# KAPITOLA 2

# Vaše organizace a cloud computing

Nabídky cloud computingu se přizpůsobují požadavkům odběratelů. Stejně jako se hardwarové a softwarové konfigurace ve vaší firmě liší od konfigurací sousední firmy, budou se rozcházet i vaše požadavky na cloud computing.

Tato kapitola vám pomůže porozumět, jak může vaše společnost cloud computing optimálně využít a která řešení by mohla být pro vaše požadavky nejvhodnější. Při diskuzi o uplatnění cloud computingu rozebereme i jeho omezení. Cloud computing tedy není dokonalý a v některých případech byste se mu měli vyhnout. Prozkoumáme také tyto případy.

## Kde můžete použít cloud computing

Vhodnost nasazení cloud computingu závisí na mnoha faktorech, mezi něž patří:

- Poměr nákladů a výnosů
- Rychlost poskytování
- Využitá kapacita
- Případné předpisy o nakládání s daty
- Organizační struktura vaší firmy a jejích informačních technologií

V některých případech představuje cloud computing optimální řešení podnikových požadavků. Jsou však firmy, pro které koncepce cloud computingu prostě není vhodná. V této sekci se podíváme jednak na to, k čemu lze cloudy použít, a také na to, kdy se jim vyhnout.

## Scénáře

Existují tři různé základní implementace cloud computingu. V detailech se uplatnění cloud computingu v organizacích značně liší, ale z obecného pohledu je lze přiřadit k jednomu z těchto tří řešení.

### Výpočetní cloudy

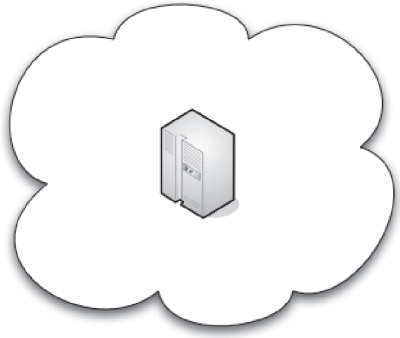
Výpočetní cloudy poskytují přístup k vysoce škálovatelným a levným výpočetním prostředkům dostupným na vyžádání, které slouží ke spouštění požadovaného kódu. Jako tři příklady výpočetních cloudů lze uvést:

- EC2 společnosti Amazon
- App Engine společnosti Google
- Berkeley Open Infrastructure for Network Computing (BOINC)

Nabídka výpočetních cloudů je nejbohatší. Můžete je použít k nejrůznějším účelům – závisí to jen na aplikaci, ke které uživatelé potřebují přistupovat.

Nyní byste mohli tuto knihu zavřít, zřídit si účet u poskytovatele cloud computingu a začít jej používat. Tyto aplikace se hodí pro organizace libovolné velikosti, ale velkým podnikům nemusejí stačit. Neposkytují totiž standardní možnosti správy, sledování a řízení, které tyto podniky očekávají.

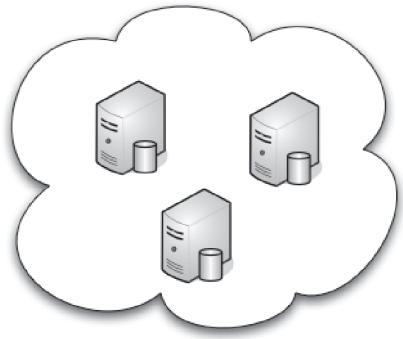
Nikdo však velkým podnikům objednávku rozmlouvat nebude. Amazon nabízí podporu podnikové třídy a objevuje se kategorie cloudů jako je Enterprise Cloud společnosti Terremark, které jsou zacíleny na velké podniky.



Výpočetní cloudy umožňují přistupovat k aplikacím, které fungují na zařízení poskytovatele.

### Úložiště cloudu

Mezi první nabídky technologie cloudu patřila úložiště, která jsou oblíbená i nadále. Oblast úložišť cloudu je velmi rozsáhlá. Tuto službu již poskytuje více než 100 dodavatelů. Jedná se o ideální řešení, chcete-li udržovat soubory mimo firmu.



Úložiště cloudu umožňuje ukládat vlastní data na zařízení dodavatele služby.

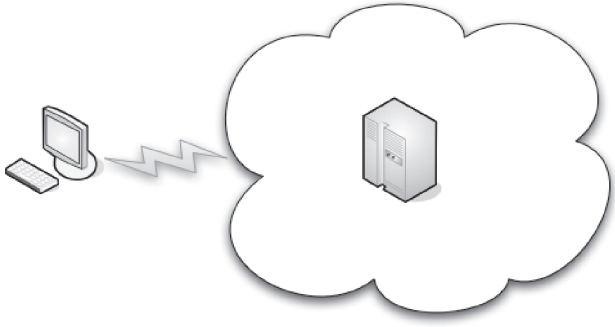
K hlavním faktorům v této oblasti patří bezpečnost a náklady, které se v závislosti na zvoleném dodavateli značně liší. Aktuálně je na špici služba S3 společnosti Amazon.

**Poznámka**

Na společnost Amazon a další poskytovatele cloudů se podrobněji podíváme v další kapitole.

### Aplikace cloudu

Aplikace cloudu se od výpočetních cloudů liší v tom, že využívají software, který závisí na infrastruktuře cloudu. Aplikace cloudu jsou verzí koncepce Software jako služba (SaaS – Software as a Service) a zahrnují webové aplikace poskytované uživateli prostřednictvím prohlížeče nebo aplikace typu Microsoft Online Services. Tyto aplikace přesunují hosting a správu IT do cloudu.



Aplikace cloudu poskytují aplikace, které závisí na infrastruktuře vlastního Internetu.

Aplikace cloudu často eliminují potřebu instalovat a provozovat aplikace v počítačích vlastněných zákazníkem, a tím snižují nároky na správu softwaru, provoz a podporu.

K aplikacím cloudu patří:

- Aplikace typu peer-to-peer (jako BitTorrent a Skype)
- Webové aplikace (jako MySpace či YouTube)
- SaaS (jako Google Apps)
- Software plus služby (jako Microsoft Online Services)

## Kdy není cloud computing vhodný

Nebylo by poctivé, kdybychom cloud computing pouze vychvalovali a doporučovali, abyste jej používali úplně ke všemu. V praxi existuje mnoho situací, kdy cloud computing jednoduše není vhodný. Důvody se přitom mohou měnit od nákladů přes požadavky na hardware až po pouhý nedostatek potřeby.

