Data v péči

ČÍSLO 7 | SRPEN 2007 | MHM COMPUTER S. R. O.

TCO – zaklínadlo výběrových řízení

Co všechno se pod zkratkou TCO skrývá?

Pole nové generace

Disková pole TagmaStore USP V

E-maily potřebujete

Neriskujte jejich nedostupnost

Budování záložní lokality

Chraňte se před fatálním výpadkem

Podzim je prý vhodným obdobím…

Podzim je prý velmi vhodným obdobím k nákupu automobilu. Jistě vás proto bude zajímat, jak nejlépe vybrat ten správný vůz.
Kupující si musí předem stanovit maximální finanční limit (pořizovací cena auta, investice). Pak si stanoví základní parametry vozu – čili jak velké chce auto, jaký má mít motor (tedy jeho obsah, spotřebu a typ – „benzin/diesel“), velikost zavazadlového prostoru. Na základě těchto základních parametrů pak můžeme vybírat z několika typů různých výrobců. Do hry ale vstupují další kritéria. Ergonomie vozu, jeho základní výbava a možnosti výbavy doplňkové (jako např. ABS, počet airbagů, klimatizace, elektricky ovládaná okénka, vyhřívaná sedadla atd.). Tato jemnější kritéria zúží výběr natolik, že rozhodnutí může už už padnout. Většinou však nepadne. Zkušenější zájemce si začne klást další otázky – jaké jsou statistiky poruchovosti po jednotlivých letech provozu, jaká je spotřeba vozu (ve městě, mimo město a smíšená spotřeba), kolik stojí náhradní díly, kolik stojí pravidelná údržba, jaká je délka záruky a co vše je v záruce zahrnuto, kde je nejbližší autorizovaný servis, jak klesá cena vybraného typu s jeho stářím a jaká je prodejnost (budoucího) ojetého auta. Teprve až kupující dostane uspokojující odpovědi na výše uvedené (a další) otázky, je připraven si auto koupit.

Z hlediska ekonomického tedy téměř každý, kdo „dbá o svou kapsu“, počítá, kolik ho ten „zatracený krám“ (nebo „rodinný miláček“) bude stát. Kalkuluje, za kolik si ho koupí, kolik ho bude stát provoz, kolik standardní servis, kolik havarijní opravy, pojištění (povinné ručení i havarijní) atd. Tedy nejen kolik za něj zaplatí při koupi, ale kolik ho bude stát celkem. Hledá tedy celkové náklady (na) vlastnictví.

Podzim je prý vhodným obdobím k nákupu výpočetní techniky.
Jistě vás proto bude zajímat, jak nejlépe vybrat…

Martin Miloschewsky

Poznámka na závěr: Statistiky uvádějí, že asi 63 % lidí si opět koupí stejnou značku automobilu (jako měli minule). A zkuste si (pánové) položit otázku, podle čeho vybírá automobil vaše žena (obvyklá odpověď: podle barvy). Koupě osobního auta je tedy často zcela iracionální záležitostí. A jak se rozhodujeme při koupi výpočetní techniky?

Definice

TCO (Total Cost of Ownership): způsob výpočtu vytvořený pro uživatele i manažery podniků, jimž má pomoci ocenit všechny, tedy přímé i nepřímé náklady a výhody související s nákupem informačních technologií. Záměrem je tedy obsáhnout všechny relevantní informace a vlivy, které hrají roli při koupi IT.

Pojem TCO analýza vznikl v Gartner Group v roce 1987. Od té doby bylo vyvinuto množství různých metod, jak zjistit TCO. Spolu s tím byly vyvíjeny i softwarové prostředky pro podporu výpočtů TCO. Je jasné, že přesné stanovení TCO není triviální záležitostí. Vedle zřejmých nákladů (pořízení a provoz) mohou být kalkulovány i vlivy méně zřejmé. Z nich uveďme např. náklady na vytvoření disaster recovery plánů, ztráta businessu nebo zpomalení práce uživatelů, nemožnost dosažení požadovaného ratingu, vlivy výpadků systému atd. Pozitivně se naopak může projevit schopnost podniku rychleji zavést nové agendy pro podporu jeho činnosti, rychlejší testování nových úloh, snížení nákladů na elektrickou energii nebo snadnější splnění enviromentálních a legislativních předpisů.

Vyhrajte s MHM!

TAŠKA NA OBLEK
ČEKÁ NA ŠŤASTNÉHO VÝHERCE. PODROBNOSTI A SOUTĚŽNÍ OTÁZKU HLEDEJTE NA STRANĚ 23.

Data v péči MHM

Občasník
Vydáno: srpen 2007
Neprodejné
Vydává:
MHM computer s. r. o.
U Pekáren 4
102 00 Praha 10-Hostivař
telefon: +420 267 209 111
fax: +420 267 209 222
www.mhm.cz

Ve spolupráci s časopisem Computerworld ve vydavatelství IDG Czech, a. s.

COMPUTERWORLD

Připomínky a náměty pište na redakce@mhm.cz, případně na adresu vydavatele.

TCO – zaklínadlo výběrových řízení

TCO JE DNES NEJEN POPULÁRNÍM VÝRAZEM, ALE I DŮLEŽITÝM ROZHODOVACÍM KRITÉRIEM, KTERÉ SE VYSKYTUJE TÉMĚŘ VE VŠECH VÝBĚROVÝCH ŘÍZENÍCH, JEŽ MAJÍ CO DO ČINĚNÍ S IT. CO **VŠECHNO** SE ALE POD NÍM SKRÝVÁ? ZVÝRAZNĚNO JE SLOVO VŠECHNO, ALE DŮLEŽITĚJŠÍ JE POSLEDNÍ SLOVO OTÁZKY – TOTIŽ **SKRÝVÁ**.

TCO – Total Cost of Ownership – lze doslova přeložit jako „celkové náklady na vlastnictví“, volněji a výstižněji jako „co mne to bude stát, když si vybrané řešení pořídím a budu ho provozovat po sledovanou dobu“. Po takto rozšířeném vysvětlení si už řada manažerů řekla, že je to jednoduché, prostě se spočítají všechny náklady, a je to. Teoreticky je to správně, v praxi se však velmi často chybuje. A to právě v tom, co se do nákladů započítá a co ne.

Samostatnou kapitolu v úvahách o všech faktorech ovlivňujících TCO je kategorie nazývaná „Missed Opportunity“. Sem lze v širším pohledu zahrnout nejen nerealizovaný zisk z produktů a služeb, které byly uvedeny na trh příliš pozdě, případně vůbec ne (trh obsadila rychlejší konkurence), ale i ztráty z výpadku produkce kvůli nefungující IT infrastruktuře. Všechny tyto vlivy je třeba do vyčíslení TCO zahrnout.

V dalších odstavcích se pokusíme upozornit i na to, na co se často zapomíná, a zmíníme, jakých chyb se dopouštějí zadavatelé výběrových řízení.

TCO se totiž používá ke dvěma základním účelům – pro zjištění nákladů, které bude nutno vynaložit, a pro porovnání alternativních nabídek. Pokud máme jedinou volbu a zjišťujeme, kolik pro ni musíme získat do rozpočtu v jednotlivých letech, je situace ještě relativně jednoduchá. Při porovnávání alternativ je už vše mnohem komplikovanější. Náklady na jedno řešení velmi často nekopírují – a to ani skladbou započítávaných položek – náklady na řešení druhé. A co více, skryté náklady se mohou diametrálně lišit. Těmi se však předkladatelé jednotlivých alternativ obvykle nechlubí. Pokud se o nich vůbec zmiňují, pak nejčastěji více nebo méně pravdivě a relevantně poukazují na skrytá úskalí očekávaných řešení konkurence.

Je tedy vůbec TCO možné smysluplně použít jako výběrové kritérium? Ano, ale je třeba si uvědomit základní fakt, že

Celkové náklady (TCO) se dělí do tří základních skupin:

- náklady zřejmé a vyčíslitelné (relativně přesně)
- náklady zřejmé, ale obtížně vyčíslitelné
- náklady skryté

a podle toho k vyhodnocování TCO přistupovat.

NÁKLADY ZŘEJMÉ

Pokud jde o hardwarové komponenty (servery, disková pole apod.), pak nás pořizovací náklady a cena záručního i pozáručního servisu napadnou okamžitě. Ty však mohou být doprovázeny dalšími vyvolanými náklady na vybudování nebo rozšíření související infrastruktury. K ní patří např. páteřní síť mezi servery, síť SAN na propojení serverů, diskových polí a páskových systémů (switche, direktory, kabeláž), klimatizace, UPS a další. I ty budou vyžadovat náklady na záruční a pozáruční servis.

