Bezpečnost a podnikový cloud computing II.

Průzkum social listeningu z internetu
zpracovaný pro společnost Cloud4com a Intel

Cloud4com®

Security
Without Compromise.

intel XEON inside™

Intel® Xeon® processors

31. října 2016

Yeseter

Obsah dokumentu

Yeseter – Vyskočilova 1326/5a, 140 00 Praha 4, Česká republika, Tel.: +420 283 061 281, E-mail: info@yeseter.com,
URL: http://www.yeseter.com

1. Shrnutí

Tato studie je zaměřena na problematiku bezpečnosti podnikového cloud computingu, jak se o ní píše a hovoří v prostředí severoamerického, západoevropského a českého kontextu na internetové platformě diskuzních fór a sociálních sítí. Jedná se o rozpracování původní studie z 11. května 2016 v oblasti bezpečnosti cloudu pro stejného zadavatele Cloud4com. Toto doplnění proběhlo ve dvou dalších studiích, přičemž první z 27. července 2016 byla zaměřená na bezpečnost cloudu v zemích Západní Evropy, Severní Ameriky a České republiky, druhá, právě předkládaná, na hardwarovou bezpečnost v cloudu v internetovém prostředí Severní Ameriky a částečně Velké Británie a Německa.

Bezpečnostní témata definovaná zadavatelem v první vlně:

Bezpečnost v cloudu
Bezpečnost virtuálních datových center
Bezpečnost uložených dat v cloudu
Ochrana osobních údajů v cloudu
Zabezpečeni dat v cloudu
Šifrovaní dat uložených v cloudu
Šifrovaní virtuálních serveru
Šifrovaní virtuálních disku
Legislativa a cloud
Zákonné úpravy cloudu
Pojištěni poskytovatelů proti odcizeni dat
Zneužiti dat v cloudu
Odcizení dat z cloudu
Umístěni datových center poskytovatelů
Fyzická bezpečnost datových center
Nebezpečí uloženi dat v podnicích

Tyto položky jsou v dokumentu prezentovány v kapitolách 2. až 9.

Bezpečnostní témata definovaná v druhé vlně:

Hardware-based server security
Hardware security-accelerated cloud
Hardware secured cloud
Geo-fencing
Geo-tagging
Trusted boot in the cloud

Tyto položky jsou v dokumentu prezentovány v kapitolách 10. až 13.

Veřejný diskurs jsme pro obě vlny sledovali v období sedmi měsíců – od 1. ledna až 25. července 2016. Za sledované období bylo prozkoumáno přes **25 tisíc** příspěvků z **USA, sedm tisíc** příspěvků ze **západní Evropy** (Velká Británie, Francie, Nizozemí, Belgie a Německo) **a 400 tuzemských příspěvků** na téma podnikové cloud computing bezpečnosti a hardwarové bezpečnosti podnikového cloud computingu**.**

Pod příspěvkem lze rozumět článek na zpravodajském serveru, blogu, dále komentáře pod článkem, blogem, v diskusním fóru a na sociálních sítích LinkedIn, YouTube, Facebook či Google+ a rovněž i pípnutí (tweet) na sociální síti Twitter.

Yeseter – Vyskočilova 1326/5a, 140 00 Praha 4, Česká republika, Tel.: +420 283 061 281, E-mail: info@yeseter.com,
URL: http://www.yeseter.com

2. Úvod

Bezpečnost stále populárnějšího cloud computingu je jednou z nejnaléhavějších výzev současného světa informačních technologií. Poškození či ztráta dat je nejen nákladná na opravu, ale může vážně poškodit pověst podniku.

Původní nabídka cloudových služeb z počátku století si pochopitelně z bezpečnostními předpisy hlavu příliš nelámala. To byl i jeden z hlavních důvodů, proč se celá řada podniků do cloudu příliš nehrnula. Od té doby se však mnohé změnilo. Poskytovatelé cloudových služeb v současnosti věnují bezpečnostním faktorům zvýšenou pozornost a lze konstatovat, že situace se v tomto směru poněkud obrátila. Bezpečnost v cloudu poskytovaných služeb bývá často výrazně vyšší než bezpečnost, kterou si zajišťují na firemní úrovni on-premise sami uživatelé. Ti často nemají potřebné znalosti, finanční prostředky nebo prostě čas zabývat se bezpečnostní politikou v potřebném rozsahu, protože primárně řeší otázky informatiky spojené s vlastním podnikáním.

Proč utrácet tyto drahocenné prostředky na hledání lepších způsobů ochrany, když se tomu poskytovatelé služeb věnují soustavně a na profesionální úrovni?

Průzkumy zabývající se bezpečností politikou ve firemním prostředí hovoří o tom, že podniky, které v minulosti investovali do cloudového prostředí mají dnes o pětinu (přesněji 22 procent) nižší výdaje na bezpečnost, než ty, co zůstávají v tradičním on-premise režimu. Příčinou je tzv. zabudovaná bezpečnost (built-in-security) poskytovatelů cloudů, kteří soustavně a programově vylepšují bezpečnostní zajištění poskytovaných služeb.

Patří sem:

- vysoká úroveň fyzické ochrany
- kontrola identity a přístupu
- systémy správy a vyhodnocování logů a automatická inspekce
- kryptografická ochrana, šifrování, uložených a přenášených dat
- síťové a aplikační firewally (paketové filtry, aplikační brány)
- anti-DDoS ochrana (hardware a služby)
- systémy pro správu a konfiguraci IS redukující chyby způsobené lidským faktorem

Yeseter – Vyskočilova 1326/5a, 140 00 Praha 4, Česká republika, Tel.: +420 283 061 281, E-mail: info@yeseter.com,
URL: http://www.yeseter.com

3. Přínosy a rizika cloud computingu v oblasti bezpečnosti

Na nabídku a řešení cloud computingu jsme si zvykli nahlížet spíš z pozice možných rizik pramenících zejména v oblasti bezpečnosti. Není na tom nakonec nic špatného, lepší je zde opatrnost, než bezbřehý optimismus. Nedůvěra k bezpečnosti cloudu nakonec přinutila poskytovatele k mnoha zlepšením v oblasti technologické – a rovněž i legislativní.

Jistou roli v šíření této celkové skepse hrálo a stále ještě může hrát několik, řekněme, politických faktorů. Těmi se v tomto dokumentu nebudeme zabývat, pouze je zmíníme a necháme na čtenářově úsudku, zda jsou oprávněné a pro něj relevantní. S příchodem nových technologických firem a nabízených cloudových řešení se proti nim, celkem nepřekvapivě, zvedla vlna odporu, která se často zaštiťovala právě bezpečností firemního provozu. Velkou měrou se o to zasadily významné technologické společnosti, jež nebyly na cloud připravené. Další odpůrci cloudu se šikovali z řad firemních útvarů, které cítily v cloud computingu buď svého konkurenta, nebo faktor omezující jejich kompetence. Byly to zejména pracovníci IT a nákupních oddělení, kteří se cítili v ohroženi.

Pohled na bezpečnost cloud computingu se pomalu začíná měnit. Organizace se k jeho poskytovatelům začínají stavět více partnersky a přicházejí k poznání, že zajištění bezpečnosti v cloudu nabízí často mnohem širší paletu možností, než jakou dokáží zavést ve svém vlastním prostředí.

Níže zmiňované možné přínosy a rizika nazírají na cloud po stránce technologické. Legislativním aspektům, které by rovněž mohly figurovat na obou stranách tohoto dělení je věnována samostatná kapitola.

Bezpečnost cloudu: Přínosy a rizika	
Přínosy	**Rizika**
Vysoká míra zabezpečení (built-in)	Ztráta dat
Certifikace a audit prostředí	Narušení dat
Pravidelné školení obsluhy	Zcizení uživatelského účtu
Centrální přístup	Nechráněná rozhraní a API
Zálohy a obnovy	Zcizení služby
Expertní podpora	Zhrzení zaměstnanci
Vícenásobná autentizace	Zneužití cloudu
Verzování a patching	Nedostatečný vstupní audit
Fyzická bezpečnost	Sdílené technologické chyby

Přínosy cloud computingu na poli bezpečnosti

Vysoká míra zabezpečení, Built-in Security

Firmy v prostředí cloudu vynakládají až o pětinu nižší finanční prostředky na bezpečnost, než organizace, které zůstávají na tradiční domácí on-premise platformě. Příčinou je zabudovaná bezpečnost (built-in security) poskytovatelů cloudů, kteří soustavně a programově vylepšují bezpečnostní zajištění poskytovaných služeb.

Certifikace, audity a školení

Yeseter – Vyskočilova 1326/5a, 140 00 Praha 4, Česká republika, Tel.: +420 283 061 281, E-mail: info@yeseter.com,
URL: http://www.yeseter.com

Poskytovatelé cloudu musí splňovat velmi přísné certifikáty ISO, absolvovat pravidelné bezpečnostní audity a školení zaměstnanců. Toto nemusí být úplnou samozřejmostí u celé řady podniků s vlastními útvary IT.

Centrální přístup
Centralizované držení citlivých firemních dat v cloudu – a ne například v mobilních zařízeních zaměstnanců – umožňuje uživatelský přístup z libovolného místa. Navíc ztráta pracovního notebooku, který neobsahuje žádná podniková data, protože ta se nacházejí někde v cloudu, významně snižuje bezpečnostní rizika.

Zálohy a obnovy
Hlavní bezpečnostní výzvy v organizacích se zaměřují na krádeže a znepřístupnění dat. Tomu jde ovšem cloud computing vstříc, zejména tím, že mnohé zjednodušuje a zefektivňuje díky své nativní způsobilosti mít více verzí jednoho zdroje uložené různými metodami – včetně záloh.

Expertní podpora
Pokud podnik přesouvá své výpočetní úkoly do cloudu, měl by mít jistotu zajištění a bezpečí. Musí si být jistý volbou vhodné strategie směrem k vlastní bezpečnosti – v souladu se současnými trendy a technologiemi pro jejich zajištění. To ještě neznamená, že do cloudu budou převedeny všechny aplikace najednou – a že vše v cloudu bude podléhat stejným bezpečnostním předpisům. Poskytovatelé drží krok s dobovými bezpečnostními trendy, zatímco pro řadu podniků je toto kritérium nesplnitelnou metou z hlediska absence vlastních odborníků i plánovaných rozpočtů.

Vícenásobná autentizace
Nazývaná též Multifactor Authentication (MFA) je nabízena mnoha poskytovateli cloudu a zajišťuje celou řadu kombinací ověřovacích a identifikačních procedur, na než mnoho podniků z pohledu vlastního zavedení dosáhne jen stěží, ať už z důvodu časových možností, peněz nebo dovedností.

Bezpečnostní patching
Upgrady a záplatování stávajících verzí programového vybavení je často uživateli podceňováno a přehlíženo. V proměnlivém prostředí stále nových a nových bezpečnostních incidentů však hraje klíčovou roli. Mnoho běžně používaných softwarových produktů vyžaduje zodpovídající každodenní péči. S instalací bezpečnostních záplat rovněž úzce souvisí i jejich testování a jistota, že byly řádně uplatněny.

Fyzická bezpečnost
Poskytovatelé cloudu s největší pravděpodobností disponují systémy a zařízeními, jež jsou vybaveny mnohem výkonnějšími a fungujícími mechanizmy pro správu fyzické bezpečnosti.

Rizika cloud computingu na poli bezpečnosti

Narušení dat, Data Breach
Narušení dat je bezpečnostní incident, při kterém jsou citlivé, střežené nebo důvěrné informace zpřístupněny, prohlíženy, odcizeny nebo jinak zneužity subjektem, který k tomu není oprávněn. Narušení dat může být primárním terčem cíleného útoku, nebo se prostě může

Yeseter – Vyskočilova 1326/5a, 140 00 Praha 4, Česká republika, Tel.: +420 283 061 281, E-mail: info@yeseter.com,
URL: http://www.yeseter.com

jednat o selhání lidského činitele, též aplikační zranitelnost nebo nedostatečné praktiky a postupy při jejich zabezpečení tu hrají roli.

Ztráta dat, Data Loss

V cloudu může docházet ke ztrátám dat nejenom z důvodu škodlivých útoků (malicious attacks), ale i náhodným smazáním dat poskytovatelem cloudové služby, resp. tzv. vyšší mocí (požár, povodeň, zemětřesení). To vše může vést k trvalé ztrátě zákaznických dat, pokud poskytovatel nebo uživatel cloudu nezvolí vhodné postupy pro zálohování dat, zachování kontinuity provozu, obnovení dat po havárii – a rovněž i jejich denní zálohování, případně ukládání mimo pracoviště běžného provozu. Data lze považovat za ztracená, například při zhroucení diskové jednotky, když majitel nemá k dispozici zálohu. Jiným příkladem může být ztráta klíče k dešifrování dat.