### Pozor na detaily

Chcete-li používat cloud computing ke zpracování dat, na která se vztahuje zákon HIPAA (Health Insurance Portability and Accounting Act), máte smůlu. Řekněme to jinak: do cloudu nesmíte odeslat data typu HIPAA. Jedná se o citlivé zdravotnické informace a fakt, že by se data typu HIPAA mohla na serveru pomíchat s daty jiné firmy, nejspíš na každého auditora HIPAA zapůsobí jako červený hadr na býka.

**Tabulka 2.1:** Teoretické postihy za nedostatečnou ochranu důvěrných dat

| | Sarbanes-Oxley | FACTA (Fair and Accurate Credit Transactions Act) z roku 2003 | HIPAA |
|---|---|---|---|
| Ředitelé a vedoucí | 1.000.000 USD | | |
| Instituce | 5.000.000 USD | 11.000 USD | 50.000 USD až 250.000 USD |
| Vězení | 20 let | | 1 až 10 let |

I přesto společnosti Google a Microsoft připravují služby pro sektor zdravotnictví: Microsoft pracuje na své službě HealthVault a Google Health má ambici stát se velkým úložištěm soukromých zdravotních dat online.

Úmysly jsou sice šlechetné – nabídnout zákazníkům přístup k jejich zdravotní dokumentaci – stačí pouze malé opomenutí, aby citlivá data unikla.

Pokud máte data regulovaná zákonem (jako jsou HIPAA či Sarbanes-Oxley), měli byste při jejich přenosu do cloudu dbát mimořádné opatrnosti. Jestliže přece uložíte finanční data zákazníka a ta uniknou, co myslíte – bude se váš zákazník hojit na poskytovateli cloudu, nebo na vás?

A mimochodem: abychom podpořili svá varování před únikem soukromých dat pádnými argumenty, připravili jsme tabulku 2.1. Tabulka 2.1 shrnuje potenciální tresty za porušení příslušných zákonů.

Pravděpodobně uděláte nejlépe, když se riziku citelné pokuty, upírských advokátů a možného vězení vyhnete.

### Právní otázky

S ohledem na citlivost soukromých dat je nutno věnovat pozornost faktu, že podle zákonů a zavedených zvyklostí mají vládní agentury snadnější přístup k datům v cloudu než na firemním serveru.

Například zákon Stored Communications Act dává FBI přístup k datům bez nutnosti získat soudní příkaz či souhlas vlastníka.

### Geopolitická hlediska

Odesílání dat do cloudu může být prostě protizákonné. Sídlíte-li například v Kanadě a chcete uložit svá data do amerického cloudu, můžete na to zapomenout.

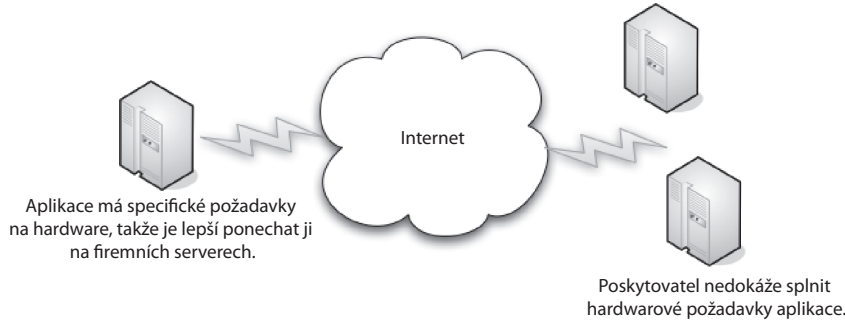
Kanadská vláda prohlásila, že vládní zaměstnanci IT nemohou používat síťové služby, které působí na území USA. Důvod spočívá v tom, že kanadská data by mohla být ohrožena americkým zákonem Patriot Act.

Kanada je sice v USA označována za přátelského severního souseda, ale v současnosti má velmi rozumné zásady. Stačilo by, aby americká vláda zabavila server se zahraničními daty, a v tu chvíli by došlo k mezinárodnímu incidentu.

Totéž se vztahuje i na cloudy, které fungují mimo USA. Pravděpodobně neznáte zákony (pokud vůbec existují), kterými se v cizí zemi řídí ochrana soukromých údajů. Nemůžete zabránit tomu, aby oddíl nohsledů nějakého diktátora neobsadil sídlo poskytovatele a neodvezl si všechny servery i s vašimi daty.

### Hardwarové závislosti

Máte-li aplikaci, která vyžaduje konkrétní hardware, čipy nebo ovladače, nemusí být řešení cloudu pro vás vhodné.




V prvé řadě platí, že máte-li specifické hardwarové požadavky, snižuje se pravděpodobnost, že bude mít poskytovatel služeb k dispozici konkrétní hardware. To může značně omezit vaše možnosti při hledání nejvýhodnější nabídky na trhu poskytovatelů.

Řekněme však, že máte mimořádné štěstí, poskytovatel má hardware, jaký potřebujete, a zakrátko již vše funguje podle vašich představ. To je sice skvělé, ale jestliže poskytovatel časem vymění čipovou sadu nebo jinou kritickou hardwarovou komponentu, můžete se dostat do problémů.

### Kontrola nad serverem

Pokud vaše aplikace vyžaduje úplnou vládu nad všemi spuštěnými procesy, nebude řešení cloudu pro vás nejspíš vhodné. Potřebujete-li podrobnější kontrolu dostupné paměti, procesoru, vlastností pevného disku nebo rozhraní, nebude cloud pro vaši aplikaci vyhovovat. Všechny tyto parametry má přece na starosti poskytovatel služeb.

**Poznámka**

V některých cloudech dokonce nedostanete ani přístup uživatele root. Jestliže potřebujete pokročilé úrovně přístupu, nezapomeňte se seznámit s tím, co váš potenciální dodavatel umožňuje.

### Náklady

Mezi velká lákadla cloud computingu patří úspora nákladů. Obvykle je totiž levnější provozovat aplikaci v cloudu než investovat do infrastruktury, koupit příslušnou aplikaci a poté zajišťovat její každodenní správu.

V delším časovém horizontu však mohou platby předplatného služeb cloudu převýšit cenu za nákup vlastních serverů. Je proto potřeba zohlednit vše od prostor přes zaměstnance a software až po hardware.

Náklady a způsob fungování cloudu představují pohyblivý cíl. Podle některých názorů může cloud přesunout servery do datového centra klienta. Jiná myšlenková koncepce se označuje jako *cloud bursting*. V tomto scénáři lze nárazově na vyžádání pořizovat kapacitu do cloudu.

### Nedostatek potřeby

Od svých dědečků známe výrok: „Když to není rozbité, nespravuj to“. A děda měl pravdu. Pokud vaše aktuální řešení funguje, proč do něj vrtat?

