Ľuboslav Lacko

Nejpoužívanější cloudové služby i pro začátečníky

Osobní cloud

Vhodné pro Windows, iOS a Android

pro domácí podnikání a malé firmy

Dropbox
SkyDrive
Box.net
iCloud
Dokumenty Google
Kalendář Google
Office 365
Office Web Apps

computer press

Ľuboslav Lacko

Osobní cloud pro domácí podnikání a malé firmy

Computer Press
Brno
2012

Osobní cloud pro domácí podnikání a malé firmy

Ľuboslav Lacko

Překlad: Martin Herodek
Obálka: Martin Sodomka
Odpovědný redaktor: Libor Pácl
Technický redaktor: Jiří Matoušek

Objednávky knih:
http://knihy.cpress.cz
www.albatrosmedia.cz
eshop@albatrosmedia.cz
bezplatná linka 800 555 513
ISBN 978-80-251-3744-4

Vydalo nakladatelství Computer Press v Brně roku 2012 ve společnosti Albatros Media a. s.
se sídlem Na Pankráci 30, Praha 4. Číslo publikace 16 156.

1. vydání

ALBATROS MEDIA a.s.

Obsah

KAPITOLA 2

Bezpečné a spolehlivé místo pro vaše soubory a dokumenty 33

KAPITOLA 3

Práce s dokumenty na webu 57

PŘÍLOHA

Úvod

V posledních letech ze všech stran skloňovaný pojem *cloud computing* by se mohl laikům zdát na první pohled spíše nehmotný, jako nějaké virtuální éterické IT prostředí, které poskytuje služby a o které se nemusíte starat. O výhodnosti cloudu pro firmy dnes už snad nikdo nepochybuje, tento fenomén ale v různých podobách proniká stále více i do IT agendy běžných domácích uživatelů, studentů a malých živnostníků. Obsahová náplň této publikace by se dala shrnout do jedné věty:

Co může cloud computing poskytnout vám osobně?

Cílem je zpřístupnit vám výhody cloudu, naučit vás umístit svoje dokumenty, osobní agendu, případně agendu malého podnikání (živnost, svobodné povolání) na web, abyste s nimi mohli pohodlně a bezpečně pracovat kdekoliv, kdykoliv a z jakéhokoliv zařízení.

Co je cloud

Cloud, nebo po našem oblak, je určitou metaforou pro komplexní síťové prostředí. Tento termín se vžil pro informační technologie na pozadí, tedy Internet. Cloud computing v jiném, trochu humornějším pojetí znamená použití výpočetních technologií za hranicemi domácí či podnikové sítě, tedy tam, kde je to pro uživatele „v oblacích". Podle jedné z definic *Cloud computing je metoda poskytování IT ve formě služby, přičemž zákazník platí jen za to, co právě využívá.*

Podle definice analytické společnosti Gartner představuje cloud computing *způsob zabezpečení výpočetních zdrojů, kde jsou masivně škálovatelné IT prostředky poskytované více externím zákazníkům prostřednictvím internetových technologií jako služba.*

Jiná definice rozumí pod pojmem cloud computingu *IT zdroje a služby plně automatizované a abstrahované od infrastruktury, prostřednictvím které jsou poskytovány. Navíc musí být poskytované „na požádání" a ve sdíleném prostředí, dostatečně škálovatelném a flexibilním.*

Cloud computing představuje nastupující trend, který je podobně jako například Web 2.0 založen na už existujících a ověřených technologiích. Měl by zpřístupňovat každý element IT infrastruktury jako službu na vyžádání: operační systémy, aplikace, úložiště, servery, zařízení a správu obchodních procesů. Cloud computing je vyvrcholením trendu využívání aplikací bez toho, abyste museli mít cokoliv nainstalované na svém počítači.

Výhody jsou zřejmé. K aplikacím, službám a údajům můžete přistupovat odkudkoliv, kdykoliv a prakticky z libovolného klientského prostředí, širokou paletu mobilních zařízení nevynímaje. Netřeba nic investovat, netřeba nic spravovat. Koncoví uživatelé jen „konzumují" požadovanou funkcionalitu, nepotřebují tedy znát žádné technické detaily, co se děje „za oponou".

Vzorem pro cloud jsou utilitní služby

Lepšímu pochopení současných trendů neuškodí krátký pohled do minulosti. Ideovým průkopníkem takzvaného utilitního modelu byl John McCarthy v 60. letech minulého století. Principem utilitního modelu je poskytovat výpočetní zdroje podobně jako ostatní utilitní zdroje, například elektrickou energii, plyn nebo vodu, přičemž uživatel platí pouze za to, co spotřebuje.

Zákazník v domácnosti si vůbec neuvědomuje, kde se elektrická energie, kterou využívá, vyrábí, jak se k němu distribuuje... Jednoduše, pokud si připojí do elektrické sítě další zařízení, očekává, že bude mít k dispozici dostatek elektrické energie na jeho provoz. Navíc automaticky předpokládá, že zaplatí jen a pouze přesnou hodnotu spotřebované energie. Stejná úroveň škálovatelnosti a flexibility ve zpoplatňování se očekává i od služeb cloud computingu.