S tím souvisejí další náklady vznešeně dnes označované jako „environmentální“, jinak též náklady na „životní prostředí“ hardwarové infrastruktury. Sem patří např. náklady na plochu či prostor, kam budou zařízení umístěna, elektrický příkon zařízení a s tím spojené náklady na provoz klimatizace apod. A zapomenout nelze ani na náklady na veškerý spotřební materiál, média a další. Jejich vyčíslení již není tak jednoduché, neboť vyžaduje predikci vývoje cen (zejména energií) na celé uvažované období, většinou 4 až 5 let.

Další nákladová skupina obsahuje náklady nějakým způsobem spojené s pracovníky zadavatele. Sem patří náklady na školení, a to na všechna zařízení, která budou v souvislosti s výběrovým řízením pořizována (tedy i na související infrastrukturu). Dalšími položkami jsou náklady na implementaci nového řešení a migraci ze stávajícího stavu do nové infrastruktury. Náklady na straně dodavatele jsou zahrnuty v ceně nabídky. K tomu je ale třeba vzít v úvahu i časovou (a tedy i finanční) náročnost na součinnost pracovníků zadavatele. Na tyto náklady se velmi často zapomíná, nebo se na ně nebere ohled. Při složitější infrastruktuře však může implementace či migrace trvat týdny nebo měsíce a zaměstnat při tom celou řadu pracovníků. To může z hlediska TCO značně změnit pořadí vyhodnocovaných řešení.

Při výběru nového softwarového řešení se s náklady na vlastní pracovníky na školení a na implementaci počítá mnohem častěji (i když ne zcela vždy ve skutečně odpovídajícím rozsahu). Na co se v těchto případech spíše zapomíná, jsou naopak požadavky vybíraného softwarového řešení na hardwarovou infrastrukturu, které se mohou pro jednotlivé alternativy softwarových řešení značně lišit. A z hlediska TCO se vracíme na začátek této kapitoly.

Kdo došel při konstrukci výpočtu TCO až sem, vypracoval obsáhlý seznam položek, které je třeba

zpracovat a vyčíslit, a má pocit, že je s vyhodnocením hotov, setrvává v hlubokém omylu.

NÁKLADY SKRYTÉ ANEB NA CO SE ČASTO ZAPOMÍNÁ

Analytická společnost Gartner ve svých studiích uvádí, že celková pořizovací cena řešení představuje v průměru pouze 1/7 skutečných nákladů. A skryté náklady mohou tvořit 40 % nákladů zjevných v případě stabilního, konsolidovaného a velmi dobře řízeného prostředí, ale mohou dosáhnout až 400 % v prostředí heterogenním, distribuovaném a špatně řízeném.

Gartner: Špatně zvolené řešení může způsobit **desetinásobně vyšší skryté náklady** než řešení skutečně optimální!

Některé oblasti, na které je třeba si dávat pozor při vyhodnocení TCO, jsou uvedeny v následujících kapitolách.

ŘEŠENÍ SLOŽITÉ NA OBSLUHU

Některá řešení, byť se to třeba ani na první pohled nezdá, mohou v provozu přinášet řadu komplikací. První z nich je prostá časová náročnost na obsluhu, management či administraci standardních provozních úkolů. V této souvislosti často slýcháme argument: *„Ty lidi tady stejně máme a musíme je platit, tak mají alespoň co dělat.“* Velký omyl. Administrátor, kterému rutinní činnosti zaberou většinu pracovního času, nemá dostatek času na přípravu a zpracování jednorázových úkolů (o soustavném zvyšování kvalifikace ani nemluvě).

Složité řešení vyžaduje časté konzultace s dodavatelem o tom, jak řešit určité situace a úkoly. Takové konzultační služby nad rámec kontraktu jsou vždy drahé a přinášejí s sebou i administrativní zátěž – tedy další náklady.

ŠETŘENÍ PŘI NÁKUPU – REDUKCE FINÁLNÍHO ŘEŠENÍ

Nákupní oddělení se velmi často chovají tak, jako by vycházela z přesvědčení, že dodavatel jim nabízí to, co všechno chce prodat, a ne jen to, co skutečně potřebují. Následkem je ve finále škrtání některých součástí řešení. A to, že někdy mají (bohužel) skutečně pravdu, je vede k přesvědčení, že tento postup je oprávněný a potřebný vždy. Ale to už pravda není.

Nízká pořizovací cena není zárukou nízkého TCO!

Jeden příklad za všechny: Při konsolidaci datových kapacit dojde k nákupu diskového pole a infrastruktury SAN. Z řešení je však vyškrtnut nástroj pro management a školení příslušného pracovníka. Každou rekonfiguraci pak musí zákazník objednat a zaplatit zvlášť, protože jeho pracovníci buď tento úkol řešit neumějí, anebo nesmějí, neboť smlouva s dodavatelem nepřipouští zásah pracovníka, který příslušné školení nemá. Neodborný zásah totiž může snadno způsobit ztrátu dat nebo poškození jejich konzistence.

NÁKLADY VÝBĚROVÝCH ŘÍZENÍ

Náklady na výběrová řízení se skládají ze tří základních částí:

- náklady na přípravu a zadání výběrového řízení
- náklady na vyhodnocení výběrového řízení
- náklady na (následné) řešení sporů

U velkých projektů je zřejmé, že náklady na výběrové řízení jsou značné. Již jen několikaměsíční příprava zadání, na níž pracuje řada odborných pracovníků, znamená nemalé náklady. Ve většině případů však ještě zdaleka nejde o položku rozhodující. I když ne za všech okolností jsou to náklady zbytečně vynaložené. Dobře připravené výběrové řízení může ušetřit daleko více nákladů následujících.

Náklady na vyhodnocení zahrnují dvě základní oblasti – vyhodnocení nabídek (ve všech kolech výběrového řízení) a testování nabízených řešení. Zadavatel by si měl vždy zvážit, zda *náklady na organizaci a vyhodnocení druhého, třetího, čtvrtého… kola výběrového řízení nakonec nepřevýší snížení nákladů (a to všech, ne jen pořizovacích!), kterého se dá druhým, třetím, čtvrtým… kolem dosáhnout.*

Táhne-li se vyhodnocování příliš dlouho, může se stát, že se i úspěšně uzavřené výběrové řízení bude muset opakovat. *Příklad ze života: Výběrové řízení na servery bylo úspěšně ukončeno po třinácti měsících od podání nabídek – a nabízené servery se již nevyráběly, a nebylo je tedy možné dodat. Vynaložené náklady se nijak nevrátily a muselo se začít znovu.*

Pokud je součástí vyhodnocení i testování (alespoň některých) nabízených řešení, mohou náklady na opakované vybudování testovací infrastruktury a vlastní provedení testů představovat zdaleka ne zanedbatelnou část ceny nabídky (a to nemluvíme o nákladech na straně dodavatelů, ale jen na straně zadavatele).

V zásadě nelze předejít tomu, aby nedošlo k odvolání se proti výsledku výběrového řízení některým z postižených soutěžících. Dobře připravené zadání (jasně definovaná a hodnotitelná kritéria) však může řešení těchto problémů podstatně zjednodušit. Pokud následuje řada odvolání – od zadavatele po Úřad pro ochranu hospodářské soutěže – a řešení skončí u soudu, jsou všechny náklady vynaloženy naprosto zbytečně a po roce (když se to nikde nezdrží) se může začít znovu.

Všechny výše uvedené skutečnosti vedou k poněkud překvapivému závěru – z hlediska výběrového řízení lze často nejvíce snížit TCO tím, že *výběrové řízení vůbec nevypíšeme* (pokud nám to zákon dovolí).

Tak se lze totiž dostat k potřebnému řešení nejrychleji. A to může být velmi podstatné. Málokdo si totiž pořizuje novou, výkonnější, spolehlivější či lépe zabezpečenou infrastrukturu dopředu, aby byl na nové požadavky, které teprve přijdou, připraven s předstihem a IT infrastruktura se nestala brzdou zavedení nového výrobku či služby. Do vyhodnocení TCO je nutno započítat i kolonku „Missed Opportunity“, v tomto případě zisk, který nebyl realizovaný díky zpožděně-

ní či přímo neuvedení výrobku či služby na trh. Tato položka totiž může výrazně převýšit poněkud vyšší náklady spojené s rychlejší obnovou IT.

NEPERSPEKTIVNÍ ŘEŠENÍ

Často opakovanou chybou je zadání pokrývající (možná i beze zbytku) současné potřeby, ale bez možnosti dalšího rozvoje. Zcela triviálních příkladů najdeme celou řadu, např.:

– SAN infrastrukturu, kde jsou již při instalaci vyčerpány všechny dostupné porty. Přidání jediného serveru znamená výměnu switchů za větší.

– Diskové pole, které má konsolidovat kapacity všech serverů je na hranici své kapacity. Zvýšení požadavků na data znamená přidání dalšího diskového pole (což neguje původní myšlenku konsolidace) nebo výměnu za pole nové.

– Do budoucna se uvažuje o vybudování vzdáleného střediska, do nějž budou replikována data, a diskové pole není možné následně vybavit potřebnou funkcionalitou.