Samozřejmě že existují případy, kdy se vám cloud computing vyplatí. A v těchto situacích po něm rozhodně sáhněte. Jestliže však přesunujete aplikace do cloudu jen proto, že je to módní, podívejte se na nějaké staré fotografie „vymóděných“ lidí. Uvědomte si, že polyesterové obleky a ulíznuté účesy možná kdysi módní byly, ale dnes už to neplatí.

### Integrace se stávajícími aplikacemi

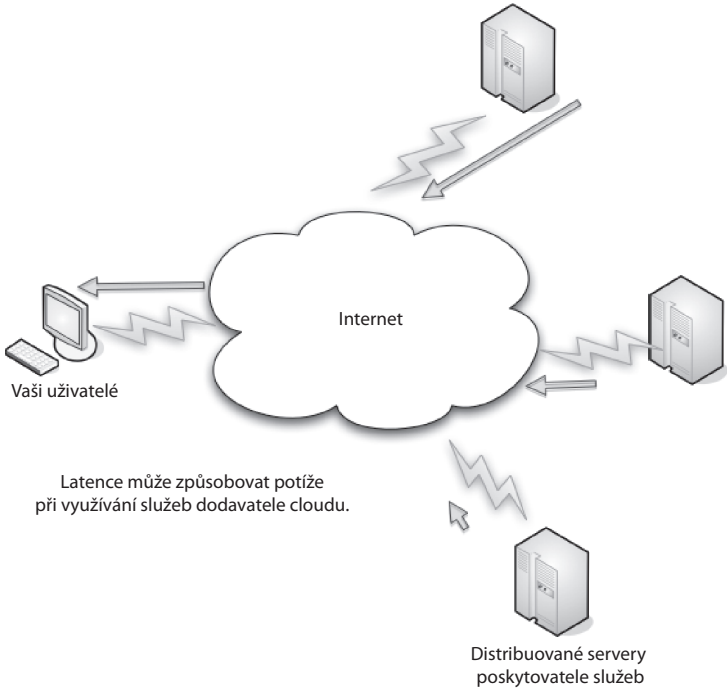
Pokud smícháte olej a vodu, dostanete lávovou lampu. Vzhledem k nadpisu této sekce už určitě víte, kam míříme. Po pravdě řečeno, máte-li dvě aplikace, které je potřeba integrovat, je lepší, když jedna nebude ve firemní síti a druhá v cloudu.

V tom případě vznikají problémy se zabezpečením, rychlostí a spolehlivostí. Jestliže máte například dvě databáze – jednu s citlivými daty hostovanou lokálně a druhou s veřejnými daty v cloudu – je velmi pravděpodobné, že se citlivá data nakonec ocitnou v cloudu.

Platí také, že pokoušíte-li se provozovat vysoce výkonnou aplikaci ve své režii a tato aplikace se spoléhá na data z cloudu, bude fungovat pouze tak rychle, jak to cloud dovolí. To opět vede ke kolísavé spolehlivosti. Nedojde kvůli všem těm přesunům k prozrazení nebo poškození dat?

### Hlediska latence

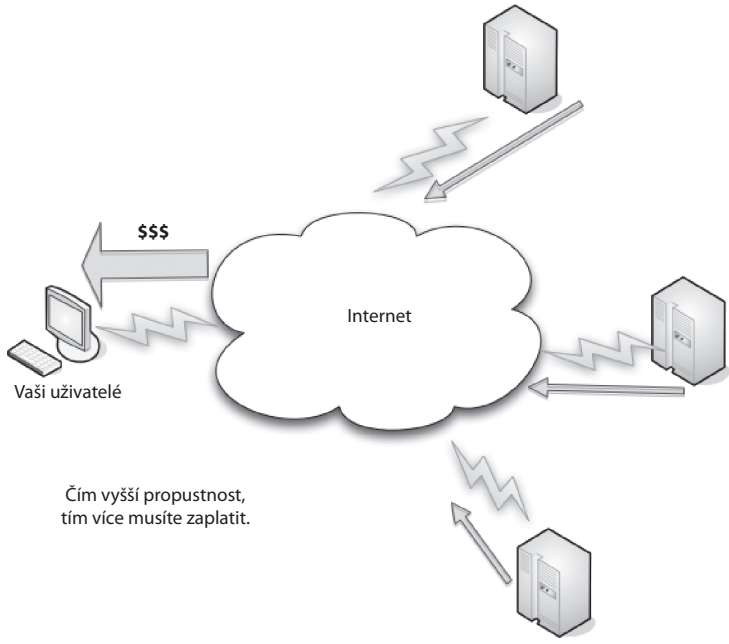
Vaše data a aplikace jsou umístěny na řadě serverů, které jsou geograficky vzdáleny od sídla vaší společnosti. Proto chvíli trvá, než se k vám potřebná data dostanou. Není to otázka hodin nebo dnů, dokonce ani minut. Pokud však potřebujete mít data dostupná okamžitě, nemusí cloud představovat optimální volbu.




Přenos dat určitou dobu trvá. Může se stát, že data vyžádaná zaměstnancem dorazí zhruba za sekundu, což je v určitých případech přijatelné. Jestliže však tento zaměstnanec požaduje data rychleji než se sekundovým zpožděním, nemusí už rychlost stačit.

### Požadavky na propustnost

Vzhledem k tomu, že se cloud computing obvykle fakturuje stejným způsobem jako voda či elektřina, platíte za spotřebu. To je skvělé a zdá se to být i spravedlivé, dokud nezačnete nasazovat aplikace, které vyžadují vysokou propustnost. V tom případě budou vzrůstat i náklady. Jestliže například streamujete video s vysokým rozlišením pro více než 100 odběratelů, budou se náklady prudce zvyšovat.




Je vhodné, když si to předem pečlivě spočítáte. Zohledněte náklady na server, jeho napájení a veškerý další hardware. Zahrňte cenu správy a příslušných mzdových nákladů na zaměstnance IT a poté výsledek porovnejte s cenou, kterou vám bude účtovat poskytovatel služeb. Jestliže je nákup serveru levnější, může být pro vás lepší, když na cloud prozatím zapomenete. Avšak i když budou náklady stejné, musíte si položit otázku, co je pro vás výhodnější.

