové připojení, bez něj se ke svým datům nedostane

Jednu z možných variant využilo právě Ministerstvo vnitra, pod které spadá eGovernment a to privátní cloud. Jedná se o stejný princip, že servery a infrastruktura patří poskytovateli, nicméně jsou umístěny u zákazníka nebo na jemu dostupném místě. Ministerstvo vnitra tedy nechalo postavit nové datové centrum. Sem se mají postupně převádět datová centra všech ostatních ministerstev. Důležitý je fakt, že tato centra budou vytvářet firmy ze soukromého sektoru.[3]
Cloud ale neznamená jen přestěhování hardware k poskytovateli. Je to především pronájem služeb, softwaru, platformy a infrastruktury. Toto řešení umožňuje je například na rozdíl od běžného webhostingu (což je pronájem hardware a platformy) ustát tzv. *digg efekt*. Je to okamžitý nárůst zátěže, ať už procesoru nebo paměti.
Obyčejný webhosting má staticky alokované prostředky, takže jsou pevně dané a při extrémním zatížení spadne. Cloud alokuje prostředky dynamicky, proto mu nevadí, když dočasně nebo i trvale překročí možnosti zákazníka.
V praxi to znamená například ochranu před Distributed Denial of Service, neboli DDOS útokem.

[3] Vnitro chystá využít pro eGovernmentu „cloud computing" – budou další zakázky pro firmy?. In: *EGov.cz: Nezávislý informační portál* [online]. 2011 [cit. 2012-11-28]. Dostupné z: http://www.egov.cz/index.php?option=com_content&view=article&id=187:vnitro-chysta-vyuit-pro-egovernmentu-cloud-computing-budou-dali-zakazky-pro-firmy&catid=1:egovernment&Itemid=3

Díky cloudu fungují také průkopníci jako je Microsoft, Gogole a Amazone. Bez této inovace by asi ani Facebook neexistoval, tak jak ho známe dnes. Také běží v privátním cloudu a pravidelně nakupuje od společnosti Dell nepřeberné množství virtuálních serverů.

2 Bezpečnost cloudu

Samotná výhoda přenechání veškerého vybavení a serverů poskytovateli a ponechat si na úřadě pouze slabší počítače, přes které budou pouze přistupovat na vzdálené úložiště, je zároveň kámen úrazu. Ekonomové ve firmách a ve státní správě se snaží ušetřit, kde se dá, proto by nejraději cloud ihned nasadili. Jenže jak mohou svěřit osobní data nás všech, někomu jinému? Když budou mít privátní cloud, budou k němu mít přístup pouze pověřené osoby, nebo i někdo jiný? Pořád se jedná o naše osobní údaje, o naši korespondenci s úřady a se státem.

- 44 % dotázaných společností považuje za největší překážku zavedení cloudových technologií bezpečnost,
- 29 % dostatečnou výkonnost systému,
- 20 % problémy s integrací cloudu do současných systémů,
- 18 % nedostatečný dohled nad IT systémy,
- 16 % ztráta plné kontroly nad daty s ohledem na zájmy zákazníků.[4]
- A jaké bezpečnostní otázky si potencionální zákazníci cloudu kladou?

Pokud nebudou mít všechny úřady, spravující osobní data občanů, svá data bezpečně uložena ve datovém centru, může nastat situace, že poskytovatel bude mít servery mimo ČR a tato data pak budou podléhat jiné legislativě než té naší, proto hrozí jejich diskreditace nebo nesprávné nakládání s daty. Poskytovatel by měl zaručit umístění dat v ČR, ale pokud to zákazník (tedy stále český úřad) nevyžaduje nebo si to neověří, může nastat problém. Dodavatel cloudového řešení totiž nepřebírá odpovědnost za úřady, které u něj ukládají osobní data. Pokud nastane jejich odtajnění, na vině bude první úřad.
Utajení dat je už pouze otázkou důvěry. Existují sice řešení, jak data ochránit před samotným poskytovatelem, ale samotná možnost cizího přístupu je hrozba.

K **přetížení systému** nemůže teoreticky vůbec dojít, díky dostatečné výkonnostní rezervě v cloudu.

Ztráta, krádež nebo zničení hardwaru naštěstí cloudovou variantu nijak neovlivní, protože servery jsou většinou umístěny v zabezpečeném datacentru a mají sdílená disková pole se zálohováním. Je tedy velmi nepravděpodobné, že by došlo ke ztrátě dat tímto způsobem.

