

AVG® V PRÁCI

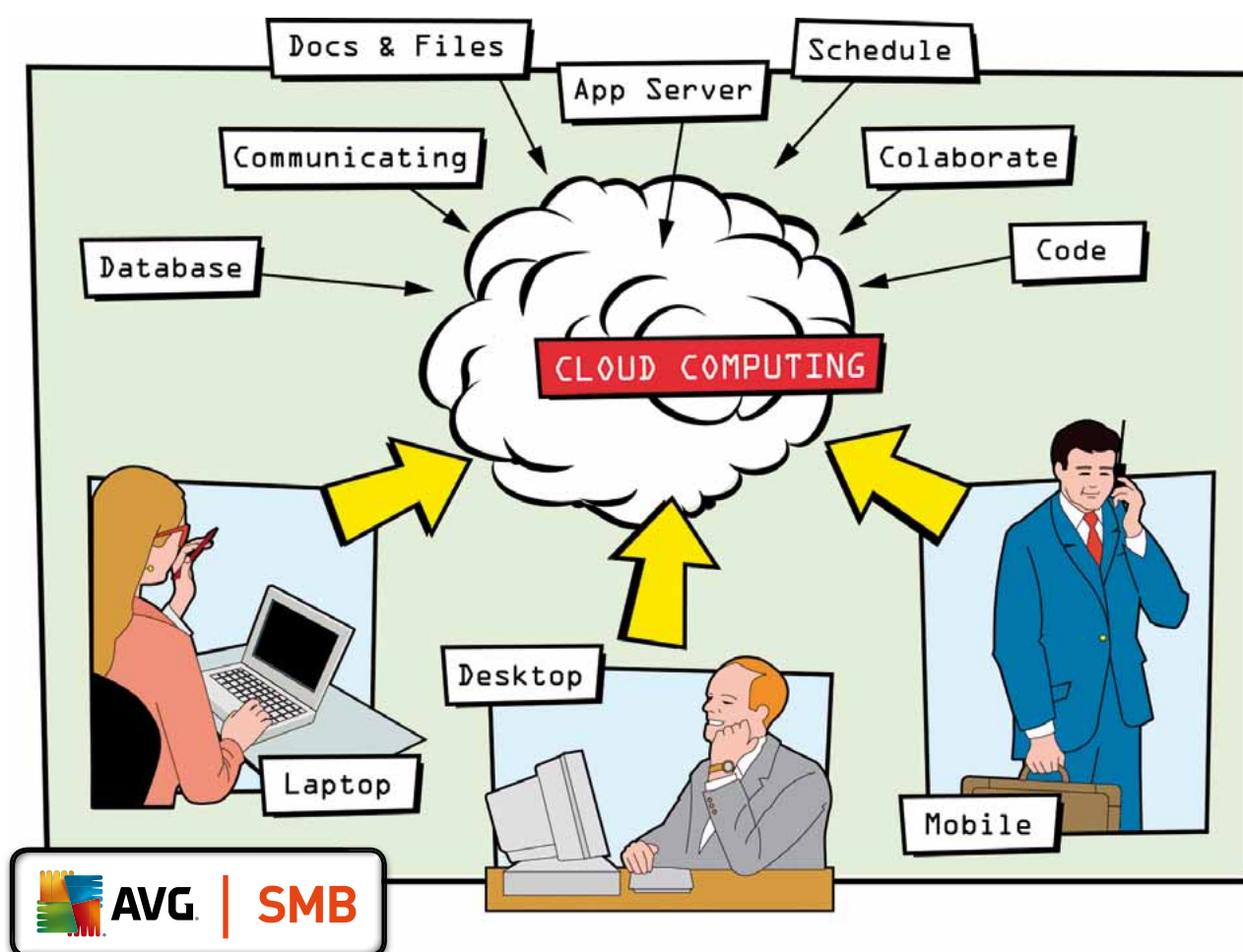
Small Business Průvodci zabezpečením

Zabezpečení a cloud computing:
Budování důvěry u nových metod
poskytování dat

Možnosti cloud computingu mohou od základu změnit způsob, jak se podniky dívají na nové aplikace a výpočetní sílu, ale přinášejí také nové bezpečnostní hrozby.

Cloud computing je v širokých odborných kruzích již nějakou dobu považován za technologii s ohromnou budoucností. Současně se však vyskytl problém, jak tuto technologii správně definovat.