Zcizení uživatelského účtu

Odcizení účtu nebo služby není žádnou novinkou. Hovoří se tu též o tzv. černé labuti (black swan), tedy události, kterou lze jen těžko předvídat či očekávat. Útočné metody typu phishing a jiné podvody a zneužívání, využívající softwarovou zranitelnost, se svým tvůrcům zatím stále vyplácejí. Opakované používání hesel a bezpečnostních přístupů uživateli, násobí dopady těchto útoků. Cloudová řešení přirozeně vnesla do této oblasti další hrozby. Pokud útočník získá přístup k uživatelským pověřením, může manipulovat nejenom s daty, ale i transakcemi a dalšími aktivitami. Může poskytovat falešné informace nebo přesměrovat klienty do ilegálních míst. Nelegálně získaný uživatelský účet umožní útočníkovi dostat se do zákaznické zóny, kde jsou tím pádem ohroženy všechny nasazené služby.

Nechráněná rozhraní a API

Bezpečnost a dostupnost obecných cloudových služeb souvisí s bezpečností základních rozhraní, jež poskytovatelé cloudů dávají k dispozici svým uživatelům. Ať už jde o sady uživatelských rozhraní (UI) nebo programovatelná aplikační rozhraní (API), která zákazníci používají k nastavení služeb, jejich správě, interakci a monitoringu. Pro autentizaci i kontrolu přístupu, šifrování a podporu monitoringu musí být tato rozhraní navržena tak, aby zajistila spolehlivou ochranu – jak proti náhodným, tak i úmyslným pokusům při obcházení bezpečnostních politik.

Zcizení služby, Denial of Service, DoS

Útoky na zcizení služby jsou útoky, jejichž cílem je zabránit uživatelům v přístupu k datům nebo k aplikacím. U zacílených cloudových služeb si útočník vynucuje zvýšenou konzumaci nadměrného množství systémových prostředků typu: napájení procesoru, kapacitu pamětí a diskových prostorů nebo síťového připojení. Způsobují tím neúnosné zpomalení systému a dob odezvy, jež vystavují legitimní uživatele velké míře frustrace a naštvání z důvodu nefunkčnosti služeb. Pokud je útočníků více, hovoříme o distribuovaných útocích na zcizení služby (DDoS). Tyto útoky jsou už na hranici počítačové kriminality, nedochází tu však ke krádežím, ale spíš k počítačovému vandalství, kdy dochází k poškození nebo znepřístupnění služby.

Zhrzení zaměstnanci

Rizika způsobená někým z vlastní organizace jsou v bezpečnostním průmyslu diskutována poměrně často. Může se jednat o bývalé i současné nepřející zaměstnance, kontraktory, resp. partnery, kteří stále vlastní autorizované přístupy k určitým cloudovým službám. Někdy bývá tento jev označován též jako zlá krev.

Yeseter – Vyskočilova 1326/5a, 140 00 Praha 4, Česká republika, Tel.: +420 283 061 281, E-mail: info@yeseter.com,
URL: http://www.yeseter.com

Zneužití cloudu
Běžnými charakteristikami zneužití cloudových služeb bývají falešné profily při nastavování cloudových služeb, podvodné zkušební trial služby, narafičené registrace a platební brány, spamování po e-mailu, phishingové kampaně.
Nedostatečný vstupní audit
Podrobná analýza a zhodnocení veškerých přínosů a rizik musí být zakomponována do každého strategického rozhodnutí organizace ohledně budoucího využívání služeb cloud computingu. Tato klíčová fáze je občas nazývána rovněž jako studie due diligence s jasně definovanou metodikou.

Sdílené technologické chyby
Sdílené prostředí cloudu vychází ze základního předpokladu, že výpočetní zdroje jsou využívány všemi uživateli. Nevhodné konfigurace aplikace nebo operačního systému ohrožují celou infrastrukturu a mohou vést k narušení bezpečnosti pronajímatelů cloudu. Sdílené služby, sdílené databáze nebo vyrovnávací paměti (cache) procesorů jsou v ohrožení. Tyto hrozby narušení infrastruktury mohou celkově oslabit ochranu osobních údajů.

Tabulka představuje jednotlivé typy bezpečnostních útoků a s nimi spojené hrozby.

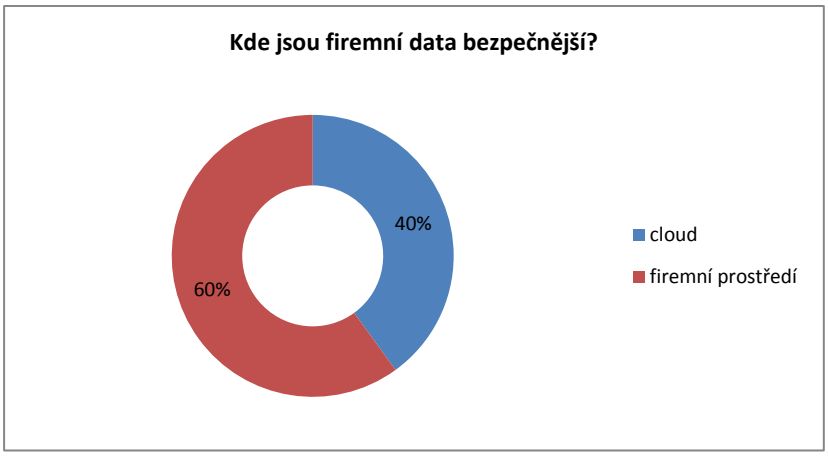
Typy útoků a hrozby s nimi spojené		
P. č.	**Typ útoku**	**Bezpečnostní hrozby**
1	Ztráta dat	dostupnost, integrita
2	Narušení dat	důvěrnost, únik informací
3	Zcizení uživatelského účtu	autentizace, integrita, diskrétnost, nepopiratelnost, falšování dat, dostupnost, spoofing, výsadní narušení
4	Nechráněná rozhraní a API	autentizace, integrita, důvěrnost, falšování dat
5	Zcizení služby	dostupnost, zcizení služby
6	Zhrzení zaměstnanci	spoofing, falšování, únik informací
7	Zneužití cloudu	narušení provozu, porušení SLA
8	Nedostatečný vstupní audit	autentizace, integrita, diskrétnost, nepopiratelnost, falšování dat, dostupnost, spoofing, výsadní narušení
9	Sdílené technologické chyby	únik informací, výsadní narušení

Poznámka: *spoofing – záměna identity*

Yeseter – Vyskočilova 1326/5a, 140 00 Praha 4, Česká republika, Tel.: +420 283 061 281, E-mail: info@yeseter.com,
URL: http://www.yeseter.com

4. Bezpečnost dat v cloudu a ve firemním prostředí

Mírný posun v prospěch cloudu (asi o pět procent) lze oproti minulosti (Q1-2015 vs. Q1-2016) sledovat u dotazu, zda firemní pracovníci mají větší důvěru v bezpečnost dat uložených mimo vlastní organizaci – před jejich správou v domácím podnikovém prostředí. Otázka poměrně prostá, ovšem s odpovědí to už tak snadné není. Nicméně cloudová řešení a DC začínají být pozvolna považována i firemními IT profesionály za místa s větší mírou expertízy a v neposlední řadě i technických možností. Přispívá k tomu stále narůstající počet firemních dat a potřeba jejich zpracování. Navíc je otázkou, jestli firemní data v době BYOD jsou skutečně pouze a jenom ve správě a pod výhradní kontrolou vlastní organizace.



Přínosy cloudových řešení zhlediska bezpečnosti lze zejména spatřovat:

- přístup k nejnovějším technologiím
- garance dostupnosti
- odbornost a know-how
- zvládnuté metodiky a postupy
- praktická neudržitelnost bezpečnostních politik na firemní úrovni
- nárůst a různorodost firemních dat
- neexistence čistého firemního prostředí, protože například fenomén BYOD

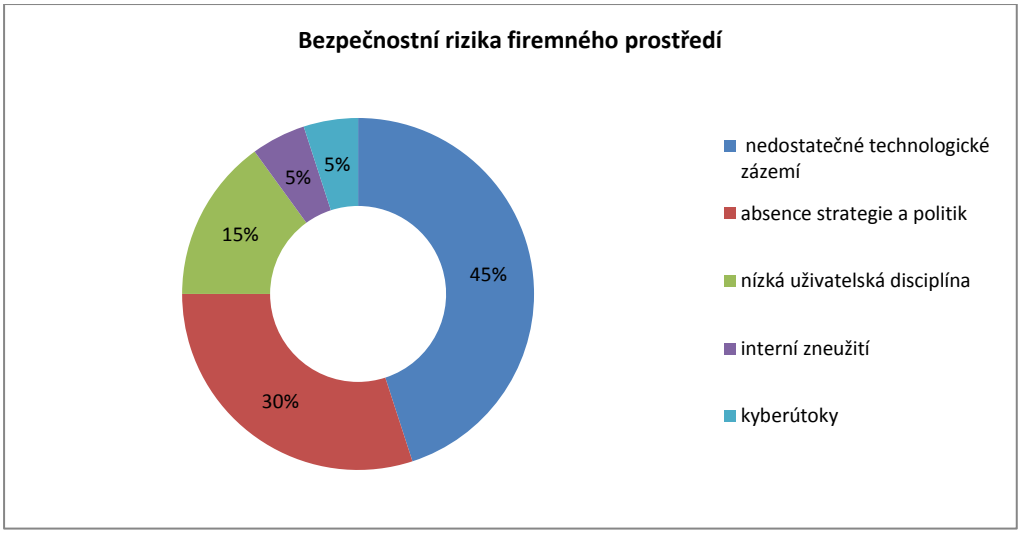
Naopak v neprospěch cloudu jsou u bezpečnosti nejčastěji zmiňovány tyto důvody

- umístění strategických dat (rodinného stříbra) mimo organizaci
- závislost na poskytovateli, případně dalších třetích stranách
- obava ze zneužití dat, tzv. syndrom NSA
- zranitelnost internetu

Nejkritičtější bezpečnostní rizika v podnikovém prostředí lze shledávat:

- nedostatečná úroveň technologických prostředků
- neuspokojivé zvládnutí (reálných, ne papírových) bezpečnostních postupů
- umístění a správa technologického prostředí
- porušení bezpečnostní politiky ze strany zaměstnanců
- interní zneužití, například ze strany zaměstnance
- externí kyberútoky a hacking

Yeseter – Vyskočilova 1326/5a, 140 00 Praha 4, Česká republika, Tel.: +420 283 061 281, E-mail: info@yeseter.com,
URL: http://www.yeseter.com



Podle ČSÚ měla v ČR formálně definovanou bezpečnostní politiku informačních systémů v lednu 2015 **třetina podniků** s deseti a více zaměstnanci. Vlastní bezpečnostní politiku mají stanovenou mnohem častěji větší firmy (50 a více zaměstnanců) – přes polovina z nich (56 %) a velké podniky s 250 a více zaměstnanci (tři čtvrtiny z nich) než malé podniky (26 %).

Monitoring veřejného diskursu na webu a sociálních sítích však vypovídá spíš o něčem jiném, a to, že mezi oficiálními odpověďmi dotázaných podniků a tím, co si myslí zaměstnanci, tu panují poměrně dost velké rozdíly. Ty ukazují dva poslední sloupce tabulky.

Počet zaměstnanců	Stanovení bezpečnostní politiky (ČSÚ)	Míra důvěry zaměstnanců v bezpečnost firemního IT (sociální sítě)	Rozdíl
10 až 49 zaměstnanců	26 %	5 %	21 %
50 až 249 zaměstnanců	56 %	25 %	31 %
250 a více zaměstnanců	75 %	40 %	35 %

Samozřejmě, že porovnávané údaje nejsou komplementární, a tudíž z nich nelze činit jednoznačné závěry. Jde tu spíš o ilustraci faktu, že vykazování bezpečnosti na úrovni zodpovědných útvarů a jejich pracovníků nemusí být vždy v souladu se skutečností či jenom s míněním ostatních pracovníků organizace.

Další tabulka ukazuje výsledky ČSÚ pro adaptaci bezpečnostní politiky v rámci jednotlivých odvětví.

Vyspělost bezpečnostní politiky dle odvětví (ČSÚ)	
Nejvyspělejší	**Zaostávající**
peněžnictví a pojišťovnictví	stravování a pohostinství
telekomunikační činnosti	maloobchodu (kromě motorových vozidel)
ubytování	

V tomto případě monitoring webu a sociálních sítí vykazuje podobné výsledky.