Dostupnost dat a závislost na internetovém připojení je také velmi častá otázka, kterou si manageři pokládají. Jistě si vzpomenete na nasazení nového registru vozidel, který poté nefungoval. Všechny dopravní magistráty byly doslova odříznuté od uživatelských dat. Při představě, že jednomu úřadu vypadne internetové připojení, nastane okamžitě stejný problém. Aby se zabránilo takovému problému i v případě datacentra, využívají se pro všechny servery

[4] KPMG. *Clarity in the Cloud: A global study of the business adoption of Cloud* [online]. 2011, 48 s. [cit. 2012-11-28]. Dostupné z: http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cloud-clarity.pdf

záložní zdroje pro případ výpadku proudu. Proti výpadku internetového připojení existuje tzv. duální linka. Jedná se o rozdělené nebo záložní připojení, které se aktivuje v případě výpadku hlavního datového toku.
Správa softwaru je v klasickém modelu někdy časově náročná operace a ne všechny klientské stanice jsou obhospodařovat z IT oddělení. Při cloudovém řešení tato odpovědnost přechází na poskytovatele platformy, který software aktualizuje téměř neustále.

Záruky a jistoty může poskytovatel služeb nabízet pouze v rámci jeho možností. Někdy je ale potřeba, tak jako u osobních dat občanů celé České republiky, aby poskytovatel zaručil cokoliv, co budou úřady a ministerstva potřeboval, včetně určení mantinelů a případných viníků problému. Únik osobních údajů občanů by byl samozřejmě velký skandál, proto je potřeba počítat i s nejhorším, aby byl případně nalezen viník a vzniklá chyba, kerá vedla k úniku informací.

Virové hrozby a útoky hackerů. V dnešní době asi nejdiskutovanější téma. Zde nastává problém, poskytovatelé cloudu slibují naprostou bezpečnost a předkládají známá jména IT světových odborníků. Bohužel při klasickém soukromém řešení je sice menší pravděpodobnost ochrany proti DOS útokům, nicméně správce IT má nad bezpečností naprostou kontrolu a nemusí doufat, že se ke chráněným datům dostane nepovolaná osoba prostřednictvím chyb jiných lidí.

Obavy z bezpečnosti jsou sice hlavní brzdou masivního nástupu cloudů, ale chyba není na straně systému, nýbrž na straně uživatelů.

Podle průzkumu společnosti Deloitte byly letošní největší hrozby způsobeny uživateli:

- Využívání mobilních zařízení - 34 %
- Porušení bezpečnosti zahrnující případy třetích stran - 25 %
- Chyby a opomenutí zaměstnanců - 20 %
- Rychlou implementaci nových technologií - 18 %
- Zneužití informací a informačních systémů zaměstnanci - 17 %[5]
- Zaměstnanci ministerstev si možná svá zařízení a data na nich hlídají, ovšem níže postavení úředníci a zaměstnanci za přepážkou pravděpodobně nevěnují takovou pozornost ochraně svých dat. Na vině jsou ztracené nebo zapůjčené mobily, notebooky, tablety nebo flash disky. Řadoví zaměstnanci často nepřisuzují svým datům takovou vážnost, jakou ve skutečnosti mají. Nebezpečná je také rutina, která snižuje míru ostražitosti.

V případě manipulování s osobními daty mohou mít (např. uložené přihlašovací údaje v mobilu) nedozírné následky.

[5] DELOITTE. *Raising the Bar: 2011 TMT Global Security Study – Key Findings* [online]. 2011, 24 s. [cit. 2012-11-28]. Dostupné z: http://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/TMT/dttl_TMT%202011%20Global%20Security%20Survey_High%20res_191111.pdf

2.1 KIVS

Komunikační infrastruktura veřejné správy je vlastně sjednocení různých datových linek do jedné datové sítě. Jelikož se vše nachází v cloudu, je cílem KIVS poskytnout jednotlivým subjektům bezpečné a kvalitní připojení do společné sítě.