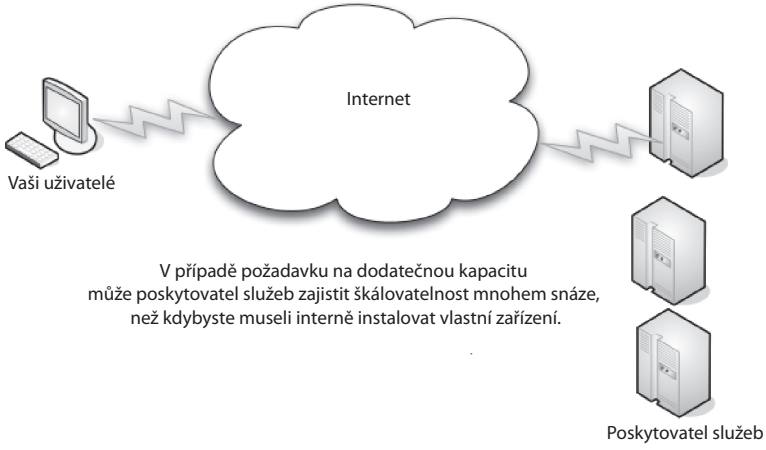
# Výhody

Vaše organizace bude mít jiné potřeby než sousední firma. Cloud computing však často dokáže s požadavky na IT pomoci. Podívejme se blíže na to, co může cloud computing vaší organizaci nabídnout.

## Škálovatelnost

Jestliže předpokládáte vysoký nárůst výpočetních požadavků (nebo jste dokonce náhlými požadavky překvapeni), může vám cloud computing pomoci tuto situaci zvládnout. Místo toho, abyste museli koupit, instalovat a konfigurovat nová zařízení, můžete si objednat dodatečné procesorové cykly nebo kapacitu úložiště u třetí strany.

Vzhledem k tomu, že náklady tohoto řešení závisejí na spotřebě, pravděpodobně nebudete platit tolik, kolik by vás stál nákup nového vybavení.




Jakmile vaše požadavky na dodatečnou kapacitu pominou, můžete služby poskytovatele cloudu jednoduše přestat využívat a nemusíte řešit, co s nepotřebnými zařízeními. Stačí pouze zvyšovat a snižovat spotřebu s ohledem na firemní potřeby.

## Jednoduchost

Jak už jsme uvedli, nemusí-li zaměstnanci IT kupovat a konfigurovat nová zařízení, mohou se soustředit na koncepční záležitosti. Díky řešení cloudu mohou aplikace okamžitě začít fungovat za zlomek ceny, kterou by si vyžádalo vnitrofiremní řešení.

## Zkušení dodavatelé

Když vzroste obliba nové technologie, objeví se zpravidla mnoho dodavatelů, kteří nabízejí svou vlastní verzi. To není často dobré, protože mnoho z nich poskytuje nekvalitní služby. Průkopníky v oblasti cloud computingu jsou však velmi renomované společnosti.

Firmy jako Amazon, Google, Microsoft, IBM a Yahoo! jsou důvěryhodné, protože poskytují spolehlivé služby, dostatečnou kapacitu a kromě toho jsou dobře známé.

## Více interních prostředků

Přesunete-li na třetí stranu ty požadavky na zpracování dat, které nejsou pro vaši firmu kritické, může vaše oddělení IT získat více prostoru k práci na důležitých úkolech souvisejících s činností organizace. Kromě toho nemusíte kvůli plnění nízkoúrovňových úkolů zajišťovat dodatečné pracovníky a jejich školení.

Výpadky sítě představují pro zaměstnance IT noční můru. Další výhoda tedy spočívá v tom, že se zátěž s jejich řešením přesunuje na poskytovatele služeb. K výpadkům samozřejmě dochází, ale ať se o opětovné zprovoznění služeb stará raději Amazon.

Když hledáte poskytovatele služeb, vyberte si takového, který poskytuje 24hodinovou pomoc a podporu a dokáže reagovat na nouzové situace.

## Zabezpečení

S využíváním služeb dodavatele cloudu je spojeno mnoho bezpečnostních rizik, ale renomované firmy se snaží zajistit maximální ochranu.

**Poznámka**

O některých aspektech zabezpečení se zmíníme v další části této kapitoly.

Dodavatelé mívají přísné zásady na ochranu soukromí a nasazují striktní bezpečnostní opatření, jako jsou osvědčené šifrovací metody pro autentizaci uživatelů.

Kromě toho můžete svá data před uložením do cloudu poskytovatele vždy zašifrovat sami. V některých případech můžou být data díky vašemu šifrování a bezpečnostním opatřením dodavatele bezpečnější, než kdybyste je ukládali v rámci své firmy.

# Omezení

Také v jiných případech není cloud computing optimální volbou pro vaše výpočetní potřeby. V této sekci si vysvětlíme, proč se některé aplikace příliš nehodí pro nasazení do cloudu. Nechceme, aby tyto případy vypadaly důležitější než jsou, ale měli byste si být některých limitů vědomi. Pokud je dokážete obejít, je to skvělé, ale před rozsáhlým nasazením byste měli tato rizika znát.

## Vaše citlivé informace

Již jsme hovořili o riziku ukládání citlivých informací do cloudu, ale tuto otázku je potřeba znovu zdůraznit. Jakmile svá data přenesete k poskytovateli služeb, ztratíte jednu úroveň kontroly.

### Proč se toho obávat?

Řekněme, že finanční analytik v aplikaci Google Spreadsheets zpracovává seznam rodných čísel zaměstnanců. Nejen účetní firma by měla tato data chránit před hackery a porušením interních předpisů o zpracování dat. V technickém slova smyslu se jedná rovněž o problém společnosti Google. Google se však může zbavit své odpovědnosti ve smlouvě, kterou s vámi uzavírá. Úkol dostatečného zabezpečení citlivých informací tedy není o nic snazší. Kromě toho jsou zde široce otevřené dveře pro vyšetřovací orgány, aby si mohly tato data vyžádat. Vlády obvykle získají informace mnohem snáze od třetích stran, než ze serveru v držení dotčené organizace.

Méně poctiví poskytovatelé služeb mohou tato data dokonce sdílet s marketingovými firmami. Jiní mohou zase na základě smlouvy, kterou jste s nimi bez čtení podepsali, získat přístup ke čtení a katalogizaci vašich informací a jejich využití způsobem, jaký jste vůbec nezamýšleli. Opět se bezpečně ujistěte, že smlouvě uzavřené se svým poskytovatelem služeb plně rozumíte, souhlasíte s jejími podmínkami a přijímáte je.

Měli byste si uvědomit, jakými zásadami se poskytovatel řídí při správě a údržbě vašich dat. Například společnost Google ve svých zásadách informuje o tom, že bude sdílet vaše data s vládou v případě, že má „dobrý důvod věřit“, že je takový přístup nutný ke splnění zákonných požadavků.

Nepochybně již došlo k uvolnění soukromých dat. V roce 2006 poskytla společnost AOL na svém veřejném webu výzkumníkům vyhledávané termíny 650.000 uživatelů. V roce 2007 předaly firmy

Microsoft a Yahoo! některá vyhledávaná data americkému ministerstvu spravedlnosti v rámci vyšetřování dětské pornografie. Samozřejmě nikdo nechce, aby sexuální násilníci unikli trestu za své zločiny, ale zamyslete se nad důsledky, pokud by vaše nevinná data byla přimíchána k datům, která společnosti Yahoo! a Microsoft poskytly vládě, a vy byste se nezaviněně dostali do vyšetřování.