Pokud prohlásím, že služba „Hotmail“ je dobrým příkladem cloud computingu, bude to dostačující definice? Koncepce této technologie je zcela jednoduchá: Uživatel se prostřednictvím internetu připojí k datovému centru a získá přístup ke službě online, jako je např. právě služba Hotmail.



Ted' pojďme na tuto definici navázat tak, aby i nadále zůstala jednoduchá. Vzhledem k tomu, že dnešní využití webu je mnohem sofistikovanější a samotné weby se staly mnohem dynamičtější, došlo ke změně definice služeb online.

Kdysi jsme web používali pouze k hledání informací. Nyní s webem vzájemně komunikujeme, protože se z jeho služeb staly aplikace. Tyto služby nyní vykonávají funkce počítačů, a to stejným způsobem, jakým tak činí samotné počítače.

Víte, že:

- ✓ **Cloud computing se potýká se stejnými bezpečnostními problémy jako jiné technické služby. Kvůli své abstraktnosti se však musí potýkat i s dalšími obtížemi.**
- ✓ **Pokud je cloud computing správně navržen a nasazen, dokáže uživatelům poskytovat škálovanější výpočetní výkon.**
- ✓ **Model Cloud Cube významné bezpečnostní asociace The Jericho Forum popisuje kroky, které by společnosti měly učinit, než cloudové služby adoptují.**
- ✓ **AVG LinkScanner[®], technologie pro bezpečné vyhledávání a surfování (<http://linkscanner.avg.com/>), dokáže u každé webové stránky aplikovat více než 100 různých detekcí potenciálních hrozeb.**

Výpočetní výkon cloud computingu vzniká v centralizovaném datovém centru a je poskytován jednotlivým uživatelům nebo na agregované úrovni celým společenstvem. Pro tuto podnikovou úroveň počítačových služeb se používá pojem Software-as-a-Service (software jako služba) nebo SaaS.

Cloud computing bez důvěry je jako tápání ve tmě

Pokud je cloud computing poskytován (a hlavně také nasazen) inteligentním způsobem, stává se z něj výkonný pomocník s potenciálem pro skutečné úspory nákladů díky sdílení hardwaru a softwaru, který používá. Navíc je třeba se zmínit o účinnosti a flexibilitě cloud computingu v případě zvyšování či snižování nároků na informační technologie. Je jasné, že cloud computing hraje v dnešních datových centrech zcela nezanedbatelnou roli.

Je však důležité si uvědomit, že cloud computing vyžaduje důvěru v poskytovatele služby, který provozuje datové centrum. A bez důvěry nelze zajistit zabezpečení.