Vysoká cena sama o sobě není ani zárukou kvality, ani nižšího TCO!

– Softwarová aplikace neumožňuje rozšíření o další potřebný modul. Ten se musí řešit jinou aplikací a vytvořením (většinou na zakázku, tedy draze) složitých integračních můstků mezi aplikacemi nebo přímo přechodem na aplikaci novou.

Ve všech případech volby neperspektivního řešení dochází k předčasné obměně infrastruktury, což má dva základní negativní dopady:

– Stávající zařízení nebyla využita po dobu předpokládanou při jejich výběru, vynaložené prostředky nebyly zhodnoceny předpokládaným způsobem.

– Nechtěně brzy se vracíme na začátek celého článku – vyhodnocení TCO nového řešení včetně všech zjevných a skrytých nákladů.

A náklady na nové řešení nemůžeme pouze vyčíslit, musíme je i vynaložit. Přitom v některých případech, jako je třeba migrace z jednoho komplexního informačního systému typu ERP na druhý, mohou být náklady na školení a vlastní migraci vyšší, než je vlastní cena systému včetně licencí a podpory!

UZAVŘENÁ ŘEŠENÍ

Jinou formu neperspektivních řešení jsou tzv. uzavřená řešení, jinak též označovaná jako „Vendor Lock“. Zákazník často podlehne lákavé ceně primárního řešení, aby pak zjistil, že všechny další komponenty potřebné pro plánovaný rozvoj musí nakupovat u téhož dodavatele – a značně dráž, než by je bylo možno opatřit z jiných zdrojů. Zařízení koupená jinde než u dodavatele primárního řešení jsou prohlášena za nekompatibilní (byť jde i o stejné zařízení) nebo alespoň za nepodporovaná řešení. Jakákoliv závislost na jediném výrobci/dodavateli je z hlediska TCO škodlivá. Vyrábí-li například páskové médium jediný výrobce, je jeho cena podstatně vyšší, než když vzájemně kompatibilní média vyrábí výrobců několik.

PLÁNOVANÉ VÝPADKY

Pokud se uvažuje o výpadcích zpracování, pak se prvoplánově téměř vždy uvažuje o výpadcích neplánovaných. Přitom plánované odstávky vyřadí velmi často aplikace z provozu na delší dobu (z pohledu dlouhodobého sledování) než výpadky neplánované.

Příčin plánované odstávky je celá řada. Nepatří sem jen implementace aktualizací a nových verzí systémového a aplikačního programového vybavení či upgrade serverů a diskových polí, ale i příčiny poněkud vzdálenější, které se týkají jejich okolí – renovace elektrických rozvodů v objektu, údržba komunikační infrastruktury apod. Pokud jsou tímto dotčeny aplikace vyžadující provoz v režimu 24 × 7 (a ty se dnes vyskytují téměř všude), je třeba v rozboru TCO počítat i s položkou „Missed Opportunity“ ve smyslu výpadku zisku z výpadku produkce dané nefunkčností IT. Z tohoto pohledu se různé alternativy řešení mohou velmi podstatně lišit.

A AŽ DOJDE K HAVÁRII…

Až dosud jsme zvažovali situace, kdy všechno probíhá normálně, bez výskytu nestandardních stavů či dokonce havárií. Těmi mohou být živelné katastrofy typu požár, povodeň (události roku 1997 a 2002 nás přesvědčily, že slovo povodeň nepatří pouze do zpráv ze zahraniční), poruchy v okolí (přerušený telekomunikační spoj mezi centrálním střediskem a vzdálenými pracovišti) či chyby v aplikaci nebo poruchy hardwarové infrastruktury. Nejčastěji však jde o selhání lidského faktoru.

Z analýzy rizik vyplynou dva základní požadavky týkající se obnovy zpracování:

– RTO (Recovery Time Objective), tedy doba, za jakou je nutno obnovit zpracování aplikací.

– RPO (Recovery Point Objective), tedy nejvzdálenější bod v minulosti, ke kterému je ještě přípustné obnovit konzistentní datovou základnu (všechny změny promítnuté od té doby do dat jsou ztraceny).

Je zcela zřejmé, že požadavky na oba faktory se mohou zásadně lišit podle typu organizace. A zásadně se také liší důsledky vlastní havárie i nemožnosti dodržet předem stanovené hodnoty faktorů RTO a RPO. Pro organizaci typu místního úřadu neznamená ani výpadek zpracování řádově ve dnech včetně ztráty provedených aktualizací do registru obyvatel velký problém – o zákazníky nepřijdou a nejvýše se budou muset zaplatit nějaké přesčasové hodiny potřebné pro znovuzavedení dat z papírových formulářů. Pro banku nebo investiční společnosti obchodující on-line na burze může mít

mnohem kratší výpadek zpracování fatální následky. Přitom nepůjde jen o ztráty způsobené vlastním výpadkem zpracování, ale zejména o ztrátu důvěry klientů a o jejich odliv, což může mít v krajním případě i katastrofální důsledky.

Ale i pro „méně náročné“ organizace může mít výpadek velké důsledky. Příklad ze života: *Firma působící na českém trhu v silně konkurenčním prostředí zaznamenala dva relativně blízko po sobě jdoucí výpadky diskového systému, čímž byla vždy cca na den zcela zastavena expedice. Důsledkem byl nejen výpadek denních tržeb (kamiony po 6 hodinách marného čekání odjely s prázdnou), ale i ztráta cca 5 % zákazníků, kteří již nikdy nepřijeli. Předchozí levnější řešení je přišlo hodně draho. Po tomto vyhodnocení povolilo vedení investici přesahující 8 mil. Kč, aby se dalšímu opakování takové situace předešlo.*

Správné stanovení parametrů RTO a RPO je důležitou podmínkou objektivního posouzení vlivu jejich splnění, respektive nesplnění, na TCO. Přitom je záhodno brát v úvahu zejména

– typ poruchy či havárie
– pravděpodobnost či přímo četnost výskytu takového typu poruchy

Je tedy zřejmé, že různé typy poruch budou vyžadovat různá řešení, budou mít různé hodnoty RTO a RPO. Vezměme například chybu lidského faktoru, která způsobí nutnost obnovy databázového prostředí jediné aplikace. Tento typ „poruchy“ je poměrně častý, lze téměř s jistotou předpokládat, že se ve vyhodnocovaném období vyskytne vícekrát. Každý tento výpadek může mít významné ekonomické důsledky a přitom ochrana proti němu (respektive řešení snižující RTO a RPO na požadované minimum) nemusí být drahá. Do TCO by se tedy měla započítat celková ztráta způsobená odhadovaným počtem výpadků při použití jednotlivých řešení.

Na druhé straně zničení celého výpočetního střediska požárem či povodní by sice mohlo mít katastrofální důsledky pro podnik, ale jeho pravděpodobnost je minimální (i když ne nulová). Je-li pravděpodobnost této havárie 0,001 % (číslo pouze pro modelový případ), pak by se do TCO mohla například započítat pouze jedna stotisícina ztrát způsobených takovou havárií.

Současný stav ale nic neříká o budoucnosti. Další součástí tohoto hodnocení by tedy měl být i odhad, jak se budou vyvíjet požadavky na RTO a RPO pro jednotlivé typy poruch v průběhu sledovaného období a hlavně jak se bude v čase vyvíjet dopad nesplnění těchto parametrů. Například pokud plánuje firma rozjet novou výrobu, může být obrat v příštím roce dvojnásobný proti stávajícímu stavu, a tedy i dopad výpadku zpracování bude výrazně vyšší.

V zásadě lze náklady vynaložené na omezení dopadu určité poruchy považovat za určitou formu pojistky proti důsledkům této poruchy. A podle toho s ní také zacházet – zhodnotit míru rizika, potenciální výši škody a výši pojistky, kterou jsem za různou míru omezení jejích důsledků ochoten zaplatit.

CO ŘÍCI NA KONEC

Při přípravě tohoto článku jsme si nedali za úkol beze zbytku vyčerpat a popsat všechny faktory, které mají vliv na celkovou výši a efektivitu vynaložených nákladů. Ani jsme nechtěli připravit univerzální systém tabulek s předprogramovanými výpočty a vazbami, do kterých by se vložily všechny dostupné (i nedostupné) informace a vypadlo by jediné číslo – hodnota TCO. To prostě nejde. Chtěli jsme jen přivést čtenáře k zamyšlení nad zdánlivě (alespoň pro někoho) „jednoduchým“ úkolem, jakým je vyčíslení celkových nákladů spojených s jednotlivými nabízenými alternativami řešení, a poukázat na některé aspekty, které bývají nedoceňovány nebo opomíjeny. Pokud to pomůže k tomu, aby alespoň v některých případech bylo k vyhodnocování TCO ve firmách a organizacích přistupováno komplexněji než dosud, byl záměr autora splněn.