Uživatel, který přistupuje k elektronické poště přes webové rozhraní nebo pracuje s dokumenty prostřednictvím cloudových služeb, nemusí mít žádné znalosti o cloudu, a už vůbec ne kontrolu nad jeho infrastrukturou. Cloud je velmi komplexní, ale vůči uživateli se tváří jako černá skříňka. Proto mu stačí umět ovládat jednoduché a intuitivní uživatelské rozhraní.

Neomezená kapacita na vyžádání

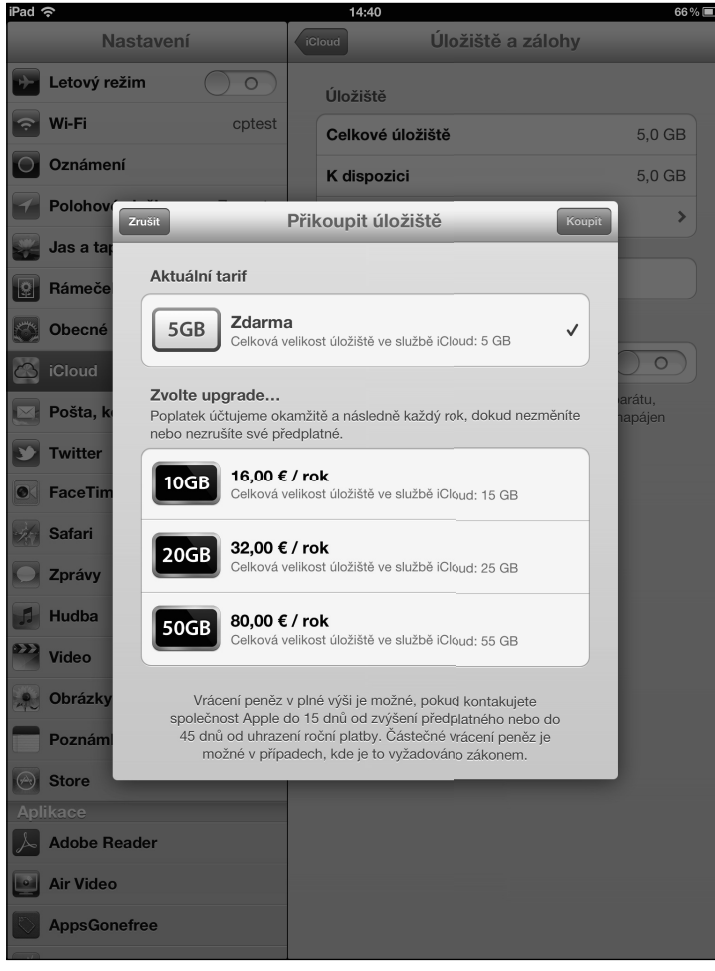
Základním atributem všech služeb cloud computingu by měla být schopnost poskytovat je „na vyžádání" ve formě a objemu, které jsou adekvátní okamžitému požadavku zákazníka. Proto se poskytovatelé řízených cloudových služeb většinou snaží zabezpečit automatizované zřizování prostřednictvím tzv. samoobslužných portálů bez potřeby komplikované komunikace se zákaznickým centrem.

Tuto možnost oceníte při samoobslužném zřizování úložného prostoru na webu (SkyDrive, úložiště Google, Box.net, Dropbox, iCloud...) či konta pro práci s dokumenty. Pravděpodobně nejatraktivnějšími vlastnostmi služeb cloud computingu je jejich škálovatelnost a flexibilnost. Máte možnost kdykoliv si alokovat dodatečnou úložnou kapacitu, případně výpočetní zdroje, podle aktuální potřeby a v potřebném objemu a později je stejně flexibilně opět vrátit.

Cloud vám v případě potřeby umožní koupit si samoobslužně dodatečnou úložnou kapacitu v cloudu přímo z klientského zařízení. Na obrázku U.1 je příklad uživatelského rozhraní pro dokoupení úložné kapacity v iCloudu přímo z tabletu iPad.

Nejen v podnikovém prostředí, ale i v malém byznysu, živnosti, svobodných povoláních a zájmových sdruženích se některé úlohy, které jsou závislé na podpoře informačních technologií, shlukují sezónně nebo se váží na stanovený termín dokončení – například přihlašování na sběratelskou výstavu či společenskou událost, případně webová kampaň pro příslušnou událost.

Pokud by se pro takovýto účel zřídila přiměřeně dimenzovaná hardwarová a softwarová infrastruktura, bylo by to investičně náročné, a navíc většinu času by se tato infrastruktura využívala jen velmi omezeně. Naplno by se využila pouze na jistý, relativně krátký časový úsek. Navíc třeba v případě úspěšné webové kampaně by kapacita serveru nemusela stačit a muselo by se to řešit. Pružnost cloud computingu umožňuje pronajmout si dostatečnou kapacitu na potřebný čas.