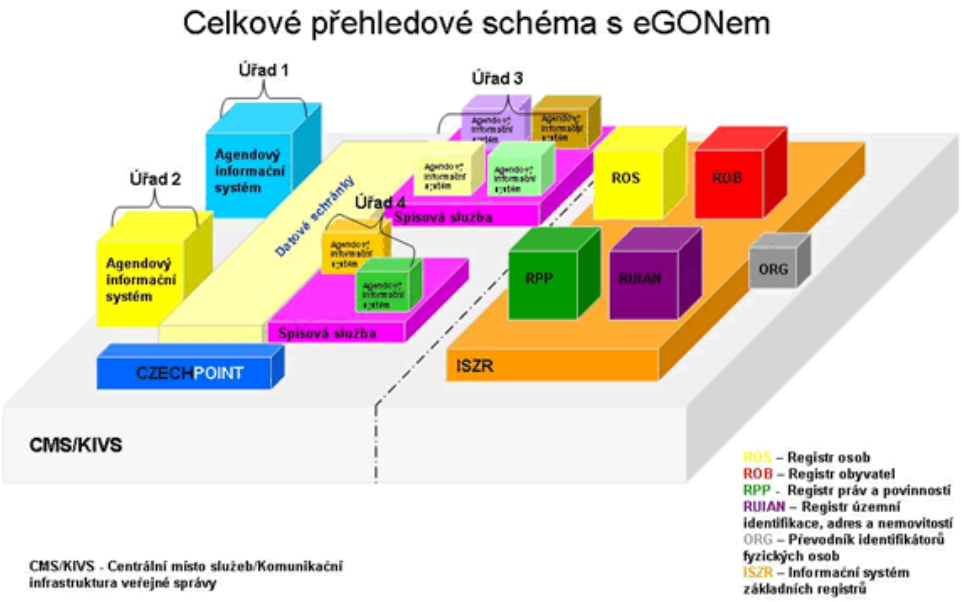


Schéma fungování základních registrů[6]

Podle schématu je jasné, že padne-li jeden ze základních stavebních kamenů v systému, znamená to, že všechny služby, které na něm stojí, jsou v ohrožení a mohou být kompromitovány nebo odpojeny také.

KIVS jak je vidět, je tedy nejdůležitějším prvkem celého systému. Jeho prostřednictvím jsou propojeny orgány veřejné správy například s Datovými schránkami, Czech POINTy nebo Základními registry.

CMS (Centrální místo služeb) je jedním z pilířů komunikační infrastruktury eGovernmentu. Zajišťuje komunikaci mezi státní správou a dalšími subjekty prostřednictvím internetu. Tvoří zároveň jediné místo, kde se propojují operátoři telekomunikačních infrastruktur, kteří poskytují služby v rámci KIVS.[7]

---

[6] *Ministerstvo vnitra České republiky* [online]. 2012 [cit. 2012-11-19]. Dostupné z: http://www.mvcr.cz/clanek/egon-symbol-egovernmentu-dokumenty-seznam-zakladnich-registru.aspx?q=Y2hudW09NQ%3D%3D

[7] *Ministerstvo vnitra České republiky* [online]. 2012 [cit. 2012-11-19]. Dostupné z: http://www.mvcr.cz/clanek/egon-symbol-egovernmentu-komunikacni-infrastruktura-verejne-spravy.aspx?q=Y2hudW09Mg%3D%3D

2.2 Datové schránky

Datové schránky jsou revolučním nástrojem komunikace mezi státní správou, výkonnými orgány a právnickými osobami. Podnikatelům a firmám je datová schránka zřizována automaticky ze zákona. Fyzické osoby si mohou o její zřízení zažádat dobrovolně.