Vyspělost bezpečnostní politiky dle odvětví (sociální sítě)	
Nejvyspělejší	**Zaostávající**
peněžnictví a pojišťovnictví	průmyslové podniky
telekomunikace	ubytování, stravování a pohostinství

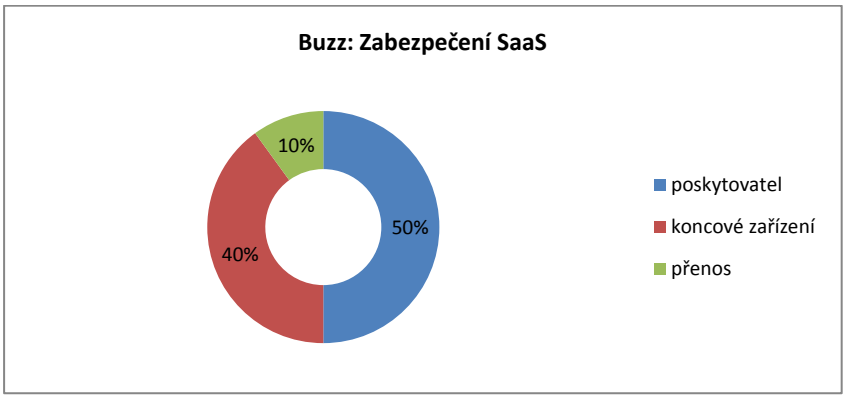
Yeseter – Vyskočilova 1326/5a, 140 00 Praha 4, Česká republika, Tel.: +420 283 061 281, E-mail: info@yeseter.com, URL: http://www.yeseter.com

retail	státní sektor

Zabezpečení dat při využití služeb typu SaaS s sebou nese nemalé nároky:

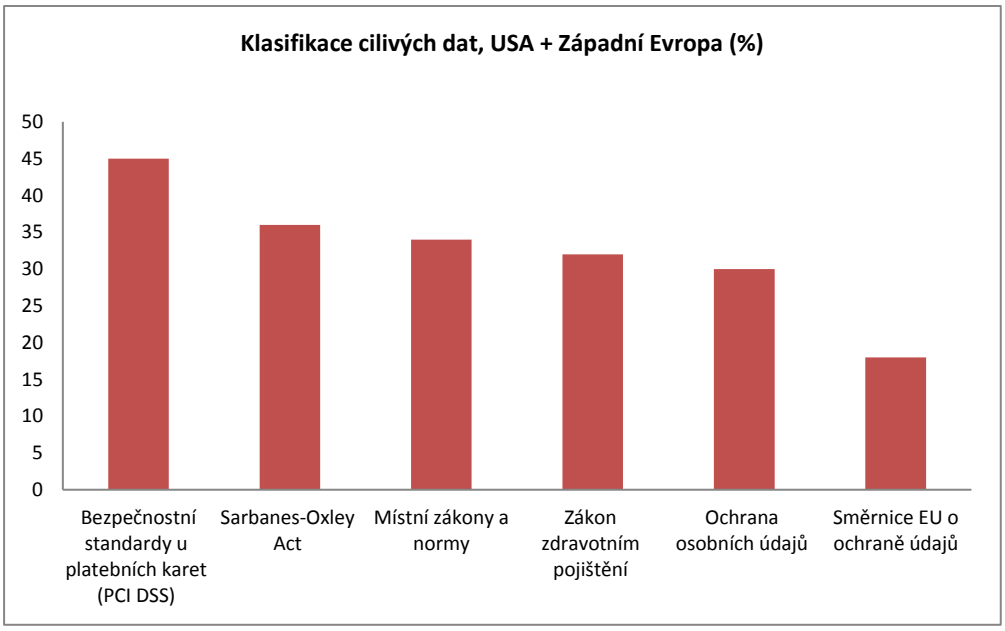
- u poskytovatele služby
- při přenosu dat
- při ochraně koncových zařízení

Tyto nároky není dobré podceňovat. I proto, že popularita cloudových služeb stále roste a trhu veřejného cloudu služby typu SaaS dominují. Podle IDC jim z hlediska výdajů patří sedmdesátiprocentní podíl na trhu – a má tomu tak být i nadále.



Citlivá data jsou v USA a západní Evropě reprezentována zejména:

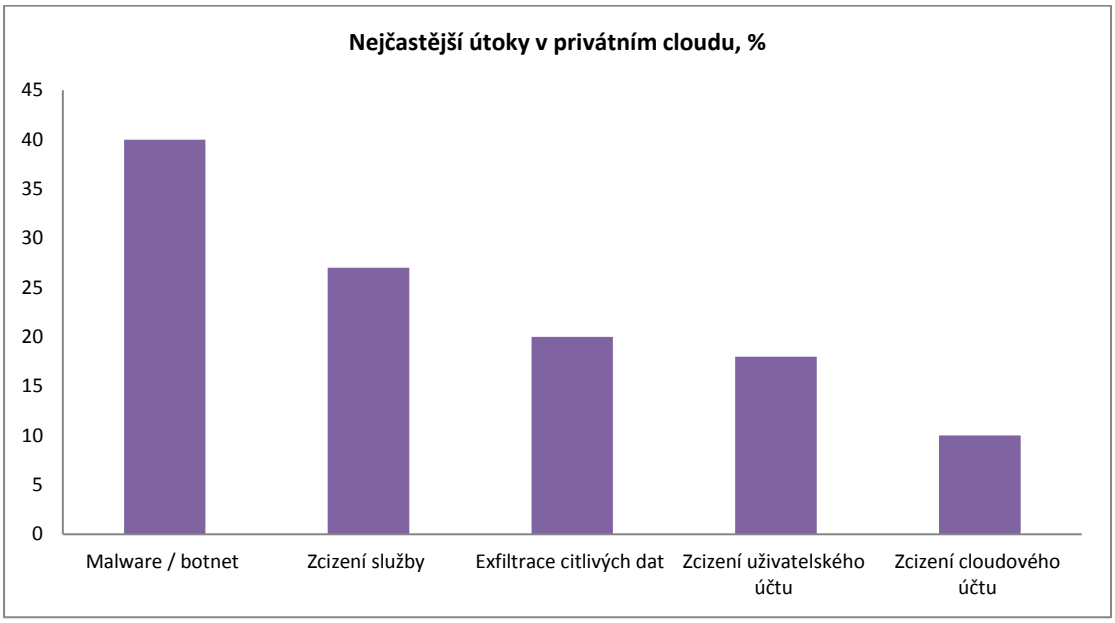
- Standardy bezpečnosti dat v odvětví platebních karet (PCI DSS)
- Zákon Sarbanes-Oxley (SOX)
- Místní jurisdikční zákony a normy
- Zákon o zdravotním pojištění
- Ochrana osobních údajů a rodinné vzdělávací právo (FERPA, PIPEDA)
- Směrnice EU o ochraně údajů



Yeseter – Vyskočilova 1326/5a, 140 00 Praha 4, Česká republika, Tel.: +420 283 061 281, E-mail: info@yeseter.com, URL: http://www.yeseter.com

Nejčastěji zmiňované případy narušení v privátním cloudovém prostředí:

- Malware / botnet infekce
- Zcizení služby
- Exfiltrace citlivých dat
- Zcizení uživatelského účtu
- Zcizení cloudového účtu



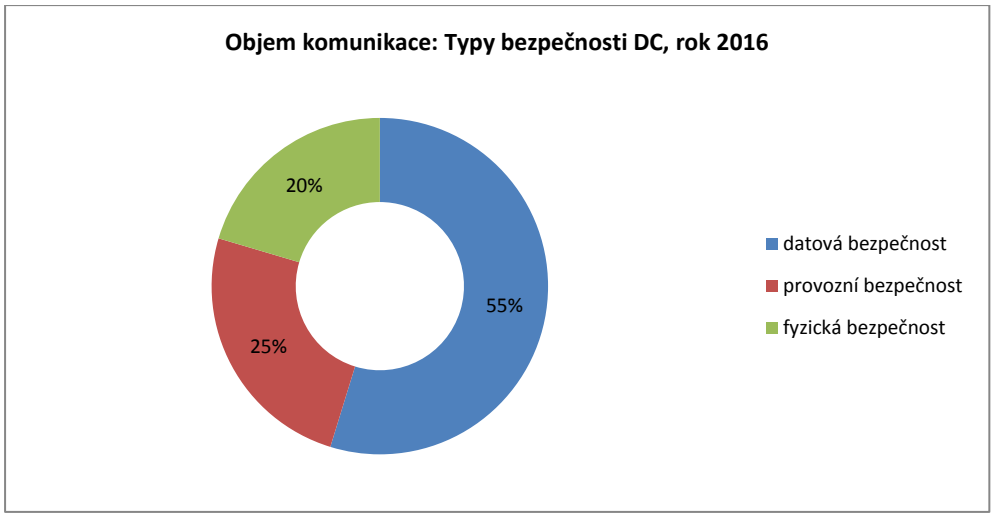
Yeseter – Vyskočilova 1326/5a, 140 00 Praha 4, Česká republika, Tel.: +420 283 061 281, E-mail: info@yeseter.com,
URL: http://www.yeseter.com

5. Bezpečnost datového centra

Praktické příklady ze světa (USA, západní Evropa), ale i z ČR, zachycené ve veřejném diskurzu na internetu a sociálních sítích ukazují, že u provozovatelů datových center lze poměrně snadno narazit na výrazné rozdíly mezi garantovanou a fakticky poskytovanou provozní dostupností. Tady prý poskytovatelé často sází na kartu, že k vzniku krizových situací, resp. havárií, jednoduše nedojde.

Pokud hovoříme o bezpečnosti datových center komplexně, máme na mysli:

- fyzickou bezpečnost
- provozní bezpečnost
- datovou bezpečnost



Fyzická bezpečnost

Preventivní ochrana dat a technologií před poškozením, respektive krádeží. Spadá sem celá řada technik technologického a personálního zabezpečení objektu. Fyzická bezpečnost DC je nejlépe postihnuta ve standardu TIA 942, ze kterého vychází evropská norma EN 50 600.

Faktory mající vliv na fyzickou bezpečnost DC:

- technologické zabezpečení DC
- personální zabezpečení objektu
- metody ověřování totožnosti
- sledování pohybu v rámci DC
- nonstop kontrola DC, dispečink
- přítomnost pracovníků ostrahy
- autorizace přístupů

Provozní bezpečnost

Zásadní činitel datového centra, jenž je ovlivněn mnoho stavebními, konstrukčními a technologickými parametry. To vše ve správě monitorovacího a řídicího systému (DCIM) pro automatizované řešení incidentů. Velkou roli tu ovšem stále hraje lidský faktor, proto jsou pravidelná testování, certifikace, a vzdělávání obsluhy DC nutnou podmínkou. Specifikace provozní dostupnosti a bezpečnosti a nejlépe postihuje Uptime Institute se svojí čtyřvrstvou klasifikací Tier úrovní.

Yeseter – Vyskočilova 1326/5a, 140 00 Praha 4, Česká republika, Tel.: +420 283 061 281, E-mail: info@yeseter.com,
URL: http://www.yeseter.com

Faktory mající vliv na provozní bezpečnost:

- lokalita DC
- konstrukce budovy
- počty přívodů elektřiny
- záložní UPS a baterie
- motorgenerátory
- automatické protipožární systémy
- řešení napájení uvnitř DC
- rozložení napájení pro servery
- chlazení (kapacita, redundance)
- nástroje DCIM
- certifikace a školení obsluhy DC

Datová bezpečnost

Tu lze zajistit kombinací hardwarových zařízení a softwarových nástrojů. Bezpečnost dat zvyšuje přímý vysokorychlostní přístup z podnikové sítě do datového centra či alespoň využití pokročilých VPN pro přístup přes internet. Zde hraje úlohu dostupná konektivita DC i připojené firmy do internetu. Využití datového připojení od více poskytovatelů též zvyšuje datovou bezpečnost. Datovou bezpečnost rovněž zdárně definuje standard TIA 942 a norma EN 50 600.