Obrázek U.1: Příklad dialogu dokoupení úložného prostoru v cloudu

Naplněním vizí cloud computingu je maximálně spolehlivá IT infrastruktura, která by z pohledu uživatele byla stejně jednoduchá jako sítě dodávající elektřinu, vodu nebo plyn. Stačí si službu objednat a používat ji v takovém rozsahu, v jakém potřebujete. Když službu nepoužíváte, nic neplatíte. Služba je spolehlivá, vysoce kvalitní a cenově nenákladná.

Pokusme se více rozvinout analogii s elektřinou z úvodu publikace. Elektrárny jsou ekvivalentem datových center, v kterých je umístěna infrastruktura. Energetické koncerny jsou poskytovateli služby. Analogický je i způsob fakturace za poskytnuté služby. Využívání cloudových služeb je ekvivalentem spotřeby elektrické energie. Dostupnost cloudu přes Internet a jednoduchost připojení je ekvivalentem dostupnosti elektrické energie přes zásuvky.

V předcházející části se několikrát zmiňovala fakturace a placení za cloudové služby. To platí v plném rozsahu jen pro komerční služby poskytované pro podnikovou sféru. Pro osobní nekomerční využití je většina cloudových služeb zdarma.

Průkopníkem trendu služeb poskytovaných přes web byl mailhosting. Prakticky každý uživatel počítače už má dávno vytvořené na webu nějaké e-mailové konto (gmail, hotmail, post...). V době, kdy jste si tato konta vytvářeli, jste určitě ani netušili, že tato oblast bude jednou pojata jako jedna z cloudových služeb.

Tyto služby poskytují nejen několik gigabajtů prostoru pro archivaci vaší elektronické pošty, ale i sofistikovanou ochranu před nevyžádanou poštou. V mnoha případech se právě tato mailhostingová sídla, na která bylo z minulosti navázáno velké množství zákazníků, stala po doplnění o další funkce, například úložiště, webový kancelářský balík či poskytování virtuálních strojů, základními pilíři současných cloudových produktů.

Výhody a nevýhody cloud computingu

Je nesporné, že cloud computing začali prosazovat giganti IT průmyslu. Proč? IT paradoxně právě svým rychlým vývojem začalo směřovat do slepé uličky (určitá analogie krize z nadvýroby). Vize osobního počítače pro každého se prakticky naplnila, počítače v podnicích vytlačily mainframe a k nim připojené terminály a mohlo by se zdát, že trh s hardwarem začne saturovat.

Proto se intenzivně hledaly cesty, jak na trh umístit další a další infrastrukturu. Kam? Nejprve servery do podniků. Vývoj jde po spirále, a tak bylo třeba v podnikových serverovnách nahradit sálové počítače. Záměr se podařil, ale co dále? Na pracovních stolech už počítače jsou, podnikové serverovny jsou infrastrukturou přeplněné, a tak na schématech IT architektury začal být stále zajímavější obrázek obláčku (anglicky cloud), což je zpravidla symbol pro Internet.

A tak se na IT konferencích začaly probírat názory, že serverová infrastruktura v podnicích je neefektivní, váže kapacity IT oddělení, servery (které zákazník nedávno za drahé peníze nakoupil) nejsou dost „green", a tak by bylo nejlepší, kdyby firmy začaly konzumovat IT jako službu. Služby by samozřejmě poskytovali už zmínění giganti IT průmyslu.

Výhody cloud computingu

- **Rychlé nasazení** – cloud přináší koncepci centralizované platformy, která je kdykoliv připravená k použití, stačí si službu samoobslužně zřídit.
- **Vysoká flexibilita** – přístupové zdroje mají virtuální charakter, výsledný potenciál cloudu není limitován výkonností a kapacitou lokálních nebo vzdálených počítačů.
- **Sdílení zdrojů** – sdílení hardwarových prostředků umožňuje lépe distribuovat výkon mezi jednotlivé uživatele.
- **Eliminace nákladů na správu a údržbu** – eliminuje podstatnou část aktivit spojených s údržbou jako projektování, výběr softwarových a hardwarových platforem, prostorů i personálu.
- **Úspory v oblasti spotřeby energie** – lepší využívání elektrické energie eliminací plýtvání.

Nevýhody cloud computingu

Jako všechno na této planetě i cloud computing má svoje nevýhody. Většina uvedených nevýhod je relevantní pro podnikové použití. To, co se v podnikovém prostředí může jevit jako nevýhoda, pro osobní použití, případně pro malý byznys, může být dokonce výhoda. Typickým příkladem je:

Nevýhoda: nemůžeme ovlivnit = Výhoda: nemusíme se o to starat

- **Závislost na poskytovateli** – zákazník využívající cloud ztrácí možnost rozhodovat, který software a kterou verzi používat. Uživatelé musí počítat i s možností, že poskytovatel může zdražit ceny služeb, to se pro nekomerční použití většinou týká dokupování úložné kapacity, a dokonce i s krajní možností, že poskytovatel může zkrachovat. To je důvod, proč v publikaci popisujeme cloudové služby etablovaných společností, jako jsou Google či Microsoft, kde je pravděpodobnost zrušení poskytování služeb nepatrná. Navíc, protože je většina služeb poskytovaná pro osobní a nekomerční použití zdarma, doporučujeme umístit svoje dokumenty do cloudových úložišť více poskytovatelů.
- **Nedůvěra** – cloud computing je relativně nový pojem v IT. Zatím neexistují dlouhodobá a spolehlivá doporučení ohledně používání technologie cloudu. A i samotné používání přes Internet vyvolává hodně otázek ohledně bezpečnosti dat. Na druhé straně jsou tu dlouhodobé zkušenosti se službami, které se poskytovaly přes web jako služba, například mailhostingem, ještě předtím, než se pojem cloud etabloval.
- **Méně funkcí a horší komfort uživatelského rozhraní** – cloudové řešení většinou poskytuje méně funkcí v porovnání s desktopovým. Samozřejmě to není způsobeno možnostmi serverů v datových centrech, ty jsou prakticky neomezené, ale omezeními vyplývajícími s protokolu HTTP, který je základním pilířem webu. Tato omezení jsou dnes do značné míry překonaná pomocí technologií AJAX, Flash, Silverlight.
- **Menší stabilita** – ani tato výhrada se netýká datových center a technologií v nich instalovaných, spíše naopak. Datová centra momentálně představují to nejspolehlivější, co si v IT dokážeme představit. Problém je v připojení. Software, ke kterému přistupujete online, může občas fungovat pomaleji, nebo vůbec, v případě, že selže internetové připojení,
- **Legislativní problémy** – tyto problémy vyplývají z toho, že poskytovatel a konzument služby sídlí v různých zemích s různými právními normami. Například společnosti sídlící v USA nebo poskytující služby z USA jsou povinny podstoupit data klienta vládě, což může představovat pro zákazníky mimo USA problém. Podobně je to s povinností ochrany osobních údajů. Lékař, který si chce uložit svou agendu i do cloudu, musí s tímto aspektem počítat.

Polemik ohledně cloud computingu přibývá, a to ve více rovinách, včetně té lingvistické. Jak tento fenomén začlenit do českého či slovenského spisovného jazyka? V slovenštině si už našly pevné místo zdomácnělé výrazy typu „hardvér" či „softvér". Používat původní anglický pojem, nebo jeho zdomácnělou podobu? A pokud zdomácnělou podobu, tak jakou? Ve slovenštině se neoficiálně, ba až slangově, používají pojmy jako „internetové počítanie", „obláčik", „oblak počítačov", „výpočtové mračno". V češtině převládá použití originální terminologie, tedy cloud.

KAPITOLA 1

Osobní digitální agenda

V této kapitole se dozvíte:

- Potenciální problémy dokumentů na lokálním počítači
- Umístění digitální agendy a dokumentů do cloudu
- Stabilní aplikační a úložné prostředí
- Optimální rozdělení agendy mezi lokálním počítačem a cloudem
- Prevence ztráty dokumentů při ztrátě, krádeži či poškození počítače
- Jak fungovat v nouzovém režimu po ztrátě či krádeži počítače
- Přestěhování agendy na nový počítač nebo novou platformu

Potenciální problémy dokumentů na lokálním počítači

Snad nejznámější zkratka v oblasti informačních technologií – PC – znamená osobní počítač. Přívlastek osobní ve většině případů znamená, že ho využívá jeden uživatel, ať už v osobním životě, nebo při práci. Přitom v poslední době dochází ke stále většímu průniku těchto oblastí, takže slovní spojení „při práci" už není ekvivalentem výrazu „na pracovišti". Na jedné straně si lidé nosí práci domů, případně z domu přímo pracují a na druhé straně v mnoha případech pracovníci, hlavně v oblasti marketingu, využívají při práci svoje kontakty a vazby na sociálních sítích.

K nejčastějším činnostem, kterým se uživatel počítače věnuje, patří práce s dokumenty. K dispozici je mnoho komplexních aplikací, souhrnně nazývaných kancelářské balíky, které umožňují pracovat s dokumenty rychle a efektivně. V současnosti se ve většině případů stále jedná

o aplikace, které běží pouze na lokálním počítači. Logickým důsledkem je, že na lokálním počítači jsou potom uložené i dokumenty se všemi výhodami a nevýhodami, které z toho vyplývají.

Zamyslete se nad způsobem, jak pracujete se svým počítačem vy. Určitě jste si postupně vytvořili více či méně promyšlený systém složek nebo knihoven dokumentů, do kterých svoje dokumenty a multimediální soubory ukládáte. Ti zodpovědnější si práci zálohují na externích discích. Mnozí neustále synchronizují dokumenty mezi počítačem v práci a doma. Proč? Aby o svou práci a důležitá data nějakou nešťastnou náhodou nepřišli.