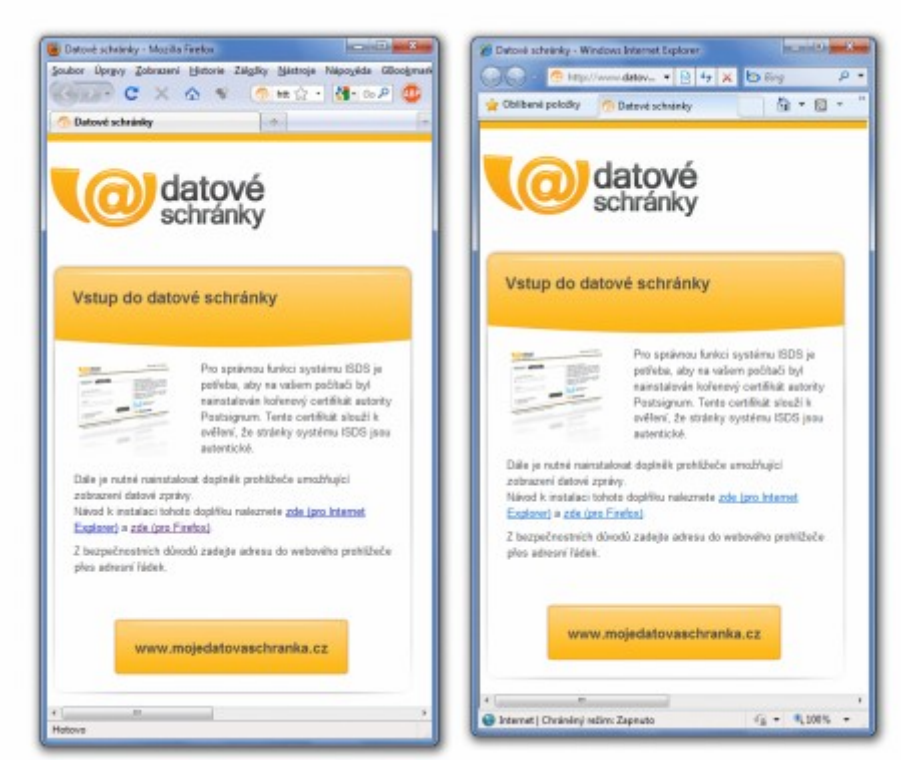
Tuto službu provozuje Česká pošta, avšak datové schránky zřizuje a spravuje Ministerstvo vnitra. Orgány veřejné moci mají tuto schránku samozřejmě také automaticky zřízenou. Seznam všech majitelů datových schránek lze najít na portálu veřejné správy (http://seznam.gov.cz), kde jsou vypsány orgány, právnické i fyzické osoby, vlastnící datovou schránku.

Služba je typickým příkladem cloud computingu. Datové schránky jsou uloženy na serverech v datacentru, takže Česká pošta k nim přistupuje vzdáleně. Je to asi jediné možné řešení, které je jednoduše proveditelné v rámci celé České republiky.

Pro přihlášení do datových schránek používá Česká pošta certifikáty s vlastní certifikační autoritou PostSignum. Při zřizování datové schránky je doporučováno dbát zvýšené pozornosti na bezpečnost.
Lidé si při přihlášení musí stáhnout certifikát, který lze samozřejmě stáhnout z webu ČP nebo MVČR, ale není to bezpečné. Navíc má spousta subjektů možnost podstrčit uživatelům falešné certifikáty a získat tak přístup do jejich schránky. Tyto certifikáty vyžadují k instalaci administrátorské přihlášení na počítači, což je další bezpečnostní riziko a pro mnohé zaměstnance ve firmě je to problém.Z minulosti jsou známy medializované případy, napadení účtu hackery a bezpečnostními firmami. První úspěšný průlom proběhl necelý měsíc po spuštění datových schránek.

Samotný princip datových schránek je opravdu povedený. Veškerá oficiální komunikace probíhá prostřednictvím nich a nedochází tak ke komplikacím a nedorozuměním. Na druhou stranu nelze věřit provozovateli, že je tato služba bezpečná.

Lidé, kteří si dřívě chtěli založit datovou schránku mohli být zmateni více podobnými odkazy, přičemž jediný pravý je www.mojedatovaschranka.cz. MVČR ani ČP nebyly schopni zablokovat alternativní adresy jako datovaschranka.info nebo datoveschranky.net a mnoho dalších. Mnozí neznalí občané naletěli podvodným stránkám, které nejen, že vypadaly jako pravé, ale chovaly se tak. Podobných phishingových stránek je spousta. Jejich autoři vymýšlejí různé kombinace na různých doménách a stát s nimi nic nenadělá. V dnešní době jsou naštěstí tyto falešné stránky zrušeny, takže při vyhledávání na internetu pravděpodobně narazí uživatel na správnou adresu. Po čase testování se rozhodlo ministerstvo zakomponovat do přihlašovacího procesu CAPTCHA kód, který by měl zamezit zkoušení přihlašovacích jmen a hesel do systému. Nepovedlo se jim však umístění této ochrany, protože se zobrazí až přihlášeným uživatelům, kteří použili správné jméno a heslo.