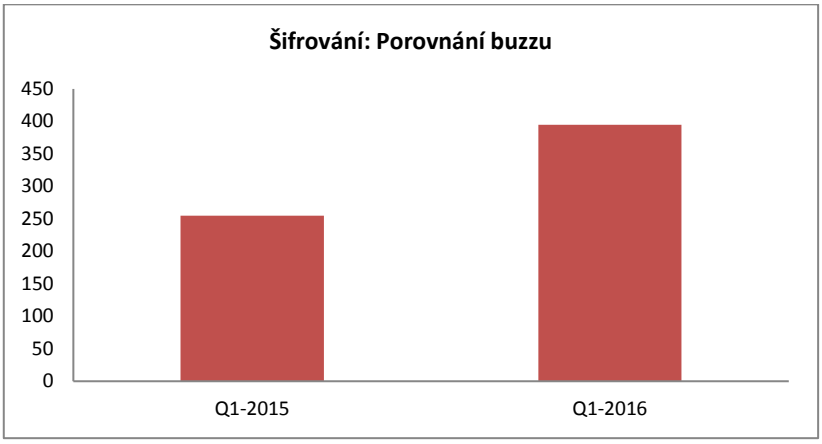
Faktory mající vliv na datovou bezpečnost:

- neoprávněné přístupy, resp. napadení dat zvnějšku
- útok zevnitř datového centra
- přímý vysokorychlostní přístup z podnikové sítě do datového centra
- využití pokročilých VPN pro internetový přístup
- dostupná internetová konektivita DC a podniku
- datové připojení od více poskytovatelů
- šifrování dat

Yeseter – Vyskočilova 1326/5a, 140 00 Praha 4, Česká republika, Tel.: +420 283 061 281, E-mail: info@yeseter.com,
URL: http://www.yeseter.com

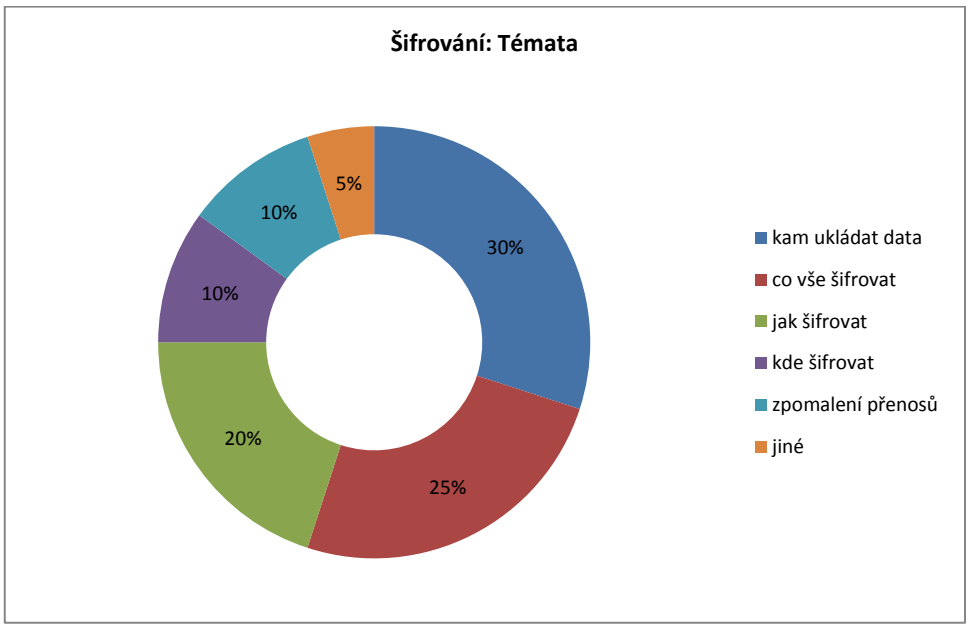
6. Šifrování: Bezpečnost nebo paranoia?

Titulek kapitoly je převzatý z názvu debaty na diskuzním fóru. Poslední zpráva společností Thales e-Security a Ponemon Institute ukázala, že se používání šifrování dat za posledních deset let ztrojnásobilo, nicméně údajně stále ještě existuje celá řada společností, které zabezpečení šifrováním podceňují – a to hlavně co se týče cloudu. Na českém internetu vzrostl objem komunikace na téma šifrování oproti loňskému roku (Q1-2016 vs. Q1-2015) o 55 procent.



Průzkum tuzemského online diskursu ukazuje, že strategii šifrování má zvládnutou pouze nepatrný zlomek firem. Nejčastěji se v tomto směru tuzemské organizace potýkají s výzvou, kam vůbec by měly svá data ukládat – v rámci organizace nebo v externím úložišti?

Klasifikací firemních dat, jejich valuací s přiřazením důležitosti se podle informací na webu prakticky zabývá nemnoho velkých lokálních firem. Častá jsou témata ohledně šifrovacího software, protokolů a algoritmů – většinou u malých a středních firem (SMB). Podobnou důležitost má i problematika, zda šifrovat na straně podniku a zašifrovaná data posílat do cloudu, nebo se samotným šifrováním zabývat až na úrovni cloudu. Diskutuje se i zpomalení přenosů v důsledku šifrování. To je prý nepřímo úměrné počtu přenášených souborů.



Bezpečnost dat pomocí šifrování v oblasti B2B cloud computingu by měla být zajištěna na těchto čtyřech úrovních:

- Ochrana osobních údajů na podnikové úrovni
- Šifrování před vlastním datovým přenosem z podniku do DC
- Trvalé šifrování v průběhu přenosu, uložení a vlastního použití
- Poskytovatel cloudu by neměl mít přístup k bezpečnostním klíčům

Poslední pravidlo je relevantní zejména pro oblast SMB, přičemž záleží na jejich využívání cloud computingu. V rámci jednoduchého sdílení souborů si lze vystačit s běžně dostupnými doplňky (add-ons) k Dropboxu a jemu podobným řešením. Při serióznějším vyžívání cloudu je ovšem potřebné zabývat se touto problematikou komplexněji, včetně zajištění – jak dešifrovacích klíčů, tak i zpracovávaných dat. Ty se ukládají do definovaných krátkodobých pamětí, bez možnosti vytváření kopií, ale s volbou kdykoli proveditelného auditu.

Komplexní ochranu dat zajišťuje kombinace šifrování s tokenizací s pokročilou správou tokenů a klíčů. Protože k většině online útoků na data dochází na serverech či v aplikacích, je potlačení tohoto rizika pro celkovou ochranu dat velmi důležité. Aplikační zabezpečení dat poskytuje vysoký stupeň ochrany, data jsou chráněna již v bodu svého vzniku a poté zůstávají nadále chráněna i v průběhu celého životního cyklu. Aplikační šifrování a tokenizace jsou pro tento typ zabezpečení dat velmi účinné.

Ukázka ze sociálních sítí

Ani šifrované data nejsou v cloudu v bezpečí. Poskytovatelé úložišť mají k dispozici takový distribuovaný výpočetní výkon, že můžou zkoušet brute-force na kterémkoliv uživateli se jim zamane. Nepomůže ani pravidelná změna šifrovacích klíčů, protože poskytovatel služby si beztak původní data ponechává a jen uživatel je vidí jako smazané, resp. nevidí je. Nebo si snad myslíte, že pokud smažete email s šifrovanou přílohou na Gmailu, že se ten email smaže fyzicky také z disků Googlích datacenter?

Když vezmeme v úvahu, že budeme mít heslo o 20 znacích a použijeme a-z, A-Z, 0-9 a speciální znaky, tj. nějakých 100 znaků. Počet výsledných kombinací tedy bude 100^20 (1,2 × 10^130). Bruto force útokem je prolomení hesla i se všemi PC absolutně nemožné. Trval by 1,1 × 10^23 let, takže prakticky nereálné. Další možnost jsou Rainbow tabulky, ty by se však museli vygenerovat, tady by však byl problém s místem (zhruba 8 × 10^15 GB). Takže šifrované data s použitím dlouhého hesla jsou absolutně v bezpečí.

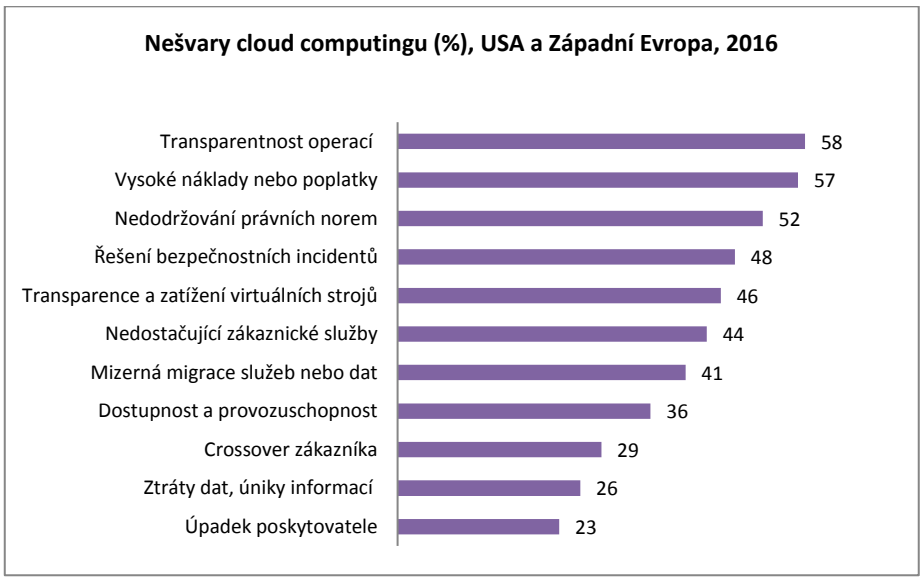
Předpokládejme, že top 500 super počítačů má výkon asi 60 PFLOPS, řekněme, že celkový výkon všech zařízení bude nějakých 200 PTFLOPS. Ati HD 5970 má výkon 4,64TFLOPS a zvládne 65 000 hesel za sekundu. Výpočtem tedy dostaneme, že všechny zařízení by zvládly 2,8 bilionu hesel za sekundu. Výsledný čas na luštění hesla o délce 20 znaků by byl asi 10^113 let.

7. Strašáci cloud computingu

Tato kapitola se věnuje nejčastějším posteskům uživatelů firemního cloudu v USA a západní Evropě. Bezpečnost tu hraje jednu z dominantních rolí. Prostředí tuzemského internetu tyto výsledky částečně potvrzuje, nicméně počet příspěvků pro samostatný precizní tuzemský výstup v tomto směru zde není dostatečný. Zastoupení internetových příspěvku z USA a Evropy je v poměru 65:35.

Největší frustrace z firemního cloudu způsobují tyto faktory:

- Nedostatečná transparence poskytovatele a prováděných operací
- Vysoké náklady nebo poplatky
- Nedostatečné dodržování právních norem, resp. transparentnost
- Slabé nebo žádné řešení bezpečnostních incidentů (transparence, protokoly)
- Neuspokojivý reporting běhu serverů a jejich zatížení
- Úzká nabídka zákaznických služeb
- Mizerná migrace služeb nebo dat
- Dostupnost a doba provozuschopnosti
- Crossover nájemce (přechody mezi virtuálními systémy)
- Ztráty dat nebo úniky informací způsobené poskytovatelem
- Ztráta aplikací nebo dat v důsledku krachu poskytovatele

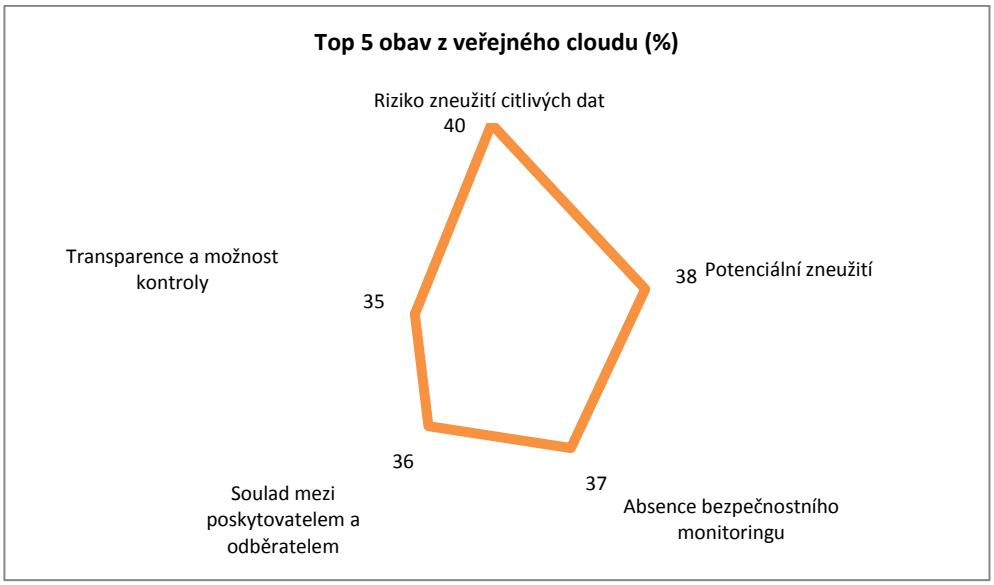


Protože výšeuvedená úzká místa generalizují cloud přes všechny jeho typy, další části kapitoly se zvlášť věnují jednotlivým typům firemního cloudu a největším obavám, které plynou z jejich používání. U každého z nich jsou tyto obavy vizualizovány grafem v procentuálním vyjádření.

Veřejný cloud

Neautorizovaný přístup k citlivým datům je největším strašákem uživatelů veřejného cloudu

- Riziko zneužití citlivých dat
- Potenciální zneužití cloudových zdrojů (stínové IT v cloudu)
- Soustavný bezpečnostní monitoring integrovaný do bezpečnostního dispečinku
- Soulad údržby mezi poskytovatelem a odběratelem služby
- Transparentnost a možnost kontroly u zpracovávaných citlivých dat



Mezi další nedostatky veřejných cloudů uživatelé uvádějí závislost na poskytovatelích, zprostředkovatelské služby, nedostatky v knihovnách třetích stran a obecně absence kontroly – vidět poskytovatelům více pod pokličku při provozování poskytovaných služeb. Nedostatek kontroly se u jednotlivých cloudových platforem částečně liší.

SaaS
Uživatelé mají úplnou kontrolu nad svými daty, ale už ne nad aplikační úrovní a stejně tak ani nad kontrolními mechanizmy v rámci celkového prostředí poskytovatele.