Jan Heřmánek

P.S.: Články na téma TCO jsem původně napsal ve dvou různých verzích. Ta první obsahovala jedinou větu: „Chcete snížit TCO? – přijďte se poradit do MHM.“ Druhá verze nastiňovala na 12 hustě popsaných stranách stručný rozbor 30 základních prvků, které mají vliv na výši TCO. Obě verze shrnovaly zkušenosti MHM v této oblasti. Obě verze mi šéfredaktor zamítl. A tak vznikla verze třetí, kterou jste právě dočetli. Pokud si laskavý čtenář po přečtení článku řekne „No to je přece jasné!“ nechť si zkusí položit i otázku: „A opravdu to všechno bereme v úvahu?“ Zda se s námi o svou upřímnou odpověď na tuto otázku podělí (což bychom rádi), nebo ne, necháváme zcela na něm.

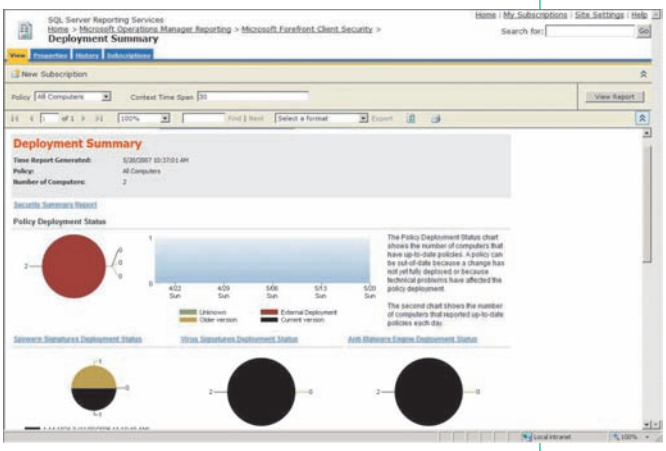
Forefront Security a System Center: Manželství z rozumu

INFORMAČNÍ BEZPEČNOST DOSUD UTĚŠENĚ BOBTNALA. A TO JAK CO DO POČTU APLIKACÍ, TAK POKUD JDE O NÁROKY NA SPRÁVU NEBO NA VÝKON. NYNÍ NASTAL ČAS, ABY ZE SVÝCH NÁROKŮ SLEVILA. NE SNAD PROTO, ŽE BY SE SVĚT ICT STAL JAKO MÁVNUTÍM KOUZELNÉHO PROUTKU BEZPEČNĚJŠÍM. ALE PROTO, ŽE SPOLEČNOST MICROSOFT PŘICHÁZÍ S ŘEŠENÍM FOREFRONT SECURITY.

Nenávratně pryč je doba, kdy k zajištění bezpečnosti informačního systému postačoval antivirový program – lhostejno, zdali na stanicích, serverech či na obojím. Jak šel čas, hrozby se měnily a bylo potřeba na ně odpovídajícím způsobem reagovat. Respektive namísto slůvka „měnily“ by bylo vhodnější použít „přidávaly“. Nové hrozby přibývaly, staré nemizely.

Po počítačových virech přišel spyware, který začal vyžadovat jiné detekční a ochranné metody, na jejichž implementaci by bylo antivirové programy příliš složité upravovat. A tak vznikla kategorie ochranného softwaru nazývaná „antispyware“.

S rozvojem elektronické pošty přišla skutečná epidemie spamu, nevyžádané elektronické pošty.



Zatímco jiné hrozby se v čase alespoň vyvíjejí, a byť nemizí docela, opouštějí přední příčky žebříčků hrozeb, u spamu tomu tak není. Jedná se o dlouhodobý problém, který v čase naopak graduje. Dnes je spam (tvoří zhruba tři čtvrtiny z veškeré e-mailové komunikace) používán nejen k nabídkám povzbuzujících pilulek či inzerování služeb pro dospělé, ale rovněž jako šiřitel škodlivých kódů, zdroj dezinformací, pomocník podvodníků či nástroj pro sondování terénu před dalším útokem. A tak se filtr spamu (antispam) posunul z kategorie „nástroj pro zvýšení efektivity práce“ do kategorie „jeden ze stavebních kamenů bezpečnosti“.

Ani to ale ještě není zdaleka všechno. Nebo je zde někdo, kdo by chtěl pochybovat o potřebnosti a užitečnosti firewallů? A to ať personálních na jednotlivých stanicích nebo síťových na přístupových bodech k internetu. Asi ne. Statistiky stroze konstatují, že počítač bez firewallu připojený k internetu má 99% šanci, že se během deseti minut stane cílem úspěšného útoku. Podotýkáme, že je zcela lhostejné, na jaké běží platformě.

V neposlední řadě pak čím dál tím větší ohrožení bezpečnosti představují různé chyby a zranitelnosti v programech, na které je nutné aplikovat bezpečnostní záplaty. Dle statistik americké organizace CERT bylo v roce 2006 oficiálně objeveno a oznámeno 8 064 nových zranitelností (což představuje meziroční nárůst o 35 %). Organizace Secunia používá jinou metodiku výpočtu, takže nových zranitelností bylo podle ní 5 128 (meziroční nárůst o 12 %). Ať tak či onak, v obou případech jde o čísla varovná, vysoká a rychle rostoucí. Roste zároveň počet tzv. zero-day attacks, útoků nultého dne. Tedy útoků, kdy je oznámená chyba aktivně zneužita v průběhu 24 hodin – tedy v době, kdy je málokdy aktualizace vydaná i nainstalovaná na cílové stroje. Tedy v době, kdy před zranitelností neexistuje ochrana. Je tedy zapotřebí věnovat odpovídající pozornost také sledování a instalaci záplat (Patch Management).

Antivirový program, antispyware, firewall, filtr spamu, Patch Management – to jsou základní pilíře, na kterých dnes stojí (a někdy s nimi i padá…) informační bezpečnost. V návaznosti na skutečné potřeby organizace ale může být ochranných programů instalována celá další řada. Namátkou jmenujme technologie IDS, VPN, šifrování, data loss prevention aj. To jsou ovšem technologie, které nepotřebuje vždy a všude každý – mohli bychom je tedy označit jako „volitelné“.

BEZPEČNOST JE TŘEBA SPRAVOVAT

Každopádně, aby toho nebylo málo: toto všechno je potřeba řídit a spravovat. Bezpečnost není jednorázový úkon, který by bylo možno ošetřit stylem „nainstaluj a zapomeň“, ale jde o kontinuální proces. Jsme-li v určitém okamžiku zabezpečeni (čestnější by asi bylo říci „cítíme se zabezpečeni“), neznamená to, že na druhém konci planety se právě nevydává do světa nový škodlivý kód nebo že někdo neobjevil novou zranitelnost, na které je náš stávající systém krátký. A díky nimž budeme muset začít zajišťovat bezpečnost znovu. Pro úplnost dodejme, že dle různých metodik výpočtů se denně objeví desítky až stovky nových škodlivých kódů. A zhruba stejný počet exploitů – útoků proti bezpečnostním chybám softwaru.

Pokud nebudeme informační bezpečnost řídit my, bude řídit ona nás. To je jednoduché pravidlo. Zkrátka potřebujeme mít bezpečnostní prvky pod kontrolou. Jen tak zajistíme, že budeme mít včas nainstalované všechny aktualizace antivirového programu, že nám neunikne žádná záplata, že se do sítě nepřihlásí nějaký neautorizovaný hardware… Zcela logicky pak chceme mít celou bezpečnost pod společnou kontrolou, neboť jinak ztrácíme přehled a nikdy nebudeme mít jistotu, že někde „nenechal tesař díru“.

Z výše uvedeného seznamu bezpečnostních aplikací je zcela zřejmé, že tyto si v posledních letech začaly žádat čím dál větší množství zdrojů. Lidských, finančních, hardwarových, komunikačních… Což samo o sobě nebylo šťastné, protože bezpečnost začala být jakýmsi molochem, se kterým bývalo často více potíží, než kolik přinášel hmatatelného užitku (byť ten nehmatatelný je evidentní – organizace se může soustředit na svoji činnost, aniž by byla valchována bezpečnostními incidenty).

ZJEDNODUŠENÍ SITUACE

Právě řešení Forefront Security od společnosti Microsoft obrací tento trend narůstající náročnosti. Pochybovači si možná v tuto chvíli řeknou: Je možné v oblasti informační bezpečnosti přijít s něčím novým? Nejsou to jen planá slova a marné sliby? Vězte, že s něčím novým lze přijít i na tak saturovaném a vysoce konkurenčním trhu, jakým ICT bezpečnost je.

Řešení Forefront Security je komplexní. Což by samo o sobě nebylo ničím zvláštním, protože dnes je v oblasti informační bezpečnosti prakticky každý „komplexní, komplexnější, nejkomplexnější“. Forefront Security ale jde ještě dále. Kromě toho, že přináší nejucelenější portfolio ochranných produktů, jaké není schopen nabídnout a dodat žádný jiný výrobce, přichází i se systémem řízení bezpečnosti pomocí produktů rodiny System Center.