Podobnost pravé a falešné datové schránky[8]

Samotná nutnost instalace pluginu 602XML od soukromé firmy, o kterém nikdo neví, zda-li neobsahuje chyby nebo bezpečnostní díry, je při nejmenším podezřelá. Tento doplněk není kompatibilní s bezpečnostními prvky známých prohlížečů, ani nejrozšířenějšího operačního systému Windows. Provozovatel dokonce nabádá uživatele, aby při instalaci pluginu vypnuli tato bezpečnostní opatření a s administrátorskými právy se vydali na milost autorům doplňku.

Vzhledem k tomu, že stát nařizuje uživatelům datových schránek dodržování bezpečnostních pravidel a uchovávání uživatelských údajů v tajnosti, je již samotná instalace zcela nemožná.

2.3 Czech POINT

CZECHPOINT

Český Podací Ověřovací Informační Národní Terminál jehož cílem bylo vytvoření garantované služby pro komunikaci se státem prostřednictvím jednoho univerzálního místa. Je možné zde ověřovat dokumenty a listiny nebo data z veřejných i neveřejných informačních systémů. Dále se zde převádějí písemné dokumenty do elektronické formy a naopak. Mimo další služby, je tu i možnost ověřit si průběh správního řízení. Podobně jako Datové schránky

[8] Co je nedostatečně bezpečné? Datové schránky, nebo osvěta?. *Jiří Peterka: archiv článků a přednášek Jiřího Peterky* [online]. 2011 [cit. 2012-11-28]. Dostupné z: http://www.earchiv.cz/b09/b1126001.php3

je i tato služba součástí modelu sdílených IT prostředků (nebo-li cloudu). Opět jsou všechna data uložena v jednotném datovém centru, a všechny strany do něj přistupují vzdáleně. Všichni zde vidí stejné, sdílené informace.

Zabezpečení přihlášení do této služby zajišťuje kvalifikovaný a komerční certifikát. Tyto certifikáty musí být uloženy na externím nosiči (iKey). Tato varianta by měla zvýšit bezpečnost a pomoci lépe identifikovat pracovníky Czech POINTu, kteří se do systému přihlašují. Opak je ale pravdou. Tím, že se uživatelé přihlašují pomocí přenosného flash disku, je šance přihlášení neoprávněného uživatele o to větší. Opomenuta zůstala také osvěta mezi úředníky, kteří tento systém přihlašování používají. Mnozí nevědí jak certifikáty používat, jiní si píší svá hesla na papírek, který nosí společně s tokenem, nebo jej mají vylepený na monitoru. Kdyby se jednalo o jejich platební karty, nejspíše by se chovali jinak. Ovšem u tokenů je to stejné.

iKey[9]

Ještě horším prohřeškem je půjčování tokenů cizím osobám, které údajně ani nepracují na úřadě. Před těmito riziky varuje ministerstvo přímo na stránkách CzechPointu. V podstatě jde o závažnou chybu svěření úkolu zabezpečení nezasvěceným osobám, jako jsou řadoví zaměstnanci. Pokud není úřad schopen zaměstnance dostatečně proškolit v bezpečném používání tokenů, neměl by jim žádné svěřovat. Nevím tedy, jestli je takovéto použití certifikátů dalším krokem k zabezpečení nebo spíše chybou v podobě neproškolených zaměstnanců a nedodržování bezpečnostních opatření, týkajících se přenosných tokenů.

Vzhledem k tomu, že se na kontaktních místech CzechPointu mohou lidé dostat k takovým údajům jako je např. trestní rejstřík nebo centrální registr řidičů, dalo by se očekávat silnější zabezpečení.

Není to zase tak dávno, kdy bylo spuštěna pilotní verze informační služby infoPORT. Administrátoři nabídli všem uživatelům přístupy včetně veškeré dokumentace k systému. Prakticky kdokoliv si mohl systém zmapovat a nahrávat do něj libovolné soubory.[10]

Za prvé tady zásadně selhal lidský faktor a uspěchal své kroky bez promyšlení. Za druhé celý infoPORT je plný bezpečnostních chyb, které může zkušenější útočník lehce zneužít a dostat se tak ke správě základních registrů.