Externí USB média

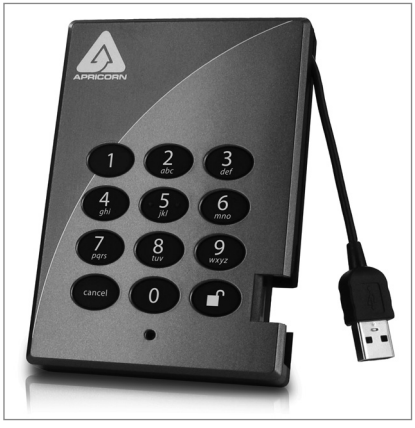
Z pohledu uživatele jsou přenosné datové nosiče, tedy USB klíče a disky, velmi užitečnou pomůckou, která může zvýšit flexibilitu přenosu údajů mezi různými, i vzájemně nekompatibilními, IT systémy. Pro IT odborníky, kteří si uvědomují širší souvislosti uvedené flexibility, jsou tato zařízení doslova postrachem. V případě nesprávného nastavení bezpečnostních politik mohou uživatelé na přenosné zařízení zkopírovat citlivé údaje, které se ocitnou mimo bezpečnou zónu firemního IT prostředí.

O tom, jak snadno lze flash disk někde zapomenout, ztratit či ukrást, nás přesvědčují i medializované případy z tak citlivých odvětví, jako je například obrana. Pokud přenosné paměťové médium nepoužívá heslo, a/nebo šifrování údajů, jsou citlivé údaje dostupné každému, kdo se datového nosiče zmocní. Každý si dokáže představit potenciálně negativní důsledky, například poškození dobrého jména firmy, ztráta image, ztráta obchodní příležitosti či únik chráněného firemního know-how.

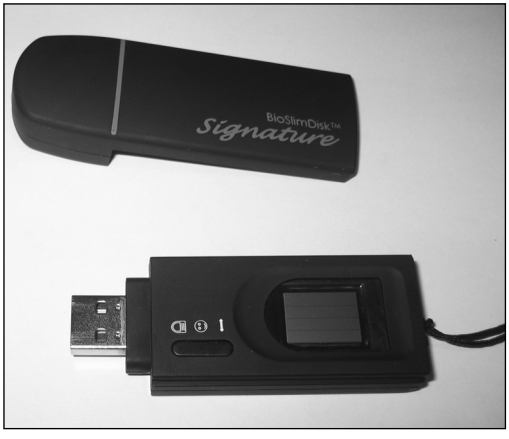
Flash disky a externí USB disky využívají na ochranu údajů identifikační mechanizmy, klasickou ochranu přístupu pomocí hesla, případně v kombinaci se šifrováním. Vysvětlíme rozdíl. Pokud disk využívá jen identifikační mechanizmus, po připojení k počítači vyžaduje přístupové heslo nebo sejmutí otisku prstu. Údaje na disku jsou však uložené běžným způsobem, tedy v nezašifrované podobě. Teoreticky stačí obejít vestavěnou elektroniku, vyjmout disk a připojit ho k počítači kabelem přímo. Určitou ochranu poskytuje nerozebíratelné zalití disku a základní desky do plastového pouzdra, takže se přístroj nedá běžným způsobem rozebrat, pro specialisty to však velký problém nepředstavuje.

Nejbezpečnější ochranou před potenciálním zneužitím údajů je dostatečně silné šifrování celého USB disku v souladu s centrálně řízenou bezpečnostní politikou. Tyto disky mohou používat pouze oprávněné osoby. Pro podnikové nasazení jsou vhodné flash disky a disky s hardwarovou podporou šifrování, kdy je celý kryptografický proces v režii zařízení. Šifrování může být kombinované s autentizací pomocí otisku prstu a hesla, nebo dokonce vzdáleným řízením přístupu k údajům na externím médiu. V některých případech se vyžaduje, aby řešení využívající externí média bylo certifikované, například na práci s utajovanými daty pro různé stupně utajení.

Šifrování je standardní vlastností některých USB klíčů, takže v dobře nakonfigurovaných systémech napříč tomu, že uživatel nic neaktivoval, disk automaticky šifruje data při zápisu.



Obrázek 1.1: Autentizace přístupu k údajům na disku pomocí kódu



Obrázek 1.2: Flash disk s biometrickou autentizací

Poznámka: Šifrování na externích médiích musí chránit i vymazané údaje, protože tato data se dají přečíst pomocí specializovaných nástrojů na obnovu údajů.

Se šifrováním však souvisí i některé komplikace, například určitá časová režie šifrování, která však podle našich zkušeností při běžném používání v byznysu, tedy ne při multimediálním provozu, nepůsobí rušivě. Faktor časové režie šifrování však trochu vystoupí do popředí při používání virtuálních počítačů, jejichž obrazy jsou uložené na externích médiích. Mnoho firem takto zakonzervuje operační prostředí pro systémy, které dodal zákazník a u kterých se v budoucnosti předpokládá jejich podpora nebo úpravy. V takovýchto případech doporučujeme nejprve překopírovat obrazy virtuálních disků do počítače.

Druhým problémem je nemožnost obnovy údajů ze šifrovaných disků. Někteří nezodpovědní uživatelé mají na flash discích důležité údaje, protože je s oblibou používají na přenášení

práce nebo na běžné zálohování. Flash disky však mají omezený počet zápisů, konzistentnost údajů se může narušit při odpojování paměťového média od počítače během zápisu, častou příčinou poškození je i mechanické rozlomení náhodným zakopnutím, pokud jste USB klíč zasunuli do počítače pod pracovním stolem.