Tyto produkty umožňují kromě bezpečnostních produktů řídit i vlastní informační systém. Nemusíte tak mít jedno „řídicí středisko“ pro správu systému a jedno (v lepším případě…) pro řízení ICT bezpečnosti. Vše máte pěkně „pod jednou střechou“. Z této symbiózy plyne celá řada výhod, které jiná řešení nenabízejí.

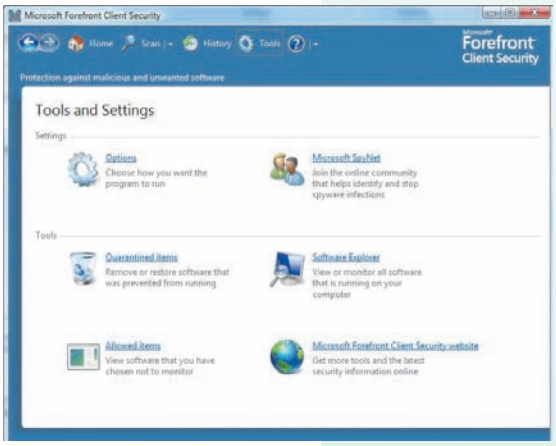
Především nemusíte sedět na dvou židlích najednou. Odstraníte tak mnoho problémů, které s tím vznikají. Příkladem budiž třeba špatně nakonfigurovaný systém řízení bezpečnosti, který nerozesílá záplaty na všechny potřebné instalace v síti – protože tyto jsou ošetřovány zcela jiným softwarem. Pokud ale oba úkony (instalace + záplatování) řeší jedna aplikace, je toto riziko eliminováno.

Homogenní prostředí totiž kromě jiného umožňuje shromažďovat a porovnávat data. Tím lze rychleji a přesněji odhalit případné bezpečnostní slabiny, které mohou představovat riziko pro celý informační systém. Některé souvislosti by totiž za běžných okolností mohly zůstat bez povšimnutí nebo by se na ně přišlo až s nežádoucí časovou prodlevou. Že jde v oblasti ICT bezpečnosti právě o čas a právě o kvalitní předcházení incidentům, jistě netřeba dvakrát zdůrazňovat.

Forefront Security plus System Center představují pokrok i v jednoduchosti. Spojením řízení do jednoho rozhraní se uvolní nemalé množství zdrojů. Jinak řečeno, dvěma samostatným systémům bychom se nemohli věnovat s takovým nasazením jako systému jednomu. Eliminujeme tím i kolize, kdy zůstávají neošetřené oblasti (protože jeden systém spoléhá na druhý, takže v praxi nikdo nedělá nic) nebo naopak se oblasti zbytečně překrývají (raději to udělám…) a konzumují zdroje.

SNÍŽENÍ NÁKLADŮ

A tím jsme se dostali k hlavní devize řešení Forefront Security a System Center, kterou je ekonomický přínos. Ten můžeme hledat nikoliv v jedné, ale hned v několika samostatných rovinách. Tak předně: při použití jednoho systému šetříme za nákup licencí i za následný provoz (práce administrátora, jeho školení…). V případě dvou systémů je výjimkou potvrzující pravidlo situace, kdy některá z jejich komponent není zdvojená – např. hardware. Odbourání tohoto zdvojení rovná se ušetřené náklady.



Ruku v ruce s tím jde vyšší efektivita práce administrátora (klesají nároky na jeho čas), ale především vyšší efektivita uživatelů (o kterou by nám mělo jít především, protože kvůli ní celý informační systém vzniká a existuje). Komunikační kapacity nejsou zatěžované, doba odstávky systémů klesá, kumulací správy dochází ke snížení počtu restartů a dalších prostojů, často odpadají i různí nadbyteční monitorovací agenti (čímž se zvyšuje výkon a využití hardwaru).

Náklady klesají také tím, že je celý systém transparentnější. Mizí z něj nadbytečné prvky, zbytečný a nepoužívaný software, je pružnější a schopný rychle reagovat na taktická i strategická rozhodnutí, kromě administrace je jednodušší i audit. Také vyšší bezpečnost znamená ekonomickou úsporu. Méně incidentů rovná se méně mimořádných výdajů na jejich likvidaci, což znamená plynulejší provoz organizace.

Z dlouhodobého hlediska tak jednoznačně klesají TCO, Total Cost of Ownership. Tedy celkové náklady na vlastnictví. Protože stejně jako u automobilu nás zajímá spotřeba, tak by nás i v oblasti informačních technologií mělo zajímat, jaké náklady budeme muset vynaložit na provoz toho či onoho systému po dobu jeho používání. Neboť náklady na pořízení licence (byť jsou na první pohled nejpatrnější) představují jen asi deset procent částky, kterou budete postupně do systému vkládat. A to v podobě nákladů na provoz, údržbu, školení personálu apod. Spojení bezpečnostní technologie Forefront Security a System Center tak představuje nejen krok dosud nevídaný, ale také skutečné „manželství z rozumu“. A profitovat z něj můžete právě vy.

Tomáš Přibyl, Microsoft

SNIŽOVÁNÍ TCO V OBLASTI PAMĚŤOVÝCH SYSTÉMŮ

Zaměřte se na dodržení svých plánů a cílů

PROVOZOVATELÉ A SPRÁVCI PAMĚŤOVÝCH ŘEŠENÍ BY SE MĚLI TRVALE VĚNOVAT SLEDOVÁNÍ CELKOVÝCH NÁKLADŮ NA JEJICH VLASTNICTVÍ. HITACHI DATA SYSTEMS SE V TOMTO ČLÁNKU ZAMĚŘUJE NA NĚKTERÉ Z PŘEKÁŽEK BRÁNÍCÍCH OPTIMALIZACI CELKOVÝCH NÁKLADŮ NA VLASTNICTVÍ V DATOVÝCH CENTRECH A NABÍZÍ STRATEGII, JAK SE S TĚMITO PROBLÉMY VYPOŘÁDAT.

Ať už se zaměříme na kterýkoli obor nebo na kteroukoli část dodavatelského řetězce, zjistíme, že všichni hovoří o tomtéž – o TCO, tedy o celkových nákladech na vlastnictví. Jedná se bezesporu o důležitou věc, kterou musíme mít na paměti a která se dotýká přímo základů podnikání, ať už je jeho předmětem cokoli.

Důležitost celkových nákladů na vlastnictví by si měla uvědomovat také IT oddělení, a to možná ještě více než kdokoli jiný. Porozumění a úspěšné zvládnutí tohoto pojmu v prostředí, které je obvykle heterogenní a skládá se z celé řady rozdílných systémů a sítí, však může být obtížné. Možná bude vhodné nejdříve si ujasnit, co přesně máme pod pojmem „celkové náklady na vlastnictví“ na mysli:

Celkové náklady na vlastnictví (TCO) nesmíme zaměňovat s prostými náklady. Například Gartner odhaduje, že pořizovací náklady na položku IT zařízení představují pouhou sedminu celkových nákladů na vlastnictví této položky.

V TCO jsou zahrnuty jak „měkké“ tak i „tvrdé“ náklady, přičemž to, do které z těchto kategorií daný náklad zařadíme, se může během času měnit. Například čas potřebný na zotavení po havárii můžeme považovat za „měkký“ náklad až do doby, kdy k havárii skutečně dojde.

Nákladové položky, ze kterých se skládá TCO, mohou ovlivnit naše investiční i provozní výdaje.

Některé náklady, které jsou součástí TCO, se mohou realizovat velice rychle, zatímco jiné vynakládáme až teprve během delšího časového období.

Pokud tedy chceme stanovit celkové náklady na vlastnictví paměťového prostředí v organizaci, musíme vzít v úvahu mnohem více než jen náklady na nákup a údržbu používaného hardwaru a softwaru. Existuje celá řada dalších aspektů, které musí řídící pracovník v oblasti IT při stanovování celkových nákladů na vlastnictví vzít v úvahu. O některých z nich se zmíníme podrobněji.

SPRÁVA PAMĚŤOVÉHO PROSTŘEDÍ

Náklady na správu paměťového prostředí můžeme jednoduše vyjádřit jako objem člověkohodin a dalšího úsilí vynaloženého na řízení paměťové infrastruktury. Tyto náklady můžeme měřit počtem ekvivalentních pracovníků na plný úvazek na instalovaný terabajt dat. Obecně platí, že pro paměťová řešení s vrstvenou (tiered) a sdílenou (pooled) architekturou je typický počet spravovaných terabajtů paměťové kapacity na jednoho administrátora vyšší, než je tomu v případě samostatných, izolovaných paměťových systémů.