[9] *Systém online* [online]. 2012 [cit. 2012-11-19]. Dostupné z: http://www.systemonline.cz/it-security/autentizacni-tokeny-v-praxi.htm
[10] *Soom.cz* [online]. 2012 [cit. 2012-11-19]. Dostupné z: http://www.soom.cz/articles/print.php?aid=580&title=Zabiti-bezpecnosti-pilotnim-provozem

2.4 Základní registry

Základní registry veřejné správy jsou tzv. eGONův mozek. Sjednocují formu a údaje v databázích různých úřadů, čímž odstraňují i duplicitní a neaktuální záznamy.

SZR, neboli systém základních registrů je spojovacím bodem pro všechny přidružené agendy. Obsahuje jistý **referenční údaj**, který slouží jako identifikátor pro všechny další systémy. Tento údaj je považován za zaručený a proto není potřeba ho dále ověřovat. V podstatě jde o to, že základní registry budou jediná databáze osobních údajů občanů a bude provázána s ostatními systémy. Změnu ve všech agendách lze tedy provést jediným úkonem v SZR.

SZR se skládá celkem ze čtyř registrů. Registr obyvatel, Registr práv a povinností, Registr osob a Registr územní identifikace, adres a nemovitostí.[11]
Všechny tyto registry fungují v rámci Informačního systému základních registrů, který má na starosti Správa základních registrů. Správa základních registrů je tedy jeden z nejdůležitějších orgánů. Musí být samozřejmě také velmi dobře zabezpečen, protože právě zde mají zaměstnanci přístup ke všem osobním údajům všech občanů ČR. Ovšem tyto údaje nejsou viditelné jako čistý text, nýbrž jako identifikátor, který generuje převodník ORG. Ten přiděluje osobním datům identifikátor, se kterým úřady pracují. Osobní údaje si tedy nemůže zobrazit každý.

Je třeba se bát?

Na jednu stranu se cloudové řešení v tak rozsáhlém měřítku vyplatí. Lidé nebudou muset každou změnu hlásit na více různých míst a úředníci nebudou muset řešit zmatky v rozdílných údajích v databázi a na formulářích. Zdánlivě ideální řešení však sebou přináší i jistá rizika. Pokud se totiž profesionální hacker se špatnými úmysly dokáže dostat k datům v základním registru, nejen že může zjistit veškeré osobní informace o každém spoluobčanovi, navíc bude moci s daty i manipulovat. Je třeba si uvědomit, že každý systém je napadnutelný. Na druhou stranu k provedení úspěšné infiltrace Základních registrů by byl potřeba tým těch nejzkušenějších profesionálů. Reálná hrozba zde ale nehrozí, proto můžeme zůstat v klidu.

Čistě teoreticky by šlo s takto nastaveným systémem, vymazat elektronickou identitu jakéhokoliv uživatele. Prakticky to tak jednoduché není a přece jen, existuje stále mnoho způsobů, jak dokázat svoji pravou identitu. Samozřejmě to ale není omluva pro fakt, že „oběť“ by musela dlouho a pracně dokazovat svoji identitu, obnovovat neplatné doklady. Vymazaný člověk by nemohl ani uzavírat žádné smlouvy, nejspíše ani vlastnit bankovní účet. Tohle jsou samozřejmě jen katastrofické scénáře, nicméně nelze je brát na lehkou váhu.

[11] *Ministerstvo vnitra České republiky* [online]. 2012 [cit. 2012-11-19]. Dostupné z: http://www.mvcr.cz/clanek/zakladni-registry-verejne-spravy.aspx

Správa základních registrů totiž opravdu není zrovna nejzabezpečenější. Ještě před pár měsíci bylo objeveno několik chyb, které umožňovaly Cross Site Scripting, čehož by leckdo schopný mohl zneužít k phishingu nebo odchytávání přístupových údajů.

3 Prevence

Systémy v cloudu lze zabezpečit různými antivirovými a antispamovými programy. Samozřejmě, že existují i bezpečná a výhodná řešení v cloudu, čehož pravděpodobně eGON využívá a pokud ne, měl by. Pokud je ochrana před spamem a kontrola dat převedena na poskytovatele služby, stát tím ušetří nemalé peníze a čas. Převodem antispamové a antivirové ochrany do cloudu ušetří každá firma, která svá data svěřuje cloudu. Tato řešení bývají často spolehlivější než běžný firewall. Nicméně musím zdůraznit, že takový poskytovatel musí být prověřený, protože má přístup k veškeré korespondenci a datům.

