

## VI. konference ČIMIB

# Cloud computing a bezpečnost

21. června 2011

Hotel Continental, Brno



# Aktuálne právne normy SR a ČR v oblasti CC

**Ing. Peter Valkovič, CME**

**PRIVATBANKA a.s.**



- **Nastavenie podmienok poskytovania služieb CC je ako majstrovstvo namiešať z desiatok komponentov nie len dobrý kokteil, to dnes už nemôže stačiť, ale prosto povedané vynikajúci kokteil.**
- **A preto potrebujeme super správny recept.**
- **A tento recept ja fakticky perfektne pripravená Zmluva o CC opretá o reálne platné právne normy (ako komponenty) a špeciálne dochutená „best practices“.**
- **Základné piliere zdravého sedliackeho ropzumu dnes nestačia. Dôveruj ale preveruj - Dvakrát meraj a raz strihaj. Kto druhému jamu kope sám do nej padá.**



- **Miešame teda kokteil s cieľom WIN-WIN**



**Najčastejšou príčinou narušenia dôvernosti, integrity a predovšetkým dostupnosti údajov, celom svojom životnom cykle, ktoré sú teda v cloude uložené a služieb, ktoré cloud nad týmito údajmi poskytuje, sú najmä:**

- **personálna bezpečnosť - chyby samotných zamestnancov, ktorí nedodržia bezpečnostné predpisy, chovajú sa nezodpovedne, chyby samotných aplikácií, bez dôsledného testovania na známe zraniteľnosti sú presunuté do cloudu, tieto spravidla neboli vyvíjané pre prácu v CC,**
- **fyzická aj personálna bezpečnosť poskytovateľov CC - zlyhanie bezpečnosti u poskytovateľa (Failure in Provider Security) –útok iného užívateľa (Attacks by Other Customers)**



- **informačná bezpečnosť vo vnútri CC (jeden nepodarený server napadnutý malware), zabezpečenia oneskorenia sieťových paketov cez internet,**
- **Ochrana osobných údajov,**
- **Dostatok výpočtových zdrojov aj pri paralelnom behu veľmi náročných výpočtov,**
- **Zabezpečenie vysokej dostupnosti zdrojov aspoň z dvoch geograficky oddelených a dostatočne vzdialených lokalít,**
- **Súlad so SOX (Sarbanes-Oxley) a iných štandardov, best practices,**
- **Hrozba monokultúry unifikovaných OS (typicky Microsoft) – mohutné dávka opravných balíčkov môžu položiť služby CC,**



- Hrozba unifikovaného hardware,
- Korektné licencovanie software v CC prostredí (garancie vyžadovať zmluvne od dodávateľa SW)
- Zabezpečiť výhodné financovanie software,
- Zabezpečiť detailnú špecifikáciu pojmov BCM – kritické systémy, kritické funkcie, časové horizonty RPO, RTO, MTO, minimálna úroveň akceptovaných služieb,
- Prevádzka služieb 24x7x365, alebo 8x5, 12x5



- zákon č. 513/1991 Zb., OBCHODNÝ ZÁKONNÍK,
- EULA (End User License Agreement)
- zákon č.618/2003 Z.z. Autorský zákon - v SR (sa riadi legislatívou štátu, kde je CC a DC dislokovaný – Írsko, Kanada, Anglicko, Sibír, Washington)
- Usmernenie NBS č.6/2004 Z.z. o outsourcingu bankami
- zákon č.428/2002 Z.z. o ochrane osobných údajov, údaje identifikujúce fyzické osoby, súlad musí zabezpečiť poskytovateľ CC a zákazník,
- zákon č.215/2004 Z.z. o ochrane utajovaných skutočností,
- zákon č.301/1995 Z.z. o rodnom čísle,



- zákon č.483/2001 Z.z. o bankách,
- zákon č. 22/2004 Z. z. o elektronickom obchode,
- Usmernenie NBS č.39/2004 Úseku bankového dohľadu NBS (7/2004) k overeniu bezpečnosti informačného systému banky a pobočky zahraničnej banky,
- Fyzická bezpečnosť DC CC – stavebný zákon
- Ekologická bezpečnosť DC CC - VYHLÁŠKA MŽP SR č.315/2010 Z.z. o nakladaní s elektrozariadeniami a s elektroodpadom,
- Zákon č.610/2003 Z.z. o elektronických komunikáciách,
- Výnos MF SR č. 013261/2008-132 o štandardoch pre informačné systémy verejnej správy