Náklady na pracovní sílu mohou představovat až 45 % celkových nákladů na vlastnictví paměťové infrastruktury, a jsou proto jedním z prvních cílů při napjatém rozpočtu. I když snaha o dosažení úspor v této oblasti může být efektivní, je důležité zajistit, aby i po úsporných opatřeních zůstával dostatečný počet pracovníků s potřebnou kvalifikací, kteří budou schopni řádně zajistit potřebné úkoly. Problém často spočívá v tom, že jsou správci paměťových systémů nuceni spravovat rozsáhlá heterogenní prostředí obsahující systémy, které nejsou schopny vzájemné komunikace. Lepším řešením proto často bývá zaměřit se na výkonnost architektury a vyšší efektivity i úspor dosáhnout touto cestou.

Software Hitachi Dynamic Provisioning umožňující „tenké“ přidělování kapacit (thin provisioning) dovoluje uživatelům přidělovat virtuální paměťové disky dle předpokládaných budoucích požadavků na paměťový prostor bez nutnosti vyhrazovat fyzické diskové paměti. Pokud v budoucnosti vznikne potřeba dokoupit další fyzické zdroje, bude možné tyto zdroje pořídit za nižší cenu, přičemž jejich implementace proběhne zcela hladce a bez rušivých vlivů na běh důležitých aplikací. Tato funkce využívá výhod stávajících služeb vyvinutých společností Hitachi, které zajišťují back-end virtualizaci a řízení paměťových prostředků, stavějí virtualizaci do popředí, a umožňují tak organizacím pohlížet na své paměťové zdroje novým způsobem.

To přináší velmi silný potenciál pro zvýšení efektivity. Poradenská firma Centrix poskytující poradenství vedoucím pracovníkům v oblasti IT ve svém nedávném odhadu uvedla, že podobně konfigurované, špičkové řešení dodávané konkurencí spotřebuje ve srovnání se řešením Hitachi Universal Storage Platform V s dynamickým provisioningem o 60 % více prostředků z IT rozpočtu. To dokládá významné snížení nákladů na konfiguraci paměťového řešení, jeho správu a přesuny dat.

VÝKONNOST PAMĚŤOVÉHO ŘEŠENÍ

Nedostatečná výkonnost paměťového systému může mít na chod podniku celou řadu negativních vlivů. Mohou být například negativně ovlivněny proce-

sy zálohování a obnovy, což zvyšuje pravděpodobnost výpadku. U podniků, jejichž obchodní aktivity závisejí na on-line interakci, může pomalá odezva způsobit, že jejich zákazníci přejdou ke konkurenci. Zároveň také může utrpět vnitropodniková produktivita, protože zaměstnanci nejsou schopni přistupovat k informacím, které potřebují. V tom nejhorším případě může dokonce firma porušit ustanovení daná zákonem – to v případě, že nejsou k dispozici firemní data za delší časová období – a může tak být ohrožena samotná její existence. Mezitím musejí pracovníci IT pracovat přesčas, aby předešli případným problémům nebo aby je vyřešili ještě předtím, než dojde k některému z výše zmíněných důsledků.

Přesná kvantifikace nákladů na výkonnost může být obtížná, proto je možná lepší o výkonnosti uvažovat ve smyslu možných dopadů na výši příjmů. Pokud je výkonnost paměťové infrastruktury nízká, bude to mít nepříznivý dopad na propustnost na úrovni serverů a to zase může nepříznivě ovlivnit výsledky obchodních aktivit, které vytvářejí podnikové příjmy.

Proto je nanejvýš důležité řádné plánování, které zajistí, že paměťové síťové řešení bude schopno nabídnout přijatelné parametry. Podniky by se proto měly spolu se svými dodavateli snažit identifikovat oblasti, ve kterých je možné dosáhnout zlepšení.

Hitachi Universal Storage Platform V dokáže vytvářet velké logické paměťové oblasti (storage pools). Každý storage pool může obsahovat stovky diskových jednotek, dovolujících paralelizovat I/O operace. To významně zvyšuje výkonnost aplikací, protože k vytváření svazků nad velkým počtem diskových jednotek není nutné používat správce svazků na úrovni jednotlivých hostitelských počítačů.

NEVYUŽITÁ PAMĚŤ

Za nevyužitou paměť se považuje kapacita, která byla zakoupena, ale právě se nevyužívá. Zajištění 100% využití je nereálné, takže existence prázdného místa je do určité míry nevyhnutelná a žádoucí, ale mnoho řídících pracovníků v oblasti IT se snaží zajistit, aby ho bylo co možná nejméně. Optimalizace využití paměti samozřejmě také znamená, že nezůstanou nevyužity náklady na uchovávání dat, vynakládané na software, na energii či na chlazení, což přispívá ke zvýšení celkové rentability nákladů. Rozpoznání zákonitostí v oblasti nevyužitých kapacit může také pomoci minimalizovat budoucí výdaje.

Existuje celá řada způsobů, jak tuto záležitost vyřešit, a to včetně deduplikace dat, tierování paměti umožňující přesun nevyužitého prostoru na nižší tier, „tenkého“ přidělování (thin provisioning) a virtualizace paměti. I když všechny tyto přístupy mohou podniku přinést vyšší hodnotu a pozitivně ovlivnit celkové náklady na vlastnictví, jejich zavedení musí být plánováno za pomoci kvalifikovaných dodavatelů paměťových systémů, aby se nestalo, že organizace vynaloží více na správu řešení než na samotné vyřešení problému.

PROSTOR V DATOVÉM CENTRU

Čím méně prostoru paměťová infrastruktura zabírá, tím levnější je její provoz. Je tomu tak kvůli nákladům na provozování datového centra – např. na fyzický prostor v budově, na energii a na klimatizaci.

Virtualizací paměťového prostředí mohou IT oddělení snížit počet potřebných fyzických serverů, a tím minimalizovat zabranou podlahovou plochu a snížit požadavky na energii i na chlazení.

Hitachi Universal Storage Platform V je v současné době jediným velkokapacitním heterogenním virtualizačním řešením v tomto odvětví a dokáže podporovat téměř nekonečné množství externích paměťových kapacit. Nyní podporuje 247 petabajtů, což je o 670 % víc než původní verze USP a o 24 600 % více než kterýkoli jiný paměťový systém. To může přispět k urychlení a zjednodušení rozhodování o virtualizaci paměti, což zase může mít bezprostřednější a výraznější dopad na rentabilitu nákladů oddělení IT.

BEZPEČNOST A OCHRANA DAT

Zabezpečení dat je zajišťováno nejrůznějšími způsoby. Některé požadavky diktují, aby bylo zajištěno především bezpečné uložení dat, zatímco jiné vyžadují také ochranu dat během jejich přenosu. Náklady na splnění těchto požadavků se liší v závislosti na stáří dat, na typech přístupu k nim a na stávajících i očekávaných přenosech příslušných dat.

Je také důležité zajistit zavedení efektivní strategie ochrany dat pro případ závažné poruchy systému (např. v případě katastrofy). Informace je třeba uchovávat bezpečně, v ideálním případě na více místech, a musí existovat plán jejich rychlé obnovy.

Na rozdíl od konkurence integrovala společnost Hitachi funkce pro zabezpečení dat přímo do kontrolérů. Systém Hitachi USP V je jedinečný v tom, že dokáže izolovat a ochránit vysoce zabezpečovaná data v jakémkoli bodě jejich pohybu v hierarchii pamětí – z kanálu do vyrovnávací paměti a dále až do vlastního paměťového zařízení (disku). K dalším bezpečnostním prvkům patří:

- integrovaná funkce protokolárního výmazu dat
- LUN Security pro řízení přístupu k LUN na základě WWN
- software Write Once Read Many (WORM) pro dlouhodobé uchovávání dat se zajištěním jejich nezměnitelnosti
- přístup podle rolí
- logování historie všech uživatelských přístupových operací provedených v systému
- Fibre Channel Secure Protocol Authorization A (FC-SP Auth A) pro autorizaci subjektů podle protokolu Fibre Channel
- podpora pro šifrovací zařízení jako NeoScale a Decru

Hitachi je jediným dodavatelem na trhu, který u svých produktů nabízí záruku 100% dostupnosti dat. Toto vše zajišťuje významné zkrácení času a minimalizaci úsilí potřebného k zálohování dat a ke vzdálené replikaci.

VEZMĚTE SI JEN TAKOVÉ SOUSTO, NA KTERÉ STAČÍTE

Minimalizace nákladů představuje rozhodně velkou výzvu. Tajemství úspěchu spočívá v identifikaci klíčových oblastí, kde je potřebné nebo možné provést zlepšení a pak najít nejlepší způsob, jak svého cíle dosáhnout. Může to být zavedením virtualizace či definováním lepších řídicích procesů u existující architektury. V oblasti paměťových systémů je to otázka identifikace slabých míst a nalezení způsobů, jak je odstranit.