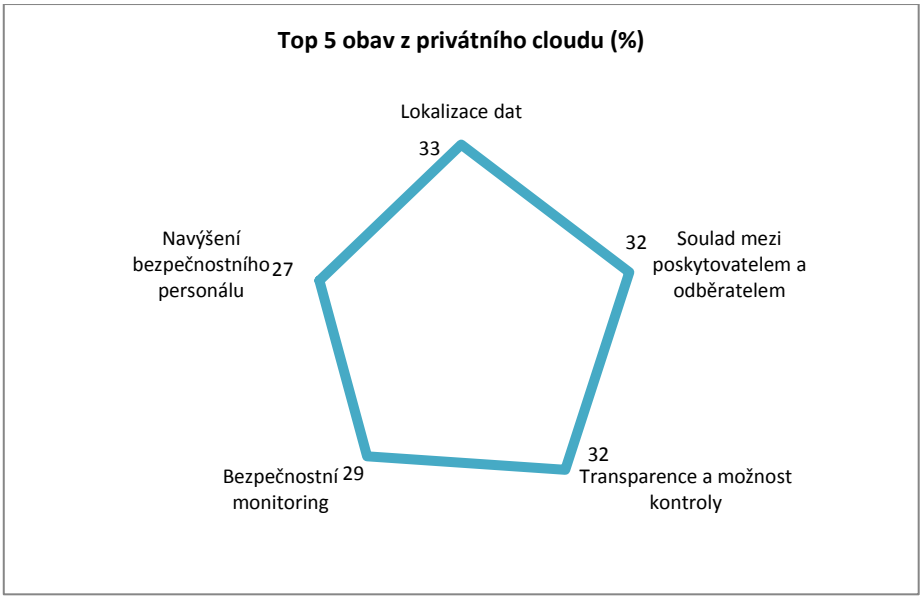
PaaS
Služby této úrovně umožňují uživatelům spravovat aplikace s pomocí několika ovládacích prvků infrastruktury, většina z nich se ovšem vztahuje k ochraně osobních údajů – jako je šifrování a monitoring.

IaaS
Uživatelé mají bezpečnost plně pod kontrolou, a stejně tak i úplný přehled o zabezpečení a správě systémů běžících na platformě IaaS. Mohou vytvářet vlastní síťové kontroly s celou řadou ovládacích prvků a kontrolních mechanizmů.

Privátní cloud

U privátního cloudu největší obavy pramení z geografického umístění uložených a zpracovávaných dat, konkrétněji:

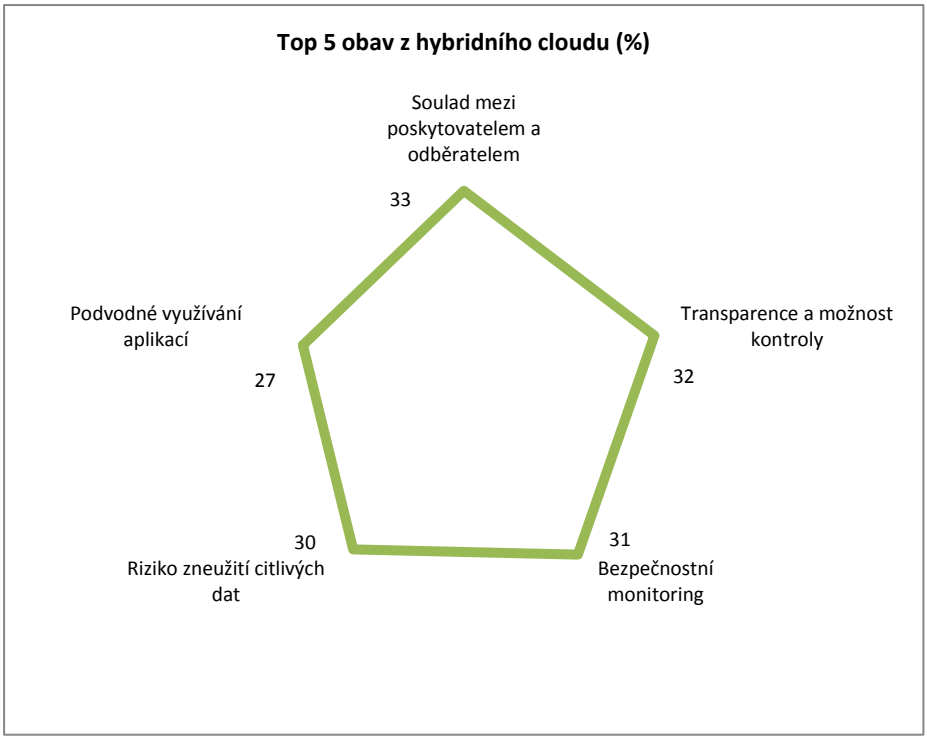
- Geografická lokalizace zpracovávaných dat
- Soulad údržby mezi poskytovatelem a odběratelem služby
- Transparentnost a možnost kontroly u zpracovávaných dat
- Soustavný bezpečnostní monitoring integrovaný do podnikového dispečinku
- Nutnost navýšení bezpečnostního personálu



Hybridní cloud

Uživatelé hybridních cloudů spatřují největší nedostatek v disharmonii spolupráce mezi dodavatelem a odběratelem služby.

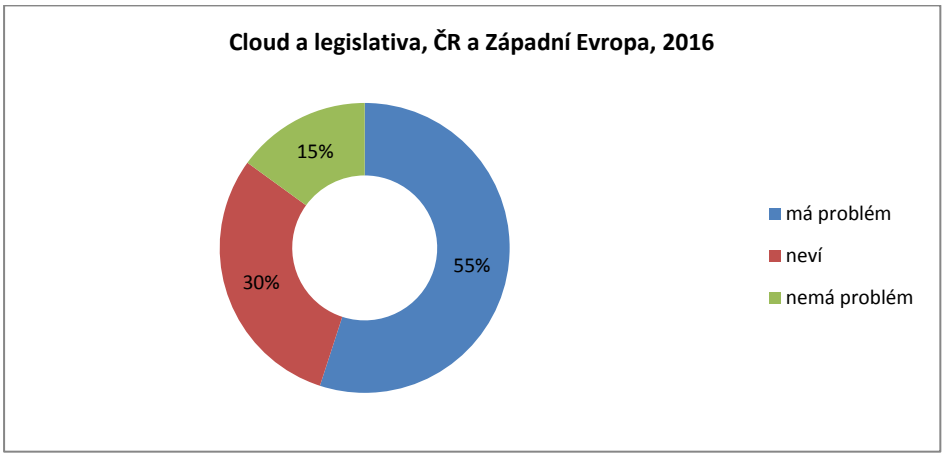
- Soulad údržby mezi poskytovatelem a odběratelem služby
- Transparentnost a možnost kontroly u zpracovávaných citlivých dat
- Soustavný bezpečnostní monitoring integrovaný do podnikového dispečinku
- Riziko zneužití citlivých dat
- Podvodné využívání aplikací cloudu (o kterých IT nemá zdání)

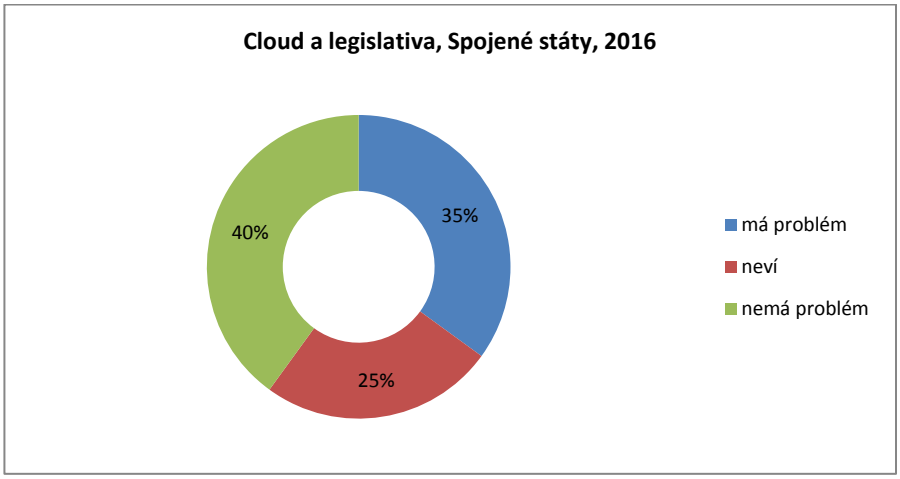


8. Cloud computing a legislativa

Současná legislativa týkající se cloud computingu není jednoznačná a to v celosvětovém kontextu. Neuralgickým bodem je místo uložení a zpracování dat, které se v cloudu může měnit. Stejně tak je zahalena určitou mlhou i prokazatelnost tohoto místa.. Právními aspekty se ovšem zabývají více evropští než američtí uživatelé, viz níže. Po zneplatnění dohody Safe Harbour mezi Evropskou unií a Spojenými státy z loňského roku se více evropských zájemců o cloud zajímá, kde budou jejich data skladována a kde zpracovávána. Podobnou nedůvěru ovšem v menší míře sdílejí i uživatelé v USA směrem k evropským poskytovatelům cloudu.

Následující dva grafy demonstrují míru důvěry uživatelů k legislativě na obou stranách oceánu. Sledované období tu bylo od 1. ledna do 25. července 2016.





Na veřejný diskurs k bezpečnosti cloud computingu mají v současnosti vedle zcela racionálních úvah silný vliv i částečně mimoběžné záležitosti z jiných stran bezpečnostního spektra, jakými jsou například imigrantská krize (Evropa) nebo bezpečnostní incidenty typu WikiLeaks a Panama Papers (Evropa, USA).

Existující rizika cloud computingu lze legislativně omezit dobrou přípravou a nastavením spolupráce s dodavatelem. Z pohledu bezpečnosti dat je například vhodné ověřit si předem, jaká práva k datům odběratele služby má poskytovatel a zda s nimi může nakládat.

Seriózní poskytovatelé cloudových služeb se smluvně zavazují, že k zpracovávaným datům nebude přistupovat žádná třetí strana, ani oni sami, a rovněž s nimi nebudou nakládat pro své vlastní obchodní účely. S tím úzce souvisí i lokalita, kde se datové centrum nachází. Pokud se jedná o lokalitu v rámci Evropské unie, vše se řídí legislativou EU.

Dodavatel by měl též prokázat, že veškeré poskytované služby jsou v souladu s evropskou legislativou. Z praktického hlediska je užitečné přesvědčit se o tom, že cloudové služby dobře navazují na existující firemní IT a vhodně se s ním doplňují – a také že poskytovatel cloudu má dobře zajištěnou lokální servisní podporu. V neposlední řadě je dobré vědět, jak snadno je možné smluvní vztah ukončit a co všechno to obnáší.

Právní rizika cloud computingu

Při výběru poskytovatele cloudových služeb by technickým a organizačním aspektům měla vždy předcházet právní rizika odběru služby. Zpracování dat v cloudu je stále úzkým místem, zejména z důvodu absentující legislativy, nedostatečných informací a limitovaných možností kontroly ze strany uživatele. I když z právního hlediska je poskytovatel povinen náležitě informovat zákazníka.

Kde se při využívání cloud computingu v reálu nacházejí uložená, respektive zpracovávaná data? Kam se předávají? Uživatel cloudových služeb většinou neví, kde se jeho data v cloudu právě nacházejí. Zároveň však z pozice jejich správce je povinen poskytovat jim dostatečnou ochranu. Současný právní rámec v tomto směru zákazníkovi dostatečnou kontrolu nenabízí. Dostatečným řešením tu může být volba poskytovatele cloudových služeb, jenž legislativně garantuje soulad s předpisy EU a navazuje na ně dalšími organizačními a technickými kroky.

Při uzavírání cloud computingových smluv je zhlediska bezpečnosti vhodné zaměřit se na:

- přístup k údajům pouze pro oprávněné osoby
- klauzule o mlčenlivosti poskytovatele a jeho zaměstnanců
- sdělování údajů třetím stranám
- zpracování a poskytování osobních údajů
- podrobná součinnost poskytovatele a zákazníka, například:
  - možnost dohledu nad zpracováním
  - oznamování narušení či poškození uložených údajů
  - upravení přístupu
  - opravy či výmaz uložených dat

- Použití zemského práva ve vztahu ke správci dat (zákazníkovi cloudu, uživateli) je dáno místem jeho sídla nebo provozované činnosti, nikoliv sídlem poskytovatele cloudových služeb

- Poskytovatel je povinen informovat zákazníka o případném předávání jeho dat třetím stranám. Pokud se zpracování dat odehrává pouze na území EU, je možné předávat data bez svolení Úřadu pro ochranu osobních údajů (ÚOOÚ)

- Ukládání dat u poskytovatele má v rámci EU jasná pravidla, upravená evropskou směrnicí č. 95/46/ES. Doplňkově i směrnicí č. 2002/58/ES, jež určuje práva a povinnosti jak poskytovatelů cloudových služeb, tak i jejich uživatelů

- Předávání dat do zemí mimo EU je považováno za rizikové a může se vyznačovat nedostatečnou mírou ochrany. Proto bez předchozího souhlasu ÚOOÚ lze předávat data pouze do zemí, které ratifikovaly Úmluvu o ochraně osob se zřetelem na automatizované zpracování osobních dat a jejich ochrana je v souladu se směrnicí 95/46/ES

- Zákon stanoví důvody, kdy lze data předávat i do zemí, které neratifikovaly Úmluvu o ochraně osob. A to v případech, kdy k předání dochází s výslovným souhlasem správce dat nebo kdy je předání nezbytné pro ochranu jeho práv či životně důležitých zájmů

- Spojené státy se od 6. 10. 2015 řadí k tzv. třetím zemím, tj. zemím s nedostatečnou úrovní ochrany osobních údajů, neboť Soudní dvůr Evropské unie v rozsudku ve věci C-362/14 Maximillian Schrems v. Data Protection Commissioner prohlásil za neplatné rozhodnutí Komise o odpovídající ochraně poskytované v USA, na základě kterého bylo dosud možné předávat osobní údaje do USA společnostem, které se zavázaly dodržovat zásady „bezpečného přístavu“ (Safe Harbor).