**Poznámka**

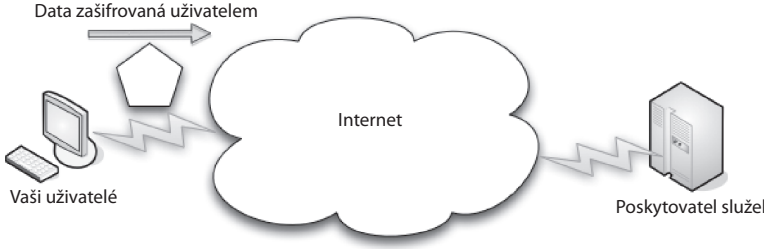
Jestliže poskytovatelé dostanou „utajené" požadavky na data, mohou mít ze zákona zakázáno sdělit svým klientům, že jejich data poskytli vládnímu orgánu.

V médiích navíc pravidelně slyšíme o případech, kdy prodejcům uniknou čísla kreditních karet. V roce 2007 britská vláda dokonce ztratila 25 milionů záznamů o daňových poplatnících.

Z toho plyne poučení, že máte-li citlivá nebo cenná data, cloud pravděpodobně není nejlepší místo, kam je uložit.

### Ochrana dat

To neznamená, že byste svá data nemohli v cloudu uchovávat. Musíte pouze zajistit, že budou chráněna. To nejsnáze zabezpečíte tak, že data před odesláním třetí straně zašifrujete. Programy jako PGP (*http://www.pgp.com*) nebo TrueCrypt (*http://www.truecrypt.org*) typu open-source umí soubory zašifrovat, aby byly přístupné pouze tomu, kdo zná heslo.




Když data před odesláním poskytovateli služeb zašifrujete, máte jistotu, že zůstanou v bezpečí i tehdy, dojde-li k narušení bezpečnostních opatření poskytovatele.

Data ochráníte tím, že je před odesláním zašifrujete. Pokud se k vašim datům dostane někdo nepovolaný, uvidí bez správného klíče pouhou změť nesmyslných znaků.

To se samozřejmě týká dat, se kterými manipulujete ve firmě a poté je odesíláte do cloudu. Jestliže pracujete s textovými či tabulkovými procesory online (oproti pouhému ukládání souborů na webu), pak nemusí být data uložená do cloudu zašifrována.

Obecně raději hledejte placené služby namísto těch, které mají příjmy z reklamy. Druhá uvedená skupina poskytovatelů pravděpodobně doluje v datech uživatelské profily, které může využít k marketingovým či jiným účelům. Žádná firma nemůže dlouho zůstat na trhu a přitom poskytovat reálné služby či zboží zadarmo. Nějak ty peníze vydělat musí, že?

Když máte pochybnosti, uložte svá data vždy tam, kde si můžete být jejich bezpečností nejvíce jisti – i kdyby to znamenalo jejich ponechání ve vlastní serverovně do doby, než vyvinete alternativní důvěryhodné řešení.

## Nepřipravené aplikace

V některých případech však na použití v cloudu nejsou připraveny samotné aplikace. Mohou mít drobná specifika, která znemožní dosáhnout jejich plného výkonu, nebo nemusí fungovat vůbec.

V prvé řadě může aplikace vyžadovat ke komunikaci s uživateli velkou šířku pásma. Pamatujte, že protože se cloud computing účtuje podle spotřeby, může být dlouhodobě levnější provozovat aplikaci lokálně, dokud ji nepřepíšete nebo jinak neupravíte tak, aby komunikovala efektivněji.

Značné úsilí si také může vyžádat integrace aplikace s jinými aplikacemi. Jestliže se pokusíte o přechod do cloudu, mohou se očekávané úspory vypařit kvůli dodatečným nákladům na integraci. V tomto případě může být ekonomičtější aplikaci i nadále hostovat místně.

Pokud aplikace potřebuje komunikovat s lokální databází, může být lepší aplikaci rovněž hostovat lokálně, dokud nedokážete do cloudu přesunout celou infrastrukturu. Opět se tím vyhnete nákladům na přenos dat do cloudu a zpět. Je to také efektivnější, protože aplikace může interagovat s databází bez přenosu zpráv po síti.

Některé aplikace nedokáží po Internetu komunikovat bezpečně. Jestliže nepodporují zabezpečenou komunikaci nebo komunikaci tunelem, ohrožují tím bezpečnost dat. V případě, že vaše aplikace neumožňuje zabezpečenou komunikaci, musíte ji hostovat místně, kde máte k ochraně dat při jejich přenosu po síti jiné možnosti.

Kromě toho při zobrazování výsledků aplikace v rozhraní typu webového prohlížeče je potřeba zajistit, že je aplikace kompatibilní s různými prohlížeči a bude správně fungovat při šifrovaném přenosu typu SSL. Pokud nelze výsledky aplikace v případě potřeby zobrazit zabezpečeně, je řešení založené na cloudu prakticky bezcenné.

Spoléháte-li se na dostupnost aplikací v cloudu, můžete rovněž narazit. Dostupnost závisí na tom, zda vývojář požadované aplikace vyvinul verzi, která je s technologií cloudu kompatibilní. V případě, že aplikace není připravena, můžete mít smůlu.

To však neznamená, že neexistuje žádné řešení. Můžete vždy napsat svou vlastní aplikaci.

## Vývoj vlastních aplikací

Potřebné aplikace jsou často již k dispozici. Někdy však můžete požadovat velmi specifickou aplikaci. V takové situaci se o její vývoj musíte postarat sami.

### Vyhrňme si rukávy

Vývoj vlastních aplikací může rozhodně představovat problém, pokud programovat neumíte a žádné programátory nezaměstnáváte. Potom musíte najmout softwarovou firmu (nebo vývojáře), případně se omezit na aplikace, jaké poskytovatel nabízí.

Určité programátorské dovednosti se hodí nejen při nasazení aplikací. Máte-li v cloudu databázi, potřebujete pro přístup k datům a jejich správu přizpůsobené rozhraní a určité znalosti jazyka SQL (Structured Query Language).

Jedná se pouze o malou překážku, protože velmi pravděpodobně již máte na výplatní listině programátory, kteří potřebný kód obratem sestaví. Jestliže takového zaměstnance nenajdete, můžete vždy zaplatit externí firmě nebo jednotlivci. Koho budete muset najmout a kolik vás to bude stát, závisí na rozsahu příslušné aplikace.