V případě poškození šifrovaného disku nastává problém se záchranou důležitých dat. Šifrované soubory se běžnými metodami obnovit nedají. Někdy mohou pomoct specializované firmy. Příkladem je společnost DATARECOVERY, které se vlastním výzkumem podařilo prolomit vnitřní šifrování některých typů flash disků.

Dilema klasického zálohování na externí USB disky a klíče

Na rozdíl od bezpečného IT prostředí ve firmách spravovaného kvalifikovanými administrátory je váš osobní počítač vystaven různým hrozbám a rizikům.

Totéž platí pro záložní média, tedy externí disky a USB klíče. Jak je správně používat? Kam je umístit? Jednoznačná odpověď neexistuje. Pokud necháte záložní médium doma, ochránili jste svoje dokumenty pro případ potenciální krádeže notebooku. Pokud se vám ale notebook na důležité, například zahraniční, pracovní cestě pokazí, máte problém, protože si sice můžete koupit nový, ale nemáte odkud v něm obnovit dokumenty, které na pracovní cestě právě potřebujete.

Pokud máte záložní médium s sebou, není problém, abyste se po příslušné finanční investici do opravy nebo nákupu nového počítače „zotavili" z poruchy. Pokud vám ukradnou aktovku, kde máte přenosný počítač i záložní USB disk, vaše dokumenty jsou ztracené. Vaší jedinou šancí je nabídnout odměnu za vrácení aspoň USB disku nebo se spolehnout na efektivnost práce policie. Sami dokážete odhadnout, že pravděpodobnost úspěchu je v takovém případě menší než nepatrná.

Jak tedy situaci s účinným zálohováním řešit? Zálohovat dokumenty na dvě přenosná média, přičemž jedno z nich, určené na zotavení pro případ krádeže, uložit na bezpečném místě, tedy doma nebo na pracovišti, a druhé, určené na zotavení po poruše přenosného počítače, nosit stále s sebou. Zdánlivě účinné řešení, jeho slabým místem je však složitost. Klidně se vám může stát, že například omylem přepíšete novější dokumenty staršími a podobně. Navíc zálohování neřeší všechna potenciální rizika, takže musíte ochránit počítače a externí disky před hrozbou, že škodlivý software poškodí dokumenty a soubory na infikovaném počítači, v horším případě i na externích médiích, které se k němu připojují.

Vývoj směruje k uzavřeným platformám

Paměťová USB zařízení a přenosné aplikace zvyšují produktivitu a pohodlí uživatele, ale též představují mnoho bezpečnostních rizik pro každou pracovní stanici s USB porty. Z hlediska bezpečnostních teorií je USB port jen jedním z potenciálních vstupních bodů pro únik informací a infiltraci škodlivého softwaru.

Vedle marketingové politiky je to jeden z důvodů, proč jsou mnohé moderní tablety a chytré telefony uzavřené, to znamená, že se k nim nedají připojit externí paměťová média, dokonce ani zasunout paměťové karty. Typickým případem je rodina produktů na bázi operačního systému Apple iOS, tedy iPad, iPod a iPhone, nebo mobilní platforma Microsoft Windows Phone 7. Údaje se na těchto platformách přenášejí jen v nezbytné míře, ve většině případů stačí zabezpečený online přístup k údajům ve firemních informačních systémech nebo použití nejperspektivnějšího přístupu k údajům bezpečně uloženým v cloudu.

Umístění digitální agendy a dokumentů do cloudu

Naznačené problémy elegantně a komplexně řeší cloud computing, který přináší okamžitou dostupnost dokumentů a výpočetní kapacity kdykoliv a odkudkoliv bezpečnost a ochranu dat před viry a jinými hrozbami. Pokud vám na klasickém počítači selže pevný disk, je vysoce pravděpodobné, že přijdete o všechna svoje data.

Na druhé straně pravděpodobnost, že by podobná situace nastala v cloudu, je téměř nulová. V datovém centru jsou všechny údaje zálohované, a navíc je možné díky virtualizaci úkol, případně celý virtuální počítač ze serveru, který má poruchu, okamžitě přesunout na jiný server, a to bez přerušení poskytování služeb, takže uživatel si to ani neuvědomí.

V případě ztráty nebo krádeže klientského zařízení, tedy notebooku či tabletu, se škoda dá vyčíslit jen hodnotou daného zařízení. Jeho majitel totiž nepřijde o žádné dokumenty ani údaje. Obnovení agendy uživatele po takovéto události, stejně jako po koupi novějšího, modernějšího zařízení, je prakticky okamžité, úplně odpadá potřeba migrace dat ze starého zařízení.