Hitachi Data Systems

Nová generace systémů Hitachi TagmaStore USP V – nové možnosti realizace datové infrastruktury

V červnu 2007 byla společností Hitachi Data Systems uvedena na trh nová generace diskových polí pod názvem Hitachi TagmaStore USP V. Názvem se výrobce přihlásil k velmi úspěšné tradici předchůdce tohoto systému – zkratka USP, která pochází z anglického Universal Storage Platform, se v uplynulých třech letech stala symbolem kvality i stability těch nejvýkonnějších diskových systémů a zároveň značkou produktu, který rychle, efektivně a především bez rizika umožnil integrovat diskové kapacity různých výrobců pod jeden management. Systémy Hitachi TagmaStore USP se tak staly tou nejlepší odpovědí na výzvu implementace tzv. tierované storage, kterou přinesl rozvoj informačních technologií. To učinilo společnost Hitachi nejúspěšnějším dodavatelem v oblasti řešení tierované storage a tyto produkty našly pochopitelně své uplatnění i v instalacích v České republice.

Společnost Hitachi přišla v tomto směru s velmi jednoduchým, robustním, a proto spolehlivým řešením. Umožnila všem diskovým polím, která uživatel provozoval, aby své kapacity – dříve připojené a poskytované serverům – připojili do diskového pole Hitachi TagmaStore USP. Servery pak komunikují pouze s jedním polem (Hitachi TagmaStore USP), které jim poskytuje jak svou vlastní diskovou kapacitu, tak i kapacitu do něj napojených diskových polí (tj. externí kapacitu).

Controller	
Basic platform packaging unit: Integrated Control/ /Array Frame and 1 to 4 optional Array Frames Universal Star Network Crossbar Switch	
Number of switches	4
Data bandwidth (GB/sec)	68
Control bandwidth (GB/sec)	38
Aggregate bandwidth (GB/sec)	106
Cache Memory	
Boards	32
Board Capacity (GB)	4 or 8
Maximum (GB)	256
Control Memory	
Boards	8
Board Capacity (GB)	4
Maximum (GB)	32
Front-end Directors (Connectivity)	
Boards	1–14
Fibre Channel host ports per board	8 or 16
Maximum Fibre Channel host ports	224
Virtual host ports	1,024 per physical port
Maximum FICON host ports	112
Maximum ESCON host ports	112
Logical Devices (LUNs) – Maximum Supported	
Open systems	65,536
IBM® z/OS®	65,536

Hard disks (GB)	
Type (Fibre Channel)	73, 146, 300
Number (minimum/maximum)	4–1152
Spare drives per system (minimum/maximum)	1/16
Internal raw capacity (TB)	
Minimum (73GB disks)	82TB
Maximum (300GB disks)	332TB
Maximum usable capacity–RAID-5 (TB)	
Open systems	288
z/OS-compatible	270
Maximum usable capacity—RAID-6 (TB)	
Open systems	247
z/OS-compatible	231
Maximum usable capacity—RAID-1+ (TB)	
Open systems	165
z/OS-compatible	144
External storage support	
Maximum internal and external capacity	247PB
Virtual Storage Machines	32
Standard Back-end Directors	1–8
Operating system support	
Mainframe: Fujitsu MSP; IBM OS/390®, MVS/ESA™, MVS/XA™, VM/ESA®, VSE/ESA™, z/OS, z/OS.e, z/VM®, zVSE™; Red Hat Linux for IBM S/390® and zSeries®; TPF	
Open systems: HP (HP-UX, Tru64, Open VMS), Sun Solaris, IBM AIX®, Microsoft® Windows (2000, 2003 Server), Novell NetWare, Red Hat and SuSE Linux, VMWare ESX	

Note: All capacities are based on 1GB = 1,000,000,000 bytes; 1TB = 1,000GB

Paralela s budováním SAN je jistě namístě, ale jsou zde dva zásadní rozdíly. Diskové pole, které do sebe integrovalo externí kapacity, je vybaveno řadou softwarových nadstaveb, které byly provozně odzkoušeny na předchozích modelech, a disponuje řádově vyšším výkonem. Takže kromě propojení se celému diskovému prostoru dostalo výkonu i provozně odzkoušené funkcionality tvorby datových klonů, snapshotů, vzdálených replikací atp. Navíc bylo možné využít stejný software pro klonování dat, vzdálené replikace atp. mezi kapacitami umístěnými na diskových polích různých výrobců. Takto vytvořené prostředí disponuje datovými oblastmi s různými SLA (Service Level Agreement). Vzhledem k jednotnému managementu bylo snadné do něj aplikovat produkty on-line migrace dat mezi datovými tiery, a tak vznikl stabilní a výkonný prostředek pro efektivní aplikaci tierovaného datového prostoru.

Společnost Hitachi tímto krokem předložila uživatelům reálný koncept výkonného a přitom spolehlivého tierovaného prostředí, které navíc zvýšilo ochranu investic (při nákupu nové technologie nebylo nutno starou technologii vyřadit, ale bylo ji možné integrovat do nového prostředí).

PŘÍNOSY NOVÉ GENERACE

Zdálo by se, že vše podstatné již bylo předchozím modelem vyřešeno. Nová generace Hitachi TagmaStore USP V však přináší další kvalitativní krok vpřed. Uživatelé nového systému totiž mohou využívat funkci **Hitachi Dynamic Provisioning**. Tato nová vlastnost opět reaguje na nastalou situaci. Řada aplikací totiž vyžaduje kontinuální rozvoj svého datového prostoru, ale mnoho případů přidání dodatečných diskových kapacit aplikaci vyvolává řadu aktivit administrátorů aplikací, databází i serverů, omezení chodu produkce a s tím spojená provozní rizika. Je proto vhodnější jednorázově poskytnout aplikaci datový prostor s dostatečnou kapacitní rezervou, která by rizika a vícepráce spojené s postupným přidáváním kapacit eliminovala. Tento přístup však až dosud vyžadoval vyšší náklady na pořízení a provoz diskového systému (nákup hardwaru a softwaru, servisní a licenční poplatky, energie...). Hitachi Dynamic Provisioning však tento rozpor vyřešil. Dokázal skloubit výhody přiřazení velkého prostoru a eliminovat dříve z toho plynoucí zvýšené náklady. Princip je jednoduchý – **každé aplikaci je možno přiřadit rozsáhlý prostor diskových kapacit, který je však realizován jen na takové fyzické diskové kapacitě, která odpovídá aktuálním potřebám aplikace**. Pokud potřeby aplikace rostou, je administrátor diskového pole včas vyrozuměn o potřebě přidat dané aplikaci další fyzickou kapacitu. Toto přidání zajišťuje jen administrátor diskového pole Hitachi TagmaStore USP V prostředky tohoto pole, a to bez jakéhokoli negativního vlivu na server, jeho operační systém, databázi či aplikaci.

Tento krok vedoucí k dalšímu snižování provozních rizik spolu se snižováním nákladů je pochopitelně doprovázen řadou technických vylepšení diskového systému, jakými jsou např.:

- plná aplikace 4Gb/s technologie
- zvýšený počet FC portů
- zvýšený výkon
- schopnost spravovat až stovky PB (1 PB = 1 000 TB) datového prostoru

atp.

Ti z vás, kteří se zajímají o technické podrobnosti diskového pole Hitachi TagmaStore USP V, najdou odpovědi na své otázky v připojené tabulce nebo u společnosti MHM computer (www.mhm.cz), která v Praze provozuje Kompetenční centrum pro produkty a služby Hitachi Data Systems (www.hds.com).

Petr Blažej

Vážně musíte JÍT do obchodu?

http://shop.mhm.cz

Pohodlný nákup komponentů pro SAN a paměťových systémů

DILIGENT TECHNOLOGIES, BROCADE, EMULEX, Sun, ca, HITACHI Inspire the Next, CISCO, Quantum, BULL, TANDBERG DATA Securing your Information

MHM Služby pro vaše data

MHM computer s.r.o.
U Pekáren 4/1309, 102 00 Praha 10-Hostivař
tel.: +420 267 209 111, fax: +420 267 209 222
e-mail: office@mhm.cz, www.mhm.cz

Data Storage Workshop 2007

Rok se sešel s rokem a blíží se další ročník konference a výstavy Data Storage Workshop (DSW). 2. ročník DSW proběhne 25.–26. září v konferenčním centru hotelu Olympik Artemis v Praze.

Téma správy, zálohování a archivace dat je stále velmi aktuální. Množství dat vygenerovaných jednotlivými společnostmi stoupá, a tak se zabezpečení dostupnosti, integrity a datové bezpečnosti stává klíčovým pro chod celé firmy, a tedy úkolem pro mnoho IT manažerů.

Konference a výstava Data Storage Workshop nabízí možnost najít efektivní řešení, jak data ukládat, archivovat i spravovat. Během dvou dnů budou mít návštěvníci příležitost zhlédnout řadu zajímavých přednášek i se seznámit s jednotlivými řešeními a technologiemi na doprovodné výstavě.