- Za zemi s nedostatečnou úrovní ochrany bude USA považováno až do doby, kdy vstoupí v platnost připravované rozhodnutí Evropské komise EU-US Privacy Shield, které nahradí původní rozhodnutí Safe Harbor. Poté bude opět možné předávat osobní údaje do USA společnostem, které se zaváží dodržovat zásady EU-US Privacy Shield.

Uzavírání smluv o užívání cloudových služeb

- Pořízení cloudových a obecně IT služeb poskytovaných po internetu (prodej sw licencí nebo elektronická distribuce audiovizuálních děl) se sice technicky liší od osobního nakupování produktů a služeb, z právního hlediska se ovšem rozdíl stírá

- V některých aspektech může být přístup jednotlivých poskytovatelů zcela rozdílný

- Pro uzavírání smluv po internetu, v rámci subjektů se sídlem na území ČR, jsou závazná především ustanovení nového občanského zákoníku (zákon č. 89/2012 Sb.), který dnem 1. ledna 2014 nahradil obchodní zákoník

- Nový občanský zákoník zrovnoprávnil podpis smlouvy s uzavřením smlouvy distančním způsobem (na dálku), prostřednictvím telefonu, e-mailu, SMS či webové stránky

- Zvláštním ustanovením o závazcích ze smluv uzavíraných distančním způsobem se věnují paragrafy 1824 – 1827. Zákon uvádí, že se za správné a úplné považují i digitální zprávy, například e-mail s potvrzením objednávky

- V případě sporů je to dodavatel, kdo musí dokázat, že přijal objednávku v digitální podobě, a to typicky předložením objednávky (e-mail, záznam telefonického hovoru apod.), u které je schopen prokázat, že nedošlo k úpravě jejího obsahu

Při uzavírání smlouvy na cloudové služby, zpravidla nedochází k jednání se subjektem sídlícím v ČR a často ani v EU. Obvyklé je spíše uzavírání smluv se subjekty sídlícími v USA. To s sebou přináší i přesun jurisdikce na americkou půdu, do státu stanoveného dodavatelem služby ve smlouvě.

- Při převádění smluvního vztahu pod jinou než tuzemskou jurisdikci je třeba počítat s jinou legislativní ochranou (zpravidla slabší), než jakou poskytuje nový občanský zákoník. Řešení případného sporu podle zahraničního práva nebude snadné ani levné

- Není s uzavřením smlouvy spojený například i aktivační poplatek, roční servisní poplatek či nějaká další platba nad rámec měsíčního předplatného?

- Označením souhlasu a kliknutím na příslušné tlačítko v objednávacím formuláři na webu dochází k závaznému odsouhlasení se všemi podmínkami smlouvy

Ukázka ze sociálních sítí

Zde platí pouze jedno pravidlo které se da použít i pro některé ostatní služby, a to že když je komunikace šifrována a provozovatel cloudu šifruje obsah do takové míry ze ho sám nevidí a nemůže ho jakkoliv analyzovat je vám úplně jedno kde jsou servery cloudu umístěny.

Provozovatel cloudu nemůže šifrovat obsah do takové míry, že ho sám nevidí. To může udělat jedině uživatel.

Libovolná společnost, která chce mít data o klientech někde v oblacích (živé nebo zálohy) dle zákona, by měla dbát o to, kde ta data fyzicky jsou. Tady přece vůbec nejde o technické řešení ale právní.

Největší problém cloudových řešení není jejich umístění, ale to, že se majitel serveru může hrabat ve vašich datech. Celý právní rozbor a usnesení ÚOOU jsou zbytečnosti. Internet je jiný, internet je globální. Dělat region-lock řešení je zpátečnictví.

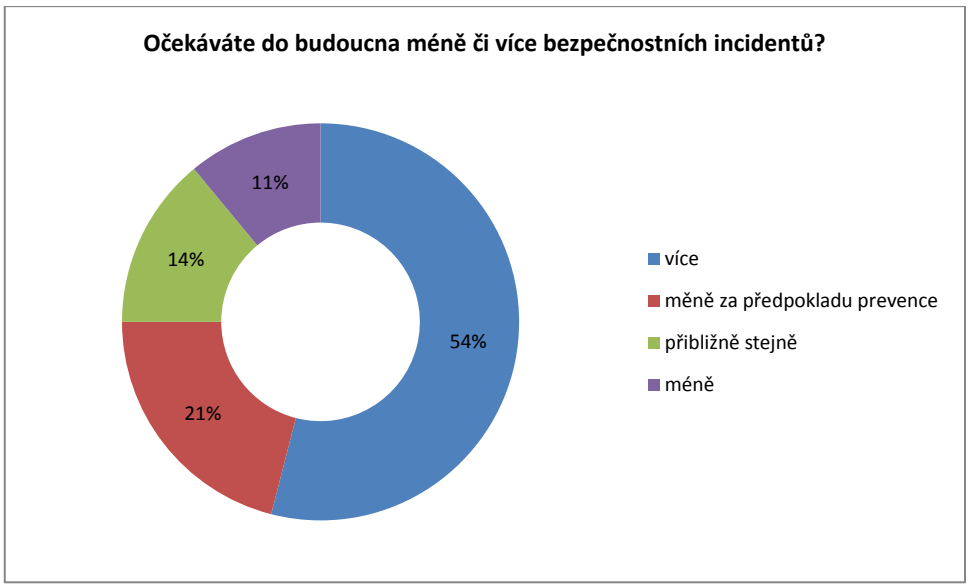
ÚOOU by se měl zaměřit hlavně na vlastní zabezpečení dat. Tzn. šifrovat je pořádně klientem a pak ať už si jdou klidně do tramtárie. Ale to by tam nesměli být hňupi, co si ani nedovedou vygenerovat klíč a používají heslo 12345.

To je hezké, ale řešíš jenom zlomek cloudových řešeni, kdy je cloud jenom víceméně tupé úložiště dat. Homomorfické šifrování by řešilo další sadu problémů, ale (zatím?) nemáme nic použitelného.

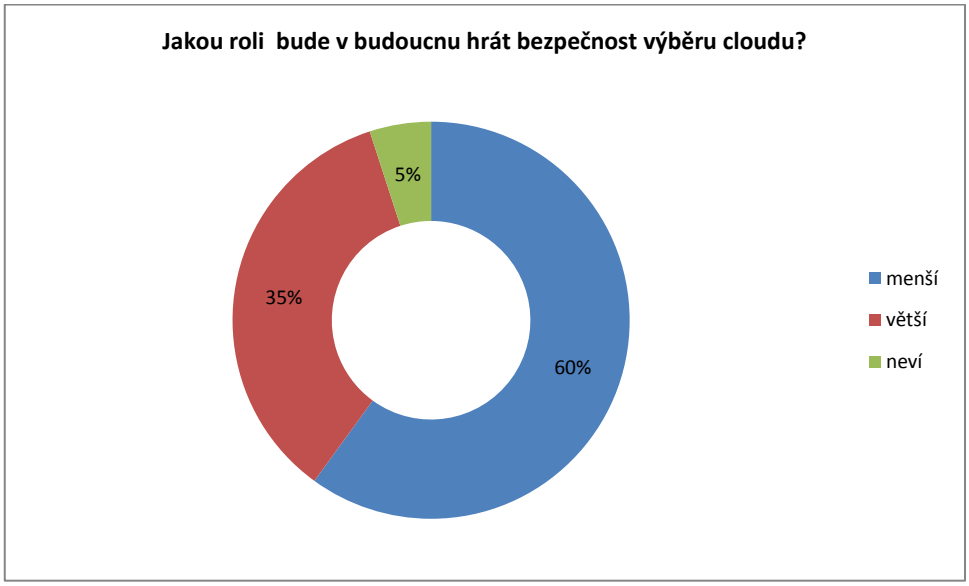
9. Vzpomínky na budoucnost

Několik stovek zmínek ze světového internetu se v rámci tématu zabývalo i budoucností bezpečnosti cloud computingu. Proto jsme sem zařadili i dvě ad-hoc předpovědi ohledně dalšího vývoje.

Lze v blízké budoucnosti očekávat více nebo naopak méně bezpečnostních incidentů na podnikové úrovni?



Bezpečnost podnikových dat a aplikací bude do budoucna hrát čím dál větší nebo naopak menší roli při volbě cloudových řešení? Odpověď „menší“ je potřebné chápat ve smyslu, že tato otázka již bude brzy vyřešena, tudíž se s ní nebudeme tak intenzivně zabývat jako dnes.



10. Úvod do problematiky hardwarové bezpečnosti

Pod zkratkou HSM (hardware security module) v tomto dokumentu rozumíme hardwarové bezpečnostní zařízení, respektive modul, někdy též označovaná jako kryptografický modul či kryptografický koprocesor, sloužící k bezpečnému provádění kryptografických operací v nedůvěryhodném prostředí.

Distribuované systémy vyžadují pro bezpečnou komunikaci použití vhodných mechanizmů pro zajištění integrity kryptografických funkcí a důvěryhodnosti šifrovacích klíčů. U běžně nasazovaných systémů to bez HSM lze zajistit jen stěží, jejich hardware bývá prakticky nezabezpečený a software vykazuje větší míru chybovosti.

Zařízení HSM se objevila prvně ve finančním sektoru za účelem zabezpečení narůstajícího počtu elektronických transakcí probíhajících v mezibankovních sítích, sítích bankomatů a rovněž karetních společností: VISA, MasterCard, American Express a dalších.

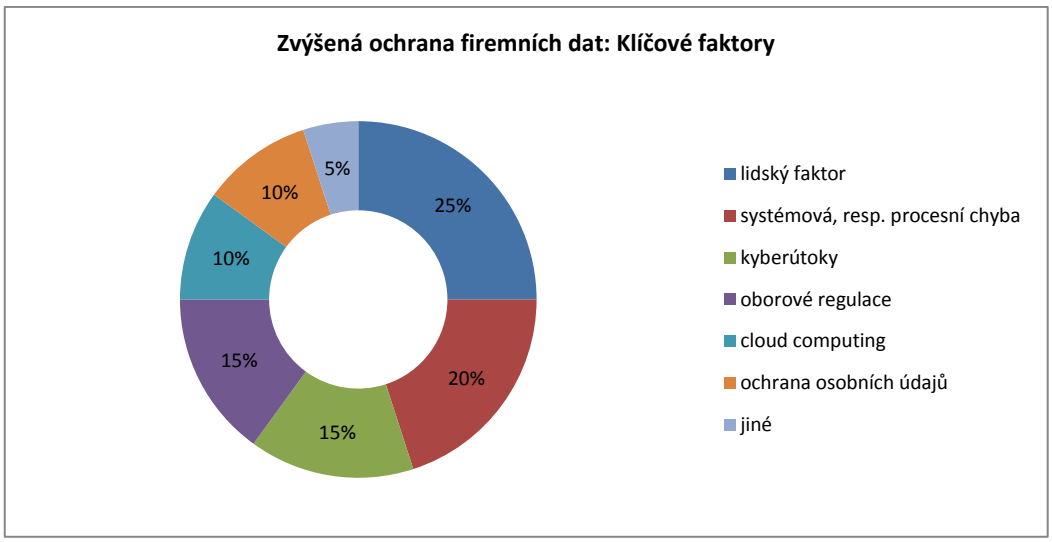
Kromě zabezpečení důvěryhodnosti datových přenosů, zajišťuje HSM i garantovanou správu kryptografických klíčů a dalších citlivých dat, například PIN kódů u čipových karet. Zatímco čipové karty jsou používány běžnými uživateli, moduly HSM bývají vesměs ve správě datových center a jejich služeb využívají serverové aplikace.