Lidský faktor také nelze podceňovat. Jak už řekl Albert Einstein: „*Jen dvě věci jsou nekonečné – Vesmír a lidská hloupost. Tím prvním si ale nejsem zcela jist.*“

Pokud jsou svěřeny zaměstnancům veřejné správy naše osobní a citlivé údaje, musí být tito uživatelé zaškoleni IT odborníky a otestováni svými manažery. Nelze čekat na první případ, kdy se něčí data dostanou do nepovolaných rukou, to už bude pozdě.

4 Závěr

Přechod na cloud je v každém případě vždy spekulativní. Soukromé subjekty jistě k této problematice musí přistupovat jinak než státní správa. Největším otazníkem, jestli přejít nebo nepřejít na poskytované služby, je stále bezpečnost. Vzhledem k citlivosti dat, o která tu jde především, je dle mého názoru tento nástup cloudu příliš rychlý a organizace není spolehlivě doladěna. Stále je největším zdrojem diskreditace lidský faktor, což cloudu samo o sobě neuškodí. Problém je však v datech, která mohou být kompromitována a jejich rozsah.

Téměř vždy je potřeba počítat s těmi nejhoršími scénáři a připravit se na ně. Pokud se budou dodržovat bezpečnostní pravidla a zaměstnanci budou průběžně kontrolováni a upozorňování na bezpečnostní hrozby, nic nebrání poklidnému vývoji eGovernmentu.

Seznam literatury

1. *Ministerstvo vnitra České republiky* [online]. 2012 [cit. 2012-11-26]. Dostupné z: http://www.mvcr.cz/clanek/cesty-k-egovernmentu.aspx
2. *Moravské hospodářství* [online]. [cit. 2012-11-15]. Dostupné z: http://www.moravskehospodarstvi.cz/clanky/legislativa/prehled-zakonu-v-oblasti-egovernmentu/
3. Vnitro chystá využít pro eGovernmentu „cloud computing“ – budou další zakázky pro firmy?. In: *EGov.cz: Nezávislý informační portál* [online]. 2011 [cit. 2012-11-28]. Dostupné z:

http://www.egov.cz/index.php?option=com_content&view=article&id=187:vnitro-chysta-vyuit-pro-egovernmentu-cloud-computing-budou-dali-zakazky-pro-firmy&catid=1:egovernment&Itemid=3
4. KPMG. *Clarity in the Cloud: A global study of the business adoption of Cloud* [online]. 2011, 48 s. [cit. 2012-11-28]. Dostupné z: http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cloud-clarity.pdf
5. DELOITTE. *Raising the Bar: 2011 TMT Global Security Study – Key Findings* [online]. 2011, 24 s. [cit. 2012-11-28]. Dostupné z: http://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/TMT/dttl_TMT%202011%20Global%20Security%20Survey_High%20res_191111.pdf
6. *Ministerstvo vnitra České republiky* [online]. 2012 [cit. 2012-11-19]. Dostupné z: http://www.mvcr.cz/clanek/egon-symbol-egovernmentu-dokumenty-seznam-zakladnich-registru.aspx?q=Y2hudW09NQ%3D%3D
7. *Ministerstvo vnitra České republiky* [online]. 2012 [cit. 2012-11-19]. Dostupné z: http://www.mvcr.cz/clanek/egon-symbol-egovernmentu-komunikacni-infrastruktura-verejne-spravy.aspx?q=Y2hudW09Mg%3D%3D
8. Co je nedostatečně bezpečné? Datové schránky, nebo osvěta?. *Jiří Peterka: archiv článků a přednášek Jiřího Peterky* [online]. 2011 [cit. 2012-11-28]. Dostupné z: http://www.earchiv.cz/b09/b1126001.php3
9. *Systém online* [online]. 2012 [cit. 2012-11-19]. Dostupné z: http://www.systemonline.cz/it-security/autentizacni-tokeny-v-praxi.htm
10. *Soom.cz* [online]. 2012 [cit. 2012-11-19]. Dostupné z: http://www.soom.cz/articles/print.php?aid=580&title=Zabiti-bezpecnosti-pilotnim-provozem
11. *Ministerstvo vnitra České republiky* [online]. 2012 [cit. 2012-11-19]. Dostupné z: http://www.mvcr.cz/clanek/zakladni-registry-verejne-spravy.aspx