- **Metodický pokyn 87/2008 k výnosu Ministerstva financií Slovenskej republiky č. MF/013261/2008-132 o štandardoch pre informačné systémy verejnej správy**
- **Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy, posledná novela č.570/2009 Z.z.**
- **Základné normy v pôsobnosti Národného bezpečnostného úradu sú Nariadenie vlády č.216/2004 Z.z. ktorým sa ustanovujú oblasti utajovaných skutočností, niektoré vyhlášky NBÚ upravujúce ochranu utajovaných skutočností, Vyhláška NBÚ č.325/2004 Z.z. o priemyselnej bezpečnosti, Vyhláška NBÚ č.331/2004 Z.z. o personálnej bezpečnosti a o skúške bezpečnostného zamestnanca, Vyhláška NBÚ č.336/2004 Z.z. o fyzickej bezpečnosti a objektivej bezpečnosti, Vyhláška NBÚ č.337/2004 Z.z. ktorou sa upravujú podrobnosti o certifikácii mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov a o ich používaní, Vyhláška NBÚ č.338/2004 Z.z. o administratívnej bezpečnosti, Vyhláška NBÚ č.339/2004 Z.z. o bezpečnosti technických prostriedkov a Vyhláška NBÚ č.340/2004 Z.z. ktorou sa ustanovujú podrobnosti o šifrovej ochrane informácií.**



Pre ČR sú to najmä:

- Zákon č.101/2000 Sb. o ochrane osobných údajov
- Zákon č.21/1992 Sb., o bankách, (bankové tajomstvo)
- Vyhláška ČNB č.123/2007 Sb., o pravidlech obezřetného podnikání bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry,
- ÚŘEDNÍ SDĚLENÍ ČNB k outsourcingu bankami
- Zákon č.277/2009 Sb. o pojišťovnictví
- Zákon č.127/2005 Sb. o elektronických komunikáciách



## Iné normy a Best Practices

- Sarbanes-Oxley (SOX) Sarbanes Oxley Act, [www.soxlaw.com](http://www.soxlaw.com), [www.sarbanes-oxley.com](http://www.sarbanes-oxley.com), [www.sarbanes-oxley-forum.com](http://www.sarbanes-oxley-forum.com), škandál okolo fy Enron bol dôsledkom – vzniku zákona vydaného Kongresom Spojených štátov amerických v roku 2002 a má veľmi významnú platnosť u organizácií, ktoré síce podliehajú legislatíve Spojených štátov, ale musia sa ním i v našom prostredí (rozumej ČR+ SR) riadiť rad globálne pôsobiacich spoločností.
- Security Guidance for Critical Areas of Focus in Cloud Computing (2009)
- Assessing the Security Risks of Cloud Computing (2008) Gartner
- Hype Cycle for Cloud Computing (2009) Gartner
- Sada noriem ISO/IEC 27000 – Information Security Management Systems – ISMS – celosvetovo najrozšírenejší štandard, model na zostavenie, implementáciu, prevádzku, monitorovanie, revíziu a zlepšovanie ISMS (kreuje sa od roku 2005),



## Niektoré zdroje

- [www.cloudsecurityalliance.org](http://www.cloudsecurityalliance.org)
- [www.c-ebs.org](http://www.c-ebs.org) Guidelines on Outsourcing (CEBS); 2006;
- [www.bis.org/bcbs/jointforum.htm](http://www.bis.org/bcbs/jointforum.htm) Outsourcing in Financial Services; Joint Forum (JF); 2005;
- [www.bis.org](http://www.bis.org) Sound Practices for the Management and Supervision of Operational Risk; (BCBS); 2003;
- <http://groups.google.com/group/cloudsecurityalliance>



## Základné články dobrej Zmluvy o CC

- Základné ustanovenia
- Pojmy
- Predmet plnenia
- Miesto plnenia
- Platnosť zmluvy a termíny plnenia
- Spôsob plnenia
- Cena plnenia
- Platobné podmienky
- Práva a povinnosti zmluvných strán
- Riešenie sporov
- Zmluvné pokuty
- Záverečné ustanovenia
- Prílohy

**Dobrá zmluva detailne stanovuje všetky pojmy, práva a povinnosti, časové a vecné rámce, hodnoty pre BCP/DRP, spôsob riešenia sporov. Draft zmluvy je možné požiadať u autora.**

**Dobrá zmluva obsahovo môže mať aj viac ako 50 strán.**

Teraz sa rozídeme do svojich  
alchymistických dielní a  
začneme miešať vlastné  
receptúry...



Ďakujem za pozornosť, podnety  
prijímam:

- [valkovic@privatbanka.sk](mailto:valkovic@privatbanka.sk)
- [pedro.valkovic@gmail.com](mailto:pedro.valkovic@gmail.com)