Veřejný diskurz týkající se problematiky hardwarových bezpečnostních zařízení HSM na severoamerickém internetu a sociálních sítích se dotýká více oblastí, například: certifikační autorita, bankomaty, platební terminály POS, čipové karty (platební karty, SIM, přístupové karty), digitální podpis, platební standardy v e-commerce a m-commerce. Předkládaný dokument na zařízení HSM nazírá pouze z pohledu zabezpečení dat v podnikovém prostředí a cloud computingu.

11. Ochrana dat v podnikovém prostředí

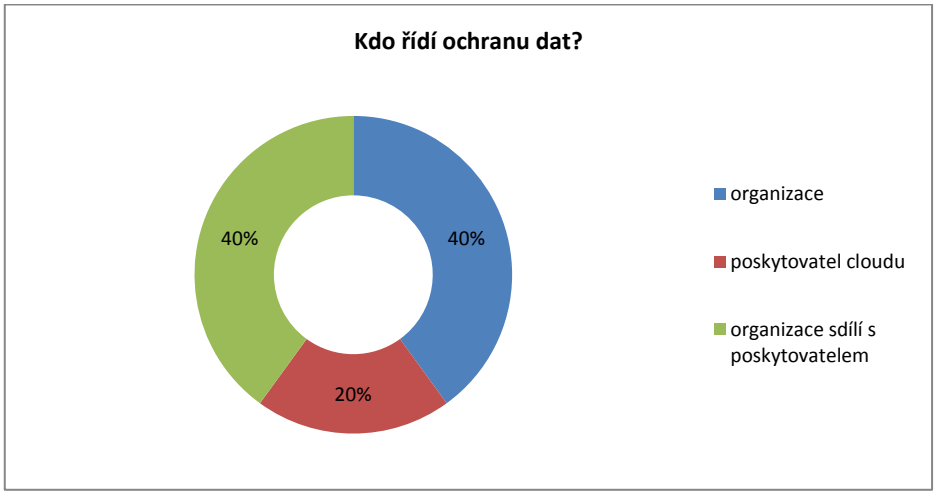
Hlavní důvody zvýšené ochrany dat v podnikovém prostředí

V podnikovém IT prostředí ve Spojených státech lze dle mnoha zdrojů registrovat zvýšení zájmu o šifrování podnikových informačních zdrojů. Klíčovými faktory tohoto jevu jsou především obavy ze selhání vlastních zaměstnanců, procesní, resp. systémové chyby, narůstající hrozby kyberútoků, přísnější odvětvové regulace a předpisy pro ochranu osobních údajů a stále rostoucí segment cloud computingu. Dále tu též hrají svou roli média a zveřejňování sugestivních příběhů souvisejících s (ne)kódováním informací a (ne)přístupy k firemním datům přes šifrovací klíče.



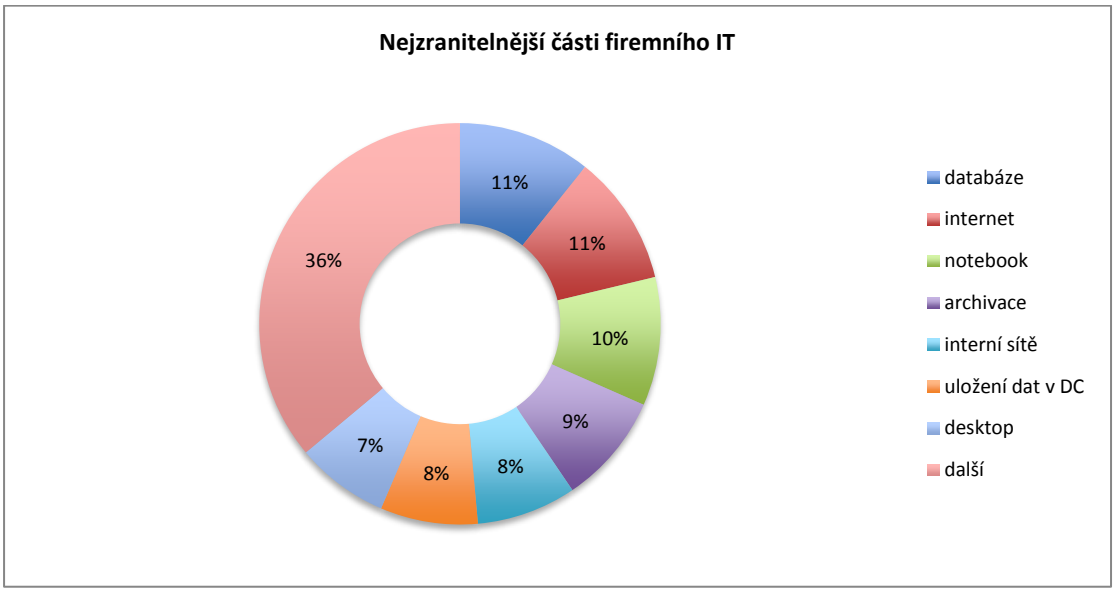
Zodpovědnost za ochranu dat v cloud computingu

Na kom leží zodpovědnost za bezpečnost firemních dat v cloud computingu? Dvě pětiny podniků deklarují správu ochrany informací ve vlastní režii. Stejný počet firem hovoří o sdílené správě ochrany dat, jež je záležitostí samotné organizace, tak i poskytovatele cloudu. Pouze pětina firem nechává ochranu firemních dat pouze na poskytovatelích cloudových služeb. Z odvětvového pohledu jsou nepřísnějšími strážci firemních dat pod vlastní správou společnosti z finančního sektoru, na opačném konci spektra naopak stojí oblast cestovního ruchu a volnočasových aktivit, jež preferuje ochranu dat v rukách poskytovatelů cloudu.



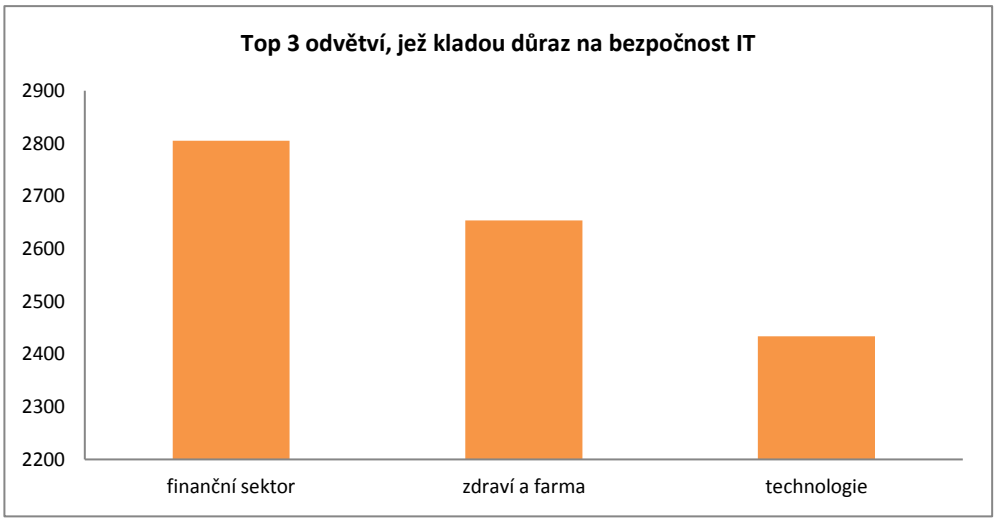
Komponenty podnikového IT nejvíce podléhající ochraně dat

Mezi nejčastěji zmiňované komponenty podnikového IT podléhající bezpečnostním rizikům patří firemní databáze, internetové připojení, pracovní notebooky, archivace a zálohování souborů a dokumentů, firemní sítě, skladování dat v datovém centru a stolní počítače. U firemních stolních počítačů a notebooků jsou pak zmiňovány především jejich diskové jednotky. Mezi další zranitelné komponenty IT podnikového prostředí patří firemní aplikace, zálohování dat v cloudu, e-maily, big data, služby veřejného cloudu a infrastruktura cloudu privátního.

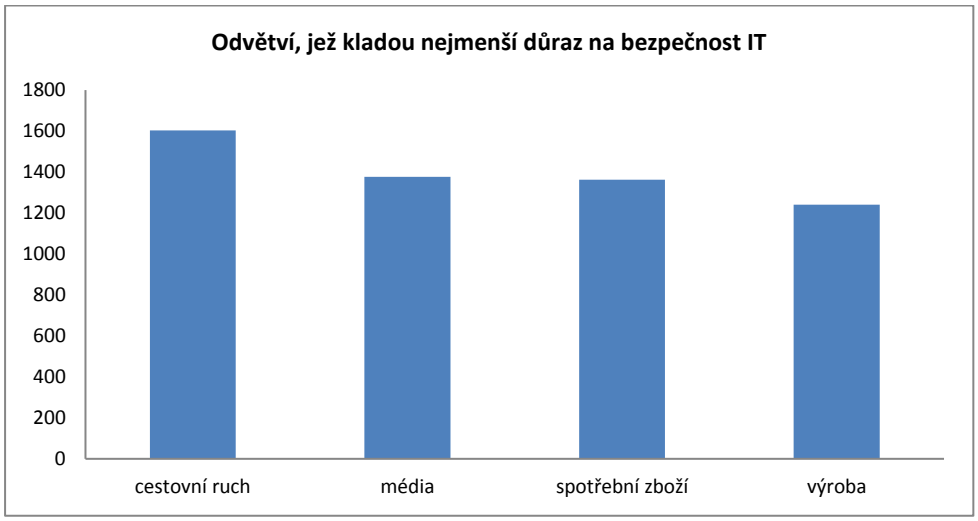


Ekonomická odvětví a bezpečnost podnikového IT

Mezi odvětví, která přičítají bezpečnosti podnikového IT a ochraně údajů velký význam náleží finanční sektor, farmacie a zdravotnictví a technologické společnosti. Do jisté míry je to dané velkou mírou regulací, které v těchto segmentech trhu panují.

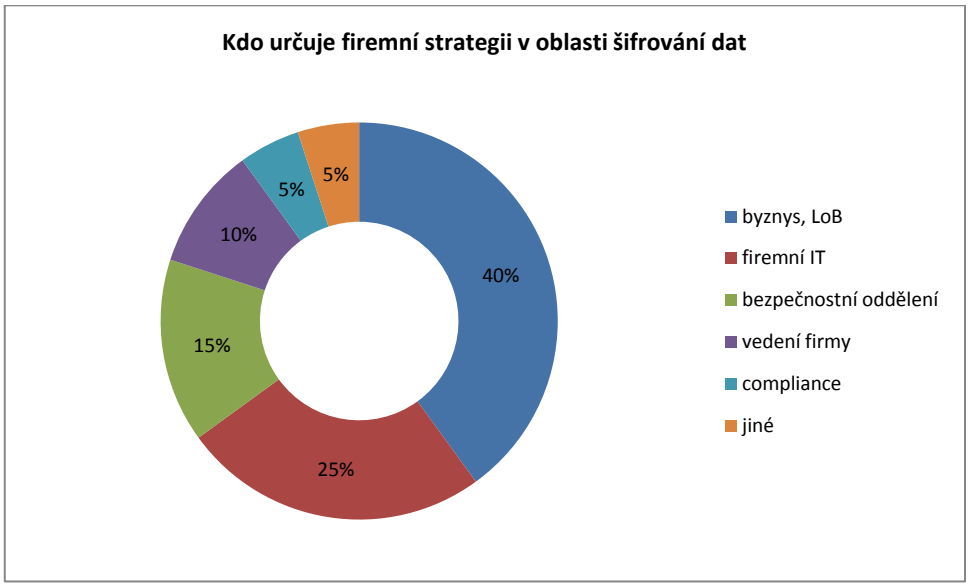


Naopak mezi odvětví s nejmenším zájmem o bezpečnost firemního IT patří oblasti cestovního ruchu, médií, spotřebního zboží a výroby.