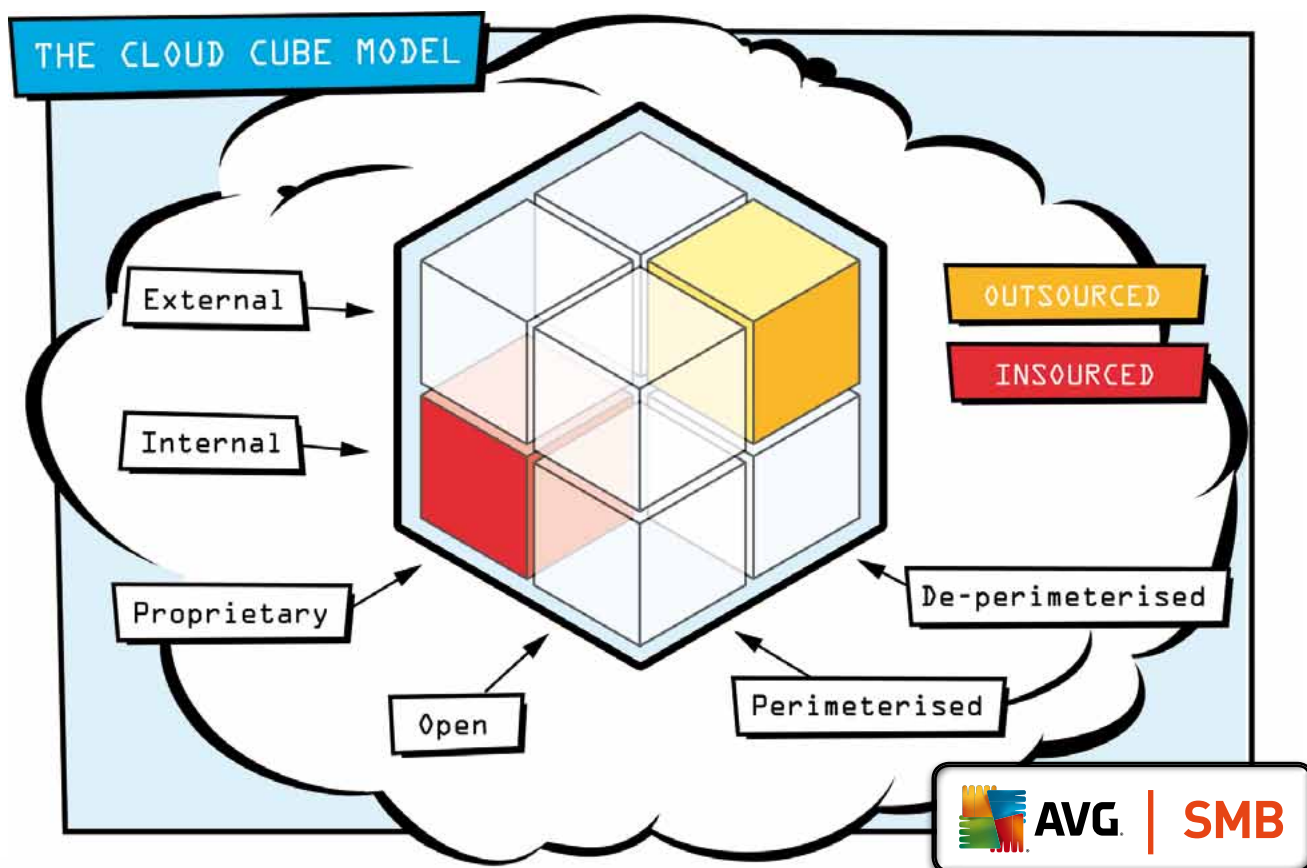
Co s tím tedy uděláme? Dalo by se říct, že technologie cloud computingu je teprve ve fázi svého dospívání. Proto je třeba analyzovat, jak velké množství dat váš podnik svěří externímu poskytovateli výpočetního výkonu.

Bezpečnostní guru Bruce Schneier doporučuje provést podrobnou analýzu problémů se zabezpečením, které se týkají přesunu prostředků do prostředí cloud. „Zabezpečení informačních technologií je o důvěře. Musíte důvěřovat výrobci svého procesoru, hardwaru, operačnímu systému, dodavatelům softwaru a také poskytovateli internetových služeb,“ uvádí Schneier na svém blogu (<http://www.schneier.com/essay-274.html>) „Cokoli z tohoto výčtu může narušit vaše zabezpečení: uvést systémy mimo provoz, poškodit data nebo umožnit útočníkovi přístup do sítě.“

„Pokud se počítač nachází ve vaší síti, můžete jej chránit pomocí ostatních bezpečnostních systémů, jako jsou brány firewall nebo systémy detekce narušení (IDS). Můžete si vybudovat odolný systém, který funguje, i když vaši dodavatelé, kterým musíte důvěřovat, nejsou natolik důvěryhodní, jak byste chtěli,“ tvrdí Schneier. „S outsourcingovým modelem, ať už se jedná o cloud computing nebo jiné řešení, tohle nemůžete. Poskytovateli této služby musíte naprosto důvěřovat. Musíte věřit nejen zabezpečení poskytovatele služeb, ale také jeho spolehlivosti, dostupnosti a stabilitě.“

Jak začít používat prostředí cloud?

Asociace Jericho Forum vytvořila sérii strategií, které by podle ní měly společnosti adoptovat při jednáních s poskytovateli služeb cloud computingu. Všechny tyto strategie popisuje její model Cloud Cube (www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf) zabývající se klíčovými faktory, které by měly společnosti před uzavřením smlouvy s dodavatelem nebo poskytovatelem služeb zvážit.



Adrian Secombe, člen výkonné rady asociace Jericho Forum a výkonný ředitel pro zabezpečení informačních technologií společnosti Eli Lilly, prohlásil: „Využití cloud computingu k organizaci práce může být bezpečnější a efektivnější než starší postupy, které využívaly vlastních technologií.“

Pokud se však na něj podíváme z jiného úhlu pohledu, otevírá se nám Pandořina skříňka plná bezpečnostních hrozeb – a to nejsou jen hrozby týkající se utajení a integrity dat.