Stabilní aplikační a úložné prostředí

Umístění dokumentů do cloudu, tedy fyzicky do bezpečných a spolehlivých datových center, je důležitým milníkem jejich zabezpečení a zajištění jejich dostupnosti v jakékoliv situaci. Je to zpravidla první krok k využívání cloudových služeb. Ve většině případů (Dokumenty Google, Office Web Apps...) jsou součástí cloudového úložiště i aplikace umožňující práci s dokumenty a aplikace na správu personální agendy, tedy kalendářů, kontaktů, elektronické pošty a podobně.

Uživatel zpravidla poměrně rychle zjistí výhody takovéhoto přístupu. Odpadají starosti s instalací a aktualizací softwaru, aplikace jsou kdykoliv přístupné „na webu“ a o všechno se stará poskytovatel služby. Vždy tedy budete mít nejaktuálnější verzi využívaného softwaru bez toho, abyste za upgrade museli platit, stahovat ho nebo svépomocí instalovat.

Neocenitelnou výhodou cloudových služeb je nezávislost na konkrétním počítači. Pokud nastane potřeba fyzicky vyměnit počítač, ať už z důvodu poruchy nebo modernizace, vaše údaje

a aplikace zůstanou uložené v cloudu a jsou vám okamžitě k dispozici po přihlášení se z jakéhokoliv zařízení, kdekoliv se právě nacházíte.

Deklarovaná nezávislost na konkrétním zařízení přináší i dosud nebývalou operativnost. Pokud se vám například během kontroly důležitého dokumentu nebo v případě podnikání během prezentace zákazníkovi pokazí počítač, vypadne lokální metalická či bezdrátová síť, nemusíte čekat na odstranění poruchy, ale prakticky okamžitě můžete pokračovat v rozpracované aktivitě ze svého chytrého telefonu. Komfort práce samozřejmě může být nepatrně snížen, ale možnost pokračovat bude v mnoha případech neocenitelná.

Optimální rozdělení agendy mezi lokálním počítačem a cloudem

Při vyjmenovávání výhod cloudu jsme zatím považovali za samozřejmost trvalé a přiměřeně kvalitní internetové připojení. Co však v případě, když takovéto připojení není k dispozici? Touto úvahou jsme intuitivně odhalili největší nevýhodu cloud computingu. Na tomto omezení v reálné praxi zatím vždy skončí úvahy, že byste mohli v běžném životě vystačit s jednoduchým klientským zařízením, na kterém by nebyly žádné lokální dokumenty ani lokální aplikace na práci s nimi.

Tuto situaci dokonce neřeší ani tablet s GSM připojením. Sednete do letadla, potřebujete pracovat, například na poslední chvíli finalizovat dokumenty, ale nemůžete se připojit ke své cloudové službě. Uvedený příklad není ani zdaleka ojedinělý. I když máte u svého mobilního operátora předplacený neomezený objem přenášených dat, v zahraničí mohou být takovéto datové přenosy velmi drahé.

Řešením je zachování možnosti práce i v takzvaném odpojeném režimu. V takovém případě však musíte mít stažené aktuální verze dokumentů na vašem počítači, tabletu, či smartphonu a musíte mít k dispozici potřebné aplikace na prohlížení a editování dokumentů. Jak najít vhodný kompromis pro optimální rozdělení agendy mezi cloudové služby a lokální počítač?

Prevence ztráty dokumentů při ztrátě, krádeži či poškození počítače

Mobilita notebooků, tabletů a smartphonů má i své potenciální nevýhody. Tato zařízení jsou vděčným objektem pro zloděje všech kategorií, tedy domovní, hotelové, vlakové či kapesní. Námětem kapitoly není teorie kriminality, ale vyjmenované kategorie zlodějů velmi názorně naznačují, kde všude vám mohou váš přenosný počítač či jiné mobilní zařízení odcizit. Samotná krádež hardwaru však není to nejhorší, co vás může postihnout.

Ve většině případů je pro uživatele důležitější obsah jeho paměťových médií, hlavně dokumenty, publikace a vlastní tvorba jakéhokoliv druhu. Pokud zanedbáme ztrátu přístroje a soustředíme se jen na ztrátu údajů a dokumentů, může potenciální škoda nabýt dvou různých dimenzí:

- **Ztráta týkající se vlastní práce**
  Na tvorbě dokumentů jste určitě strávili desítky až stovky hodin, nemluvě o několikaměsíčním rozsahu práce na rozsáhlejších dílech, například při psaní knihy. Pokud nemáte dokumenty zálohované, vaše úsilí vyšlo vniveč se všemi důsledky, které z toho vyplývají, jako jsou například sankce za nedodržení termínu a podobně.
- **Ztráta citlivých údajů**
  Bez toho, abychom rozlišovali druh citlivých údajů, tedy osobní údaje, utajované skutečnosti, průmyslové či bankovní tajemství, je tento scénář nejhorší možný. Důsledkem je legislativní postih nebo možnost, že citlivé údaje, které představují know-how, získá konkurence.

Poznámka: Podle statistik je průměrně každou minutu ukraden nějaký přenosný počítač, případně tablet, a téměř polovina z nich obsahuje citlivá data, přičemž jen malé procento počítačů je vybaveno šifrováním nebo jinou sofistikovanou metodou ochrany údajů.