### Výhody tohoto řešení

Je potřeba říci, že přesunutí databázových požadavků do cloudu může být velmi užitečné z hlediska škálovatelnosti. Pokud k serverům přistupuje příliš mnoho uživatelů, nastanou v určitém bodě problémy. Toto riziko lze zmírnit díky automatické škálovatelnosti prostředků, které spoléhají na cloud.

Často se říká, že tato generace webových služeb je založena na LAMP. To je sada jednoduchých a výkonných webových technologií, které pohánějí mnoho oblíbených i menších webů. LAMP je zkratkou následujících termínů:

- **Linux –** operační systém typu open-source
- **Apache –** webový server typu open-source
- **MySQL –** relační databáze jazyka SQL (Structured Query Language) pro webové servery, která je rovněž typu open-source
- **Perl –** programovací jazyk

LAMP se často používá díky své jednoduchosti. Vzhledem ke snadnému použití můžete aplikace zprovoznit velmi rychle.

Toto řešení samozřejmě není dokonalé. První problém leží ve škálovatelnosti.

Potíže se škálovatelností vycházejí z počtu vláken a připojení soketu ve webovém serveru Apache. Není-li server správně vyladěn a zvýší se jeho zátěž, mohou nastat problémy.

Větší potíže se škálovatelností způsobuje databáze MySQL. Relační databáze těžko překračují určitou kapacitu, což je dáno způsobem, jakým reprezentují informace. Když dosáhnete daného limitu, komplikuje se správa databáze.

Uvedené potíže můžete obejít postupem, který se označuje jako rozdělování dat. Tato metoda dovoluje rozdělit data na nezávislé sady, již lze neomezeně škálovat. Pokud však data není možné rozdělit, můžete přejít na distribuovanou databázi, což směruje na řešení cloudu.

To přestavuje výhodu, protože cloud dovoluje neomezené škálování. Stačí pouze přidávat další servery. V praxi můžete škálovat od 1.000 k 1.000.000 uživatelů pouhým přidáváním více serverů.

# Hlediska zabezpečení

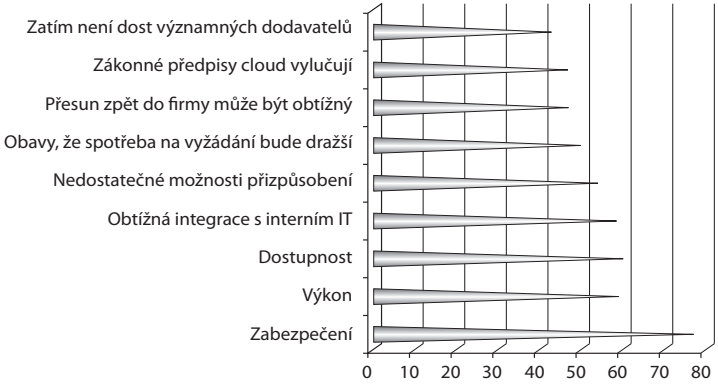
Stejně jako u mnoha jiných technických voleb má zabezpečení v oblasti cloud computingu dvě strany – existují výhody i nevýhody. V této sekci prozkoumáme zabezpečení v cloudu a ukážeme si, co je dobré a čemu je potřeba věnovat zvláštní pozornost.

Společnost IDC provedla průzkum u 244 vedoucích pracovníků IT o službách cloudu. Jak je patrné z obrázku 2.1, představovalo zabezpečení se 74,5 procenty nejčastější zdroj obav.

Dodavatelé, kteří chtějí uspět, musejí při nabízení svých služeb cloudů brát podobná data v úvahu.

## Obavy o soukromí dat u třetí strany

Hlediska ochrany soukromí se automaticky objevují jako první. Pokud tedy jiná organizace hostuje všechna vaše data, jak víte, zda jsou v bezpečí? Ve skutečnosti to nemůžete vědět. Pro začátek předpokládejte, že cokoli umístíte do cloudu, bude přístupné pro kohokoli jiného. Existují také obavy dané tím, že vyšetřovací orgány se mohou k datům udržovaným v cloudu dostat snáze než k datům na serverech dotčené organizace.




**Obrázek 2.1** Podle zjištění IDC jsou otázky zabezpečení hlavním problémem, se kterým se cloud computing potýká

To neznamená, že neexistují renomované firmy, které by nikdy nenapadlo vaše data narušit a které se nacházejí na špičce síťového zabezpečení dat. Ve světě, kde jsou sklenice napůl plné, to dělají všechny firmy. V praxi je však situace taková, že i když se poskytovatelé maximálně snaží data zabezpečit, může přesto dojít k útoku hackerů a vaše citlivé informace jsou pak vydány na milost a nemilost útočníkům.

Nejlepším plánem prevence útoku je neprovádět na platformě cloudu kriticky důležité činnosti ani vysoce citlivé aktivity, aniž by vaše organizace implementovala rozsáhlé bezpečnostní kontroly. Jestliže zabezpečení na této přísné úrovni nedokážete zajistit, zůstaňte u méně kritických aplikací, které se lépe hodí pro cloud a více odpovídají standardním bezpečnostním nastavením. Pamatujte, že nikdo nemůže zcizit kritické informace, které nejsou k dispozici.

## Dělají pro zabezpečení dost?

Než se upíšete známému dodavateli, pamatujte také na to, že se o ochranu vašich dat maximálně snaží. Podle některých názorů se dodavatelé musejí předhánět, aby zajistili co nejvyšší ochranu dat. Jedná se prostě o obchodní nutnost. Pokud se rozkřikne, že ukládaná data nechrání, nikdo si jejich služby nebude chtít objednat.

Je také potřeba zmínit otázku výkonu a efektivity. Platíte za průběžnou spotřebu a pokud tedy věnujete na provoz bezpečnostních nástrojů dodavatele nadměrnou kapacitu procesoru, bude lepší poohlédnout se po konkurenci.

Zatímco bychom tedy chtěli věřit, že dodavatelé dělají, co mohou, nemusí to stačit. Existuje mnoho způsobů, jakými může dojít k narušení cloudu a vašich dat.