Pečlivě analyzovaný a vybraný přístup k implementaci cloud computingu dokáže tyto bezpečnostní problémy udržet na uzdě," tvrdí Secombe. „Každý podnik si musí vybudovat ty správné základy pro vývoj cloudového modelu – takového, který umožní pozitivní využití, sníží náklady a odstraní rizika.“

Kromě potenciálních problémů souvisejících s migrací e-mailu na hosting u poskytovatele spravovaných služeb se nezdá, že by existovaly nějaké specifické bezpečnostní hrozby ze strany samotných aplikací online.

Aktualizovaný antivirový software, jako je AVG Anti-Virus Business Edition 2011 (<http://www.avg.com/gb-en/product-avg-anti-virus-business-edition>), však dokáže poskytovat neocenitelnou ochranu pro všechny vaše důležité systémy.

Software LinkScanner® (<http://linkscanner.avg.com/>) od společnosti AVG pomáhá při obraně před webovými útoky, které by potenciálně mohly být integrovány v cloudových aplikacích a souvisejících webových stránkách. Dle společnosti AVG používá software LinkScanner® cloudovou databázi, která hodnotí, zda určitý web neobsahuje zlomyslný kód.

„LinkScanner® dokáže u každé webové stránky aplikovat více než 100 různých detekcí potenciálních hrozeb," uvádí společnost. „Pokud jsou výsledky neprůkazné, provede nástroj LinkScanner® pomocí modelu cloud kontrolu velkého počtu phishingových kanálů spojených s výzkumnou sítí společnosti AVG a podle výsledků poskytne konečné vyhodnocení možné hrozby.“ Ačkoli cloud computing není tak úplně tím, za co jej mají mnohé reklamy, dá se logicky považovat za novou generaci vývoje výpočetních technologií. S jistotou lze tvrdit, že většina podniků dříve či později adoptuje některé z charakteristik tohoto modelu – zejména pokud se prokáže jako úspornější a flexibilnější.

Je nevyhnutelné důvěřovat všem poskytovatelům cloudových služeb. Společnosti ale mohou podniknout některé kroky, kterými lze možná rizika zmírnit. Mezi ně patří implementace vyšší úrovně modelů nebo způsobů využití již prověřeného zabezpečení přístupu k internetu a hardwaru.

Co je třeba

- ✓ Před uzavřením smlouvy s dodavatelem nebo poskytovatelem internetových služeb si přečtěte informace o modelu Cloud Cube pro cloud computing od asociace Jericho Forum.
- ✓ Proveďte analýzu, jak velké množství dat bude umístěno v externích počítačích a jak velké riziko z toho pro váš podnik hrozí.
- ✓ Používejte aktualizovaný antivirový software, jako je AVG Anti-Virus Business Edition 2011 (<http://www.avg.com/gb-en/product-avg-anti-virus-business-edition>), k ochraně důležitých podnikových systémů.



Skupinu AVG SMB
najdete na adrese:
bit.ly/AVGSMB



Staňte se fanouškem
společnosti AVG na adrese:
facebook.com/avgfree



Přečtěte si naše blogy
na adrese:
blogs.avg.com



Sledujte nás na adrese:
twitter.com/officialAVGnews



Staňte se partnerem
společnosti AVG
na adrese:
avg.com/gb-en/affiliate



Sledujte náš videokanál
na adrese:
[youtube.com/user/
officialAVG](http://youtube.com/user/officialAVG)

AVG Technologies CZ, s.r.o.
Holandská 4, 639 00 Brno
Česká republika
www.avg.cz

AVG Technologies USA, Inc.
1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
USA
[www.avg.com/us-en/
homepage](http://www.avg.com/us-en/homepage)

AVG Technologies UK, Ltd.
Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
Velká Británie
www.avg.co.uk

AVG Technologies GER GmbH
Bernhard-Wicki-Str. 7
80636 München
Německo
www.avg.de

AVG Technologies CY Ltd.
Arch. Makariou III.
2-4 Capital Centre
1505, Nicosia, Cyprus
Fax: +357 224 100 33
www.avg.com