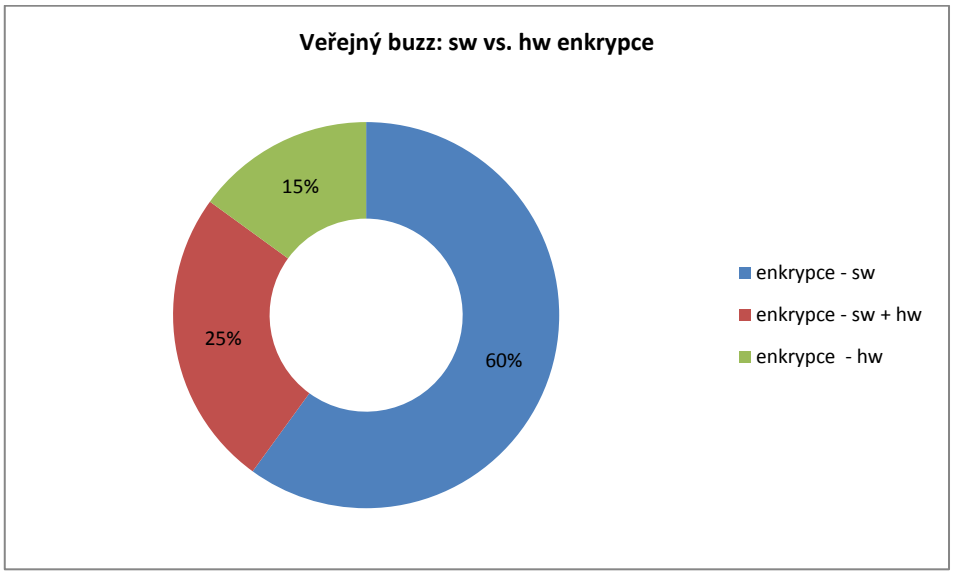
Kdo v rámci firmy zodpovídá za strategii v oblasti šifrování dat

Největší podíl na formování strategie pro bezpečné šifrování dat a přenosů mají v amerických firmách odborná oddělení (LoB, line of business). Druhým nejvýznamnějším podnikovým subjektem majícím vliv na tuto oblast jsou oddělení IT a až na třetím místě to jsou firemní bezpečnostní oddělení. U menších firem též rozhoduje nejvyšší vedení. Nejmenší podíl na tomto rozhodování byl přiřknut oddělením Compliance, úlohou kterých je dbát na dodržování odvětvových či mezinárodních standardů a postupů, včetně shody podnikových procesů s platnou legislativou a s regulačními opatřeními. Jak již bylo výše naznačeno, zapojení jednotlivých oddělení závisí často na velikosti podniku.



12. Srovnání hardwarové a softwarové enkrypce

Zamezení neautorizovaným přístupům v podnikovém prostředí založené na použití programových nebo hardwarových zařízení je jednou ze základních otázek při rozhodování o bezpečnosti. Enkrypce pomocí programového vybavení je více běžná než enkrypce pomocí hardware. Veřejný diskurz za sledované období to rovněž potvrzuje.



Šifrování pomocí software

Mezi výhody šifrování pomocí software patří: zajištění ochrany všech zařízení v organizaci, jejich snadná ovladatelnost, nižší pořizovací a provozní ceny, jednoduchá implementace vylepšených verzí, podpora veškerých operačních systémů, ochrana dat na různých zařízeních. Mohou obsahovat další doplňkové bezpečnostní vlastnosti.

Bezpečnost softwarových šifrovacích řešení a postupů je ovšem limitována bezpečností operačních systému zařízení, na nichž je implementována. Bezpečnostní chyba v operačním systému může taktéž ohrozit zabezpečení jištěné šifrovacím kódem. Konfigurace šifrovacího software může být složitá pro pokročilé nasazení a rovněž tu hrozí zásahy ze strany uživatelů, například jeho vypnutí. Tento typ enkrypce bývá rovněž provázen poměrně velkým snížením výkonu zasažených systému.

Softwarová enkrypce	
Silné stránky	**Slabé stránky**
zajištění ochrany všech zařízení v organizaci snadná ovladatelnost nákladová efektivnost jednoduchý update a upgrade podpora všech operačních systémů ochrana dat ve všech režimech (uložení, provoz, zálohování) na různých zařízeních obsahuje další doplňkové bezpečnostní vlastnosti	limitace bezpečností operačních systémů složitá konfigurace pro pokročilé nasazení hrozba uživatelských zásahů snížení výkonu systémů

Šifrování pomocí hardware

Enkrypce na bázi hardware využívá pro šifrování a dešifrování speciálně navržené autonomní bezpečnostní moduly, tzv. hardware security modules (HSMs), jenž nevyžadují další podporu dalšího hardware. Proto jsou imunní vůči kontaminaci či infekcím ze strany škodlivých kódů, nebo jiné zranitelnosti. Pokročilá šifrovací zařízení na bázi hardware instalované v hostitelském počítači, nevyžadují načtení dalších ovladačů, takže další interakce s hostitelským systémem nejsou potřebné. To vyžaduje minimální konfiguraci a interakci s uživatelem a také nezpůsobuje pokles výkonu.

Hardwarová šifrovací zařízení jsou velmi vhodná pro zajištění bezpečnosti citlivých dat na přenosných zařízeních typu notebook nebo USB flash disk, což zvyšuje ochranu takto uložených dat. Ty jsou pomocí hardwarových klíčů efektivně chráněny i v případě odcizení disků a jejich reinstalace v jiných počítačích.

Úzká místa hardwarových šifrovacích zařízení tkví v jejich cenové náročnosti a závislosti na konkrétním zařízení. Jedno řešení není nasaditelné v rámci celého systému a jeho jednotlivých částí. To zvyšuje nároky na složitost a komplexnost při jejich implementaci Nové a dokonalejší verze musí být řešeny výměnou celého šifrovacího modulu.

Hardwarová enkrypce	
Silné stránky	**Slabé stránky**
autonomní moduly nevyžadují další podporu imunita vůči zranitelnosti a kontaminaci viry nevyžadují instalaci dalších driverů časová úspornost konfigurací a interakcí s uživateli vhodné pro bezpečnost přenosných zařízení nezpůsobují pokles výkonu systémů	cenová náročnost závislost na konkrétním zařízení jedno řešení není nasaditelné pro celý systém složitost a komplexnost řešení nové verze se řeší náhradou zařízení

Technické přínosy HSM

Mezi technické přínosy HSM zmiňované uživateli dále patří:

- certifikace v souladu s bezpečnostními standardy a normami
- zdvojená kontrola ochrany přístupů
- spolehlivost a rozložení zátěže (vysoká dostupnost, sdílení a vyrovnávání zátěže)
- nativní podpora kompletní sady standardních krypto-algoritmů
- tisíce transakcí za sekundu
- dostupnost více klíčů na jednom HSM
- integrace na nejnižších úrovních architektury
- výkonné vývojové nástroje
- flexibilita pro individuální přizpůsobení
- škálovatelnost výkonu

Technické nešvary HSM

Mezi technické nedostatky HSM zmiňované uživateli dále patří:

- nutnost kontroly aplikačních serverů
- potřeba modifikace aplikačního serveru při integraci
- náročnost plánování ve virtualizovaných prostředích

Základní kroky pro nasazení HSM

Hardwarová enkrypce je vhodná pro ty organizace, které spravují extrémně citlivá data. Tyto se v USA rekrutují zejména z odvětví finančních institucí, zdravotnictví a veřejného sektoru. Ovšem ne každá organizace si může dovolit vynaložit vysoké náklady při nasazování těchto řešení a podstoupit komplexnost doprovodných projektů.

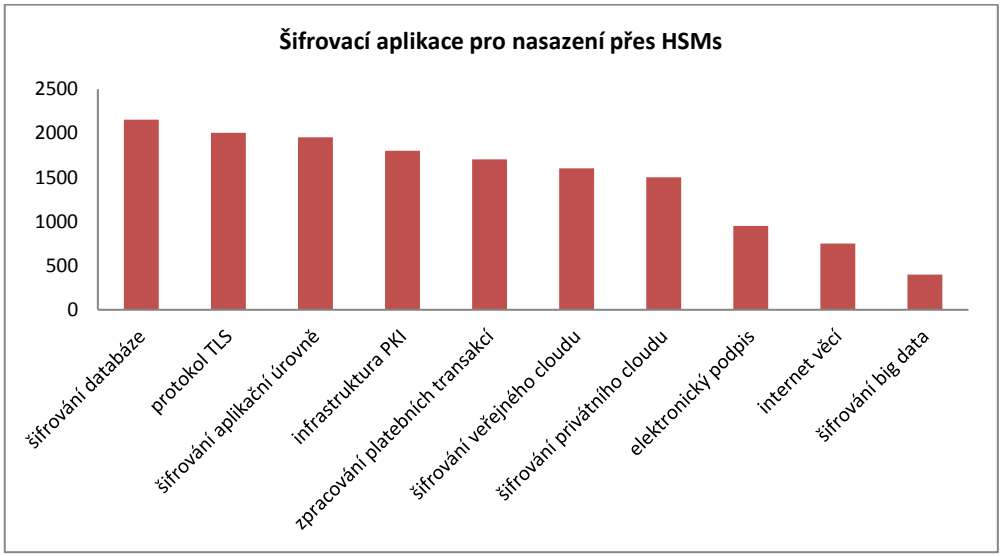
Scénář jednotlivých kroků při přípravě implementace HSM v rámci organizace by měl obsahovat tyto kroky:

- Identifikace kritických datových úložišť
- Zmapování klíčových firemních procesů
- Definice serverů podporujících kritické procesy
- Mapa možných hrozeb
- Naroubování fyzických serverů k definovaným procesům a kritickým datovým souborům
- Posouzení rizik
- Určení aplikačních priorit
- Přijmutí opatření pro zmírnění rizik
- Provedení gap analýzy pro definici a zaměření se na klíčové oblasti implementace

Nasazení HSM v podnikovém prostředí

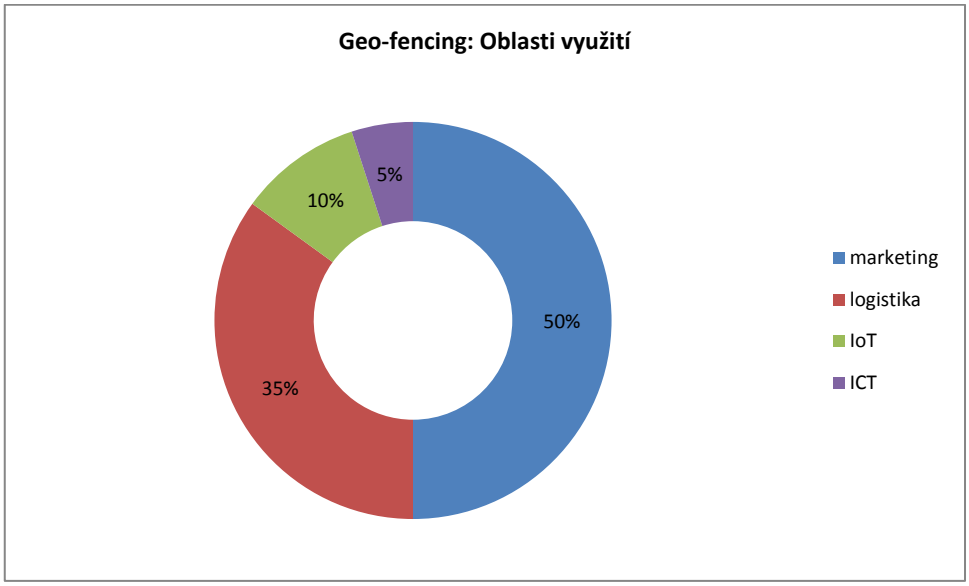
Existují dva možné scénáře zapojení HSM pro šifrování v podnikovém prostředí. První je celkové nasazení HSM v této oblasti (databáze, soubory, TSL, paměti a zálohování), druhý je ten, že HSM supluje pouze šifrovací klíče u jinak softwarového šifrování.

Mezi nejčastěji zmiňované šifrovací aplikace k nasazení HSM v podnikovém prostředí se řadí šifrování databází, šifrování aplikační úrovně a kryptografický protokol Transport Layer Security (TLS), respektive jeho předchůdce SSL (Secure Sockets Layer) poskytující možnost zabezpečené komunikace na internetu pro služby typu elektronické pošty, www a dalších datových přenosů.



13. Geo-fencing čili geo-oplocení

Pojem geo-fencing spojovaný s virtuální perimetrií geografických lokalit založený na globálním polohovém systému GPS je na severoamerickém internetu nejvíce používán v geomarketingu, kde jeho primárním cílem je oslovení zákazníků nacházejících se v konkrétní lokalitě, majících aktivované služby LBS (location based services). Dalším odvětvím, hojně využívajícím geo-fencing je logistika, kde podporuje zajištění pružného sledování zásilek. To je už ale jenom krůček k internetu věcí. Zde se rovněž očekává velké využití geograficky oplocených zón fungujících jako výchozí body pro řízení přístupů z vlastní či sousedních zón. Výraz má ovšem svůj význam i v oblasti IT, kde v rámci tzv. boundary control umí zajistit dedikaci konkrétních serverů, anebo jejich celých clusterů pouze pro určité typy výpočetních úloh. Provést analýzu tohoto termínu ve veřejném americkém diskurzu v kontextu dedikace serverů je o to složitější, že u všech tří vyjmenovaných oblastí hraje svou roli zabezpečení provozu.



SWOT Geo-fencing	
Silné stránky	**Slabé stránky**
navýšení bezpečnosti zvýšení efektivity práce zvýšení produktivity práce tracking provozu možnost bezpečného propojení sítí zaměření na větší územní celky	navýšení správy a administrativy zatížení sítí a připojených zařízení nároky na životnost baterií fixace na definované územní celky (proti Beacon) větší počet schvalovacích procesů
Příležitosti	**Hrozby**
tracking zákazníků větší ad-hoc informovanost zákazníků navýšení počtu zákazníků a tržeb	kyberútoky a hacking zvýšená zranitelnost centralizovaných systémů zvýšená zranitelnost přes radiové vlny