### Hackeři

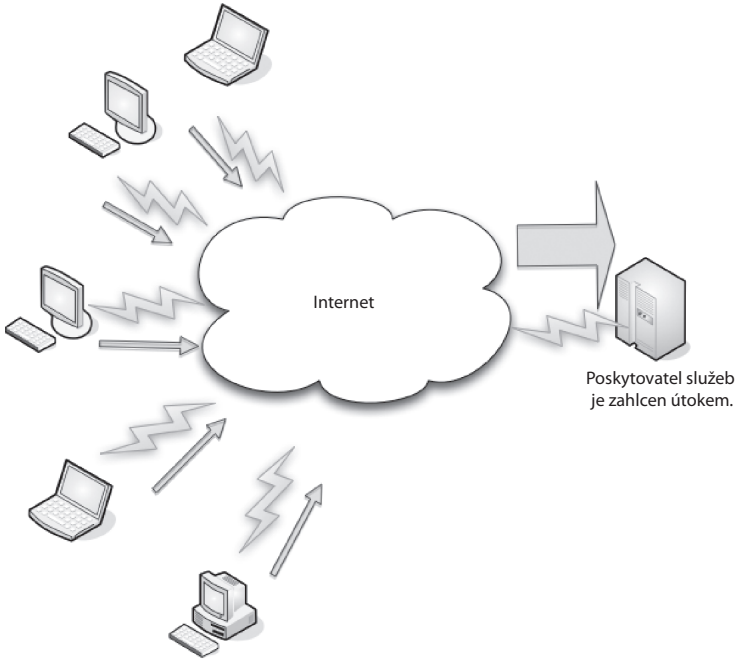
Hackeři nejsou ti milí podivíni, jaké nám ukazuje Hollywood. Většina z nich nesedí u coly a nesnaží se proniknout do zabezpečené sítě jen proto, že to jde. Chtějí něco konkrétního.

Pokud se jim podaří narušit vaše data, mohou nadělat hodně škod. Může se jednat například o prodej vašich firemních tajemství konkurenci nebo o pokoutné zašifrování dat, aby vás pak mohli vydírat. Případně mohou vše vymazat s cílem poškodit váš podnik, což si zdůvodňují svou ideologií. To se může stát a také se to stává.

V každém případě představují hackeři skutečnou hrozbu datům, která udržujete v cloudu. Vzhledem k tomu, že svá data udržujete na cizím zařízení, můžete být odkázáni na libovolná bezpečnostní opatření, která dodavatel podporuje.

### Útoky botnetů

Jako nejhorší případ se často udává scénář, kdy útočníci pomocí botnetů provedou útok typu DDoS (distributed denial of service). Hackeři poté za zastavení útoků na síť požadují peníze.




Hackeři nakonfigurují systémy pro odesílání paketů útoků typu DDoS, které poskytovatele služeb vyřadí z provozu.

V Japonsku se vydírání spojené s útoky DDoS objevuje stále častěji. Jedna velká firma v Tokiu musela zaplatit 3 miliony jenů (asi 31.000 USD) poté, co útok botnetů její síť zcela zablokoval. Vzhledem k tomu, že tento typ útoků je tak rozptýlený, nedokázala policie útočníky vystopovat.

Ve světě cloud computingu se rozhodně jedná o oprávněnou obavu. Pokud dojde k útoku na vaše data v cloudu, ke komu si vyděrači přijdou pro peníze? Budete to vy? Nebo snad dodavatel? A bude někdo výkupné skutečně platit?

## Výhody zabezpečení

Tím nechceme naznačit, že vaše data v cloudu nejsou v bezpečí. Poskytovatelé se snaží bezpečnost zajistit. Jinak by se to rozneslo a jejich podnikání by se nerozvíjelo. Kvůli samotné povaze cloudu je však nutné nasadit některé velmi silné bezpečnostní metody.

### Centralizace dat

Již jsme zmínili riziko ztráty dat uchovávaných na jednom místě. Centralizace dat je však spojena s některými velmi účinnými bezpečnostními postupy. V praxi můžete svůj systém lépe zabezpečit už z podstaty.

**Omezení ztráty dat –** na letištích v USA se každý rok ztratí více než 12.000 notebooků. Dost nepříjemná je už samotná ztráta dat, ale zvláště citelná je pro společnosti, které přijdou o firemní tajemství nebo jiné kritické informace.

Kolik notebooků je pak chráněno skutečně silnými bezpečnostními opatřeními, jako je šifrování celého datového disku? Pokud je možné systém notebooku snadno narušit, dostanou se informace do rukou zloděje.

Když udržujete data v cloudu, nasadíte silné řízení přístupu a umožníte zaměstnancům stahovat pouze data, která ke své práci potřebují, může cloud computing omezit objem potenciálně ztracených informací.

**Monitorování –** pokud udržujete data v cloudu, můžete sledovat zabezpečení snáze, než kdybyste se museli starat o bezpečnost mnoha serverů a klientů. Samozřejmě, data jsou ohrožena rizikem narušení vlastního cloudu, ale pokud si budete bezpečnostních hrozeb vědomi a budete jim aktivně předcházet, můžete se soustředit pouze na jediné klíčové místo.

### Okamžitá výměna

Jsou-li vaše data narušena, můžete při zjišťování pachatelů okamžitě přesunout svá data na jiný stroj.

Nechcete přece vysvětlovat nejvyššímu vedení, že systém nefunguje kvůli bezpečnostnímu incidentu. Uživatelé si přepnutí nemusejí ani všimnout. Není nutné strávit hodiny replikací dat nebo opravou průniku. Díky abstrakci od hardwaru to lze provést během okamžiku.

### Protokolování

Protokolování v cloudu se dostává na vyšší úroveň. Protokolováním se zákazníci obvykle zabývají později, až nastávají potíže s úložným místem. V cloudu není potřeba odhadovat, kolik úložného místa budete potřebovat. Pravděpodobně si ponecháte protokoly od samého začátku, když pro nic jiného, tak kvůli kontrole své spotřeby.

Můžete také nasadit pokročilejší metody protokolování. Je například možné aplikovat záznam pro audit C2. Tato volba se obecně používá jen zřídka, protože by mohla mít značný vliv na výkon sítě. Cloud však dovoluje dosáhnout i takové úrovně granularity.

### Bezpečná sestavení softwaru

Chcete-li při vývoji vlastní sítě dosáhnout požadované úrovně zabezpečení, musíte nakoupit bezpečnostní software třetích stran. U řešení cloudu mohou být tyto nástroje zahrnuty ve službě a svůj systém můžete rozvíjet s libovolnou požadovanou úrovní bezpečnosti.

Lze také aplikovat opravy a upgrady offline. Když instalujete opravu serveru, můžete jej ponechat v bezpečí ve stavu offline. Virtuální počítač můžete znovu převést do stavu online, až práci dokončíte.

Nakonec se zlepšují možnosti testování dopadu bezpečnostních změn. Stačí vyzkoušet v produkčním prostředí verzi offline. Díky tomu můžete ještě před přesunutím online zkontrolovat, zda provedené změny nenaruší síť.