Možnosti prevence

I v případě, že máte svoje dokumenty a osobní agendu bezpečně zálohovaní v cloudu, určitě máte kopie některých dokumentů, na kterých aktuálně pracujete nebo je potřebujete i na svém přenosném počítači. Nejčastěji proto, abyste na nich mohli pracovat i v odpojeném režimu, kdy nemáte k dispozici připojení k Internetu, například v letadle. Ztráta nebo krádež notebooku v takovémto případě nebude znamenat ztrátu dokumentu, dokumenty na vašem nezabezpečeném počítači se ale mohou dostat do rukou nálezce či zloděje a tomu je potřeba zabránit.

Intel Anti-Theft

Pokud máte přenosný počítač s procesorem Intel, můžete využít technologii Intel Anti-Theft, která je integrovaná v procesorech od verze Intel Core vPro. Tato technologie na základě nastavení definovaných majitelem rozpoznává podezřelé chování, které by mohlo být způsobeno krádeží notebooku.

Může to být sledování počtu neúspěšných pokusů o přihlášení, změna BIOSu či opakované neúspěšné pokusy o připojení k bezpečnostnímu serveru. Pokud míra takovéhoto chování přesáhne nastavené limity, počítač se uzamkne na úrovni hardwaru (smažou se případné šifrovací klíče) a znemožní se přístup do operačního systému a k datům. Intel Anti-Theft umožní po zjištění ztráty nebo krádeže i uzamknutí „na dálku". Ve firmě stačí událost nahlásit zodpovědnému pracovníkovi IT oddělení, který notebook následně hardwarově uzamkne. Fyzicky se tak stane samozřejmě až při připojení počítače k Internetu.

Dobrou zprávou je, že pokud se notebook podaří získat zpět, je možné ho znovu uvést do původního stavu pomocí kódu, který má majitel uložený na bezpečném místě. Technologii Intel Anti-Theft je možné používat samostatně nebo prostřednictvím nadstaveb, které nad ní vytvořili výrobci notebooků. Například HP nabízí funkci LoJack, která umožňuje vystopování ukradeného notebooku prostřednictvím GPS. Technologie Computrace od společnosti Dell umožňuje vzdálené vymazání údajů.

Zabezpečovací hardwarový modul TPM

Modul TPM (Trusted Platform Module) bývá vestavěný v některých novějších počítačích. Jeho jádrem je mikročip, který umožňuje počítači využívat rozšířené funkce zabezpečení, jako je například šifrování jednotek BitLocker. Počítač s modulem TPM může vytvořit šifrovací klíče, které může dešifrovat jen stejný modul TPM. Modul „zabalí" šifrovací klíče pomocí vlastního ukládacího kořenového klíče, který je uložen přímo v modulu. Uložení ukládacího kořenového klíče na mikročipu TPM nikoliv na pevném disku nabízí lepší ochranu před útoky s cílem odhalit šifrovací klíče.

Při spuštění počítače s aktivovaným modulem TPM a šifrováním BitLocker zkontroluje modul TPM operační systém, aby zjistil, zda obsahuje místa, která by mohla představovat bezpečnostní riziko. Mezi takovéto okolnosti patří chyby disku, změny v BIOSu, případně indikace, že pevný disk byl odstraněn z jednoho počítače a spouští se v jiném. Pokud modul TPM zjistí některé ze zmíněných rizik zabezpečení, funkce BitLocker zamkne systémovou oblast, která se odemkne až po zadání hesla.

V porovnání s klasickým softwarovým šifrováním je modul TPM mnohem bezpečnější, protože odbourává i šifrování v operační paměti, která je přístupná například trojským koňům. TPM vám notebook nenajde ani nevrátí, v případě ochrany dat jde ale o zajímavé řešení.

Ochrana pomocí biometrických snímačů

Bezpečným způsobem pro zabezpečení přenosných počítačů jsou i biometrické snímače, přičemž ve většině případů se jedná o autentizaci na principu snímání otisků prstů. Nejsofistikovanější snímače porovnávají na otisku až 80 bodů. Pro zajímavost: je to víc, než potřebuje justice v USA na odsouzení pachatele za vraždu. Každý bod má přidělený vektor a identifikaci typu okolí, například sbíhání nebo rozbíhání čar. Některé notebooky využívají při autentizaci vestavěnou kameru na identifikaci tváře. Ještě bezpečnější je tato metoda v kombinaci s modulem TPM. Takto zabezpečený notebook bude pro zloděje prakticky nepoužitelný.

Volně dostupné aplikace na ochranu a vypátrání počítačů

Komerční aplikace na ochranu přenosných počítačů, například Computrace na vypátrání ztraceného či ukradeného počítače, případně na vzdálené smazání dat, jsou určené pro střední a velké firmy. Pro běžného uživatele v našich končinách, kde je poměr ceny notebooku k průměrnému platu stále velmi vysoký, je ve většině případů prioritní získání zařízení. K tomuto účelu slouží například aplikace Prey (*http://preyproject.com/*), která vám poskytne poměrně