### Lepší zabezpečení softwaru

Dodavatelé obvykle vyvíjejí účinnější bezpečnostní software. Vzhledem k tomu, že se účtují cykly procesoru, můžete si náročného programu všimnout a stěžovat si, jestliže cena příliš vzrůstá. Dodavatelé nechtějí přijít o své zákazníky, a proto jsou tlačeni k tomu, aby jejich bezpečnostní software fungoval co nejefektivněji. Dodavatel navíc obvykle sleduje celou bezpečnostní konfiguraci a vyladí její jednotlivé prvky s ohledem na celý systém. Smetanu slízne ten dodavatel, jehož bezpečnostní produkt funguje nejlépe.

### Bezpečnostní testování

Poskytovatelé SaaS nefakturují bezpečnostní testování jednotlivým uživatelům. Tyto náklady se dělí mezi všechny uživatele cloudu. Vzhledem k tomu, že sdílíte cloud s jinými zákazníky (nikdy se s nimi nesetkáte, ale jsou tam), můžete své výdaje na bezpečnostní testování snížit.

To platí i u koncepce PaaS, kde vývojáři vytvářejí svůj vlastní kód. Nástroje cloudu pro skenování kódu jej však automaticky testují, zda neobsahuje bezpečnostní slabiny.

# Otázky zákonných předpisů

Málokdy voláme po tom, aby stát do našeho podnikání zasahoval více. V případě cloud computingu však může být regulace přesně tím, co obor potřebuje. Bez platnosti určitých pravidel by nebylo nic snadnějšího, než aby neseriózní poskytovatelé šetřili na zabezpečení dat, nebo je dokonce zcizili.

## Aktuálně chybějící předpisy

V současnosti není obor nijak regulován, i když by měl být. V září 2008 převzala vláda USA kontrolu nad bankou Washington Mutual. Považuje se to za největší pád banky v americké historii. Měli bychom si tedy uvědomit, že zkrachovat mohou všechny společnosti bez ohledu na svou velikost.

Podívejte se například na firmu Google. Je hodně velká a nedávno dosáhla tržní kapitalizace 107 miliard USD. Vzhledem k velikosti a hodnotě by se mohlo zdát, že je nezranitelná. Banka WaMu však před svým kolapsem měla hodnotu 307 miliard USD.

Poskytovatele služeb cloudu sice není možné házet do jednoho pytle s bankami, ale toto přirovnání přesto naznačuje potřebu regulace. Banky sice manipulují s penězi a poskytovatelé služeb cloudu s daty, ale obě tyto komodity mají pro jednotlivce i firmy mimořádnou cenu. Fakt, že na banky se určitá regulace vztahuje (v podobě zákonného pojištění vkladů), zabránila útoku střadatelů na banku. Když se banka WaMu zhroutila, díky pojištění vkladů nikdo o peníze nepřišel. Neexistuje přitom žádná třetí strana, která by pojišťovala jakákoli data v cloudu. Jestliže se poskytovatel rozhodne ukončit svou podnikatelskou činnost, mohou být vaše data ztracena.

## Vláda jako zachránce?

Je úkolem vlády regulovat cloud computing? Jak jsme již uvedli, platí kvůli Velké depresi v USA předpisy, které ochránily zákazníky banky WaMu při jejím pádu před ztrátou peněz.

Tato otázka rozděluje odborníky na dvě skupiny. Jestliže vláda dokáže najít způsob, jak data zabezpečit (buď před ztrátou, nebo zcizením), měla by to přivítat každá společnost, která takové ztrátě čelí. Na druhou stranu existují ti, kdo si myslí, že vláda by neměla překážet a ponechat vývoj cloud computingu na konkurenci a tržních silách.

### Kdo vlastní data?

Existují důležité otázky, na které musí vláda najít odpověď. Za prvé: kdo vlastní data? Měly by mít navíc vládní vyšetřovací agentury snadnější přístup k osobním informacím v datech cloudu, než k informacím uloženým v osobním počítači?

Velký problém spočívá v tom, že uživatelé služeb cloudu nerozumějí důsledkům, jaké má práce s jejich e-mailovými účty online, účty služby LinkedIn, stránkami na Facebooku atd. na jejich soukromí a bezpečnost. Jedná se sice o oblíbené weby pro jednotlivce, které se však přesto považují za služby cloudu a jejich regulace by ovlivnila služby cloudu pro firmy.

Americké soudy se při svém rozhodování zatím přiklánějí k názoru, že soukromá data uložená v cloudu nepožívají stejné úrovně ochrany před prohlídkami vyšetřovacích agentur jako data uložená v osobních počítačích.

Zpráva, kterou v září 2008 vydal projekt Pew Internet and American Life, informuje o tom, že 49 procent občanů USA, kteří používají služby cloud computingu, mají značné obavy z toho, že budou poskytovatelé jejich data sdílet s vládními vyšetřovacími agenturami.

Uveďme si některé zjištěné obavy, které se týkají cloud computingu:

- Osmdesát procent respondentů řeklo, že by jim značně vadilo, kdyby dodavatel použil jejich fotografie nebo jiné informace v marketingových kampaních.
- Šedesát osm procent prohlásilo, že by jim značně vadilo, pokud by jim dodavatel na základě jejich osobních informací zobrazoval přizpůsobené reklamy.
- Šedesáti třem procentům uživatelů by značně vadilo, jestliže by si poskytovatelé služeb ponechali jejich data i po jejich uživatelském vymazání.

### Používání státními institucemi

Existují také otázky, zda mohou vládní agentury ukládat svá data do cloudu. Pokud vládní orgány budou chtít služeb cloudu využívat, bude nutné změnit předpisy o veřejných zakázkách.

Agentura General Services Administration v USA se snaží koncepci cloud computingu prosadit, aby mohla snížit spotřebu energie svými počítači. Společnosti Hewlett-Packard a Intel vytvořily studii, která ukazuje, že americká federální vláda utrácí každý rok za energii na provoz svých počítačů 480 milionů USD.

Agentura GSA v praxi spolupracuje s dodavatelem na vývoji aplikace, která spočítá, kolik energie vládní agentury konzumují.

Tato snaha je sice odpovědná a ekologicky příznivá (nehledě na každoroční úsporu milionů dolarů pro daňové poplatníky), ale vládní organizace se možná v dohledné době na služby cloudu spoléhat nebudou. Opět je nutné vyřešit otázky soukromí dat a jejich vlastnictví.

Použití řešení cloud computingu má své klady i zápory. Vaše organizace je jedinečná a neexistuje jediná správná odpověď na otázku, zda má či nemá cloud využívat. Zvažte však firemní potřeby a porovnejte výhody a nevýhody, jaké by byly s přechodem do cloudu v současnosti spojeny.

V další kapitole si povíme o některých klíčových hráčích v oboru cloud computingu a podrobněji se podíváme na to, co mohou nabídnout.