Mezi hlavní témata letošního ročníku budou patřit Data Management – správa a konsolidace dat, plány obnovy po havárii, zálohování dat, přínosy storage technologií a SOA (Service-Oriented Architecture) pro vaše podnikání. Součástí programu budou i praktické ukázky a případové studie jednotlivých řešení.

Konferenci a výstavu pořádá společnost Exponet s generálním partnerem společností Emwac Group a s hlavním partnerem, společností Hitachi Data Systems, i s partnery – společnostmi MHM computer a Convenio consulting.

V bohatém programu vystoupí také odborníci z předních firem v oboru, jakými jsou např. Deltax Systems, Silicon Graphics, Storyflex, Gapp, Rekonix, Agora plus a další.

Data Storage Workshop se koná pod záštitou oborové organizace The Storage Networking Industry Association SNIA Europe.

Další informace a možnost registrace na www.dsw.cz.

Po předregistraci vstup zdarma!

KUP EGAP: Data pod dohledem

Komerční úvěrová pojišťovna EGAP, a. s., (dále KUPEG) zahájila svoji činnost 1. 10. 2005 jako dceřiná společnost Exportní garanční a pojišťovací společnosti, a. s., (dále jen EGAP) a jako největší česká komerční úvěrová pojišťovna. Budování samostatného informačního systému (dále IS) společnosti KUPEG započalo v dubnu 2005. Převzata byla pouze část pojistného systému Incredit, která je dále vyvíjena externí organizací.

Vzhledem k omezenému počtu pracovníků IT bylo zapotřebí navrhnout progresivní řešení, které by splňovalo vysoké požadavky na komfort a kvalitu služeb poskytovaných našim uživatelům i zákazníkům. V této první fázi budování IS byla použita virtualizační technologie na serverové platformě, RSA tokeny namísto klasických hesel, kvalitní Document Management System a spolehlivá podniková aplikace. Požadována byla maximální možná integrace mezi aplikacemi a externími databázemi, centralizovaná správa aplikací a v neposlední řadě i dálkový přístup pro všechny zaměstnance z jakéhokoli místa, kde je dostupné internetové připojení.

Použité technologie a nabízené služby mohou vypadat krásně a velmi užitečně, ale bez náplně, tj. vlastních dat a jejich plné dostupnosti, jsou zcela zbytečné. Přestože veškerá obchodní data, a to i na vstupu v KUPEG (např. v elektronické podatelně), jsou uchovávána v digitální podobě, objem dat se zatím pohybuje pod 1 TB. Objem ani technické požadavky na výkon tedy nebyly nejdůležitějšími kritérii pro nákup datového úložiště. Tím se stala ochrana dat a jejich snadná dostupnost. Jediná námi požadovaná technologie bylo SAN pole, a to i s požadavkem na plné využití virtualizačních technologií VMware (VMotion, nyní i DRS a HA). Dalším požadavkem byla možnost vzdálené on-line replikace dat do záložní lokality.

NASAZENÍ SAN POLÍ

Technologie SAN polí byla společností MHM computer úspěšně nasazena a spravována již v mateřské společnosti EGAP. Pro KUPEG byla vybrána produktová řada polí Hitachi Thunder 9570V. Nabídka se vyznačovala příznivou cenou, nadstandardní zárukou a poměrně variabilním systémem vhodným k dalšímu rozšiřování. Důležitým argumentem bylo i dohledové centrum MHM computer a příznivé reference od ostatních zákazníků.

Ke konci roku 2006 začala druhá fáze budování IS spočívající ve vytvoření záložní lokality. Zde již byla navržena diverzifikace mezi levnějšími a pomalejšími disky a dražšími a rychlejšími disky jak v centrále společnosti, tak i na druhém systému v záložní lokalitě. Některé disky byly navrženy v zapojení RAID10 oproti používanému zabezpečení na úrovni RAID5. Dalším krokem bylo zvolení diskových oblastí pro on-line replikace. V této přípravné části probíhaly konzultace mezi KUPEG a MHM computer, jejichž výsledkem byl návrh topologie a konečná nabídka řešení.

Z výše uvedených důvodu bylo nutné přistoupit k celkové rekonfiguraci stávajícího řešení SAN. Rekonfigurace datových polí probíhala přes celý jeden víkend a byla úspěšně dokončena uvedením obou SAN polí do ostrého provozu.

Společnost MHM computer nám navíc pomohla s oslovením poskytovatelů datových okruhů, posouzením jejich nabídek a dodala a implementovala druhé datové pole SAN včetně nastavení on-line replikací dat. Zároveň vůči KUPEG vystupuje MHM computer jako dodavatel datových okruhů a backupových řešení. To nám umožňuje částečně přenést problematiku dat a jejich poskytování na bedra pouze jediné společnosti a řešit či konzultovat tuto zásadní oblast jako jeden celek. Jak je patrné, patří MHM computer ke klíčovým dodavatelům KUPEG.

Ing. Radek Pohnán,
Komerční úvěrová pojišťovna EGAP, a. s.

O Komerční úvěrové pojišťovně EGAP, a. s.

Komerční úvěrová pojišťovna EGAP, a. s., poskytuje komerční úvěrové pojištění a je jedničkou na českém trhu. Na tomto trhu začala působit již v roce 1992, tehdy jako součást společnosti EGAP, státem plně vlastněné pojišťovny zaměřené na pojišťování vývozních úvěrů. Posláním společnosti je pomocí pojištění pohledávek poskytovat ochranu podnikatelům před riziky nezaplacení, aby se mohli v plné míře věnovat klíčovým činnostem, jako je výroba nebo obchod.

EGAP Komerční úvěrová pojišťovna EGAP, a.s.

Využití systémů Hitachi pro vybudování záložní lokality

KUP EGAP je jednou ze společností, které replikují svá data do záložní lokality vybudované na technologii Hitachi. Co to vlastně je záložní lokalita a jaká je její podstata?

Záložní lokalita představuje geograficky vzdálené IT prostředí, které obsahuje plnou kopii všech důležitých systémů a dat. V případě nenadálého, nepředvídatelného výpadku produkční lokality (požár, povodeň, vichřice, atd.) je společnost disponující záložní lokalitou schopna během okamžiku zprovoznit svoji kompletně funkční IT infrastrukturu v záložní lokalitě. Aby byl přesun funkce produkční lokality do záložní lokality (tzv. failover) vůbec možný, musí být nejprve zajištěn přesun dat. Navíc musejí být data v záložní lokalitě v použitelném, tzv. konzistentním stavu. Tuto nejdůležitější funkci v případě technologií Hitachi zastává software TrueCopy.

CO UMÍ TRUECOPY

TrueCopy umožňuje vzdálenou replikaci dat mezi diskovými poli Hitachi. Produkční data z produkčního diskového pole jsou synchronně nebo asynchronně replikována do záložní lokality. Replikace dat může být obousměrná (tzv. bidirectional), což dovoluje také replikovat data ze záložní lokality do produkční lokality. Produkční data a záložní data tvoří tzv. TrueCopy pár. Jakákoliv změna produkčních dat je aplikována i na záložní data. Konzistentní záloha produkčních dat v záložní lokalitě vznikne rozpojením (tzv. splitnutím) daného TrueCopy páru. Software TrueCopy je navržen tak, aby proces vytvoření zálohy nebo obnovy produkčních dat trval co nejkratší dobu. Proto, jakmile je TrueCopy pár rozpojen (vznik zálohy produkčních dat), si obě diskové pole (produkční i záložní) uchovávají informaci o tom, která data na jejich straně (produkční, záložní) byla změněna. V případě další zálohy nebo obnovy produkčních dat se tak kopírují pouze data změněná od předchozí zálohy, což celý proces zálohy nebo obnovy značně urychluje.

Proces vytvoření zálohy produkčních dat v záložní lokalitě je pro produkční servery zcela transparentní. To znamená, že výkonnost produkčních serverů není zálohovacím procesem nikterak poznamenána. Vytvoření zálohy je otázkou zlomku sekundy, což významně zkracuje tzv. backup okno. TrueCopy umožňuje propojit produkční a záložní lokalitu nejen pomocí nákladného optického FC (Fibre Channel) spojení, ale také přes FCIP (Fibre Channel over IP) nebo iFCP (Internet Fibre Channel Protocol) spojení, čímž výrazně snižuje celkové investiční náklady. Dalším obrovským přínosem TrueCopy pro zákazníky je skutečnost, že tento produkt umožňuje mezi sebou propojit jakýkoliv AMS/WMS systém. To v praxi znamená, že záložní lokalita může být vybavena klidně tím nejlevnějším diskovým polem Hitachi, bez ohledu na to, jaké diskové pole je v produkční lokalitě. Výsledkem nasazení řešení Hitachi TrueCopy je maximální bezpečnost, spolehlivost a dostupnost firemních dat s maximální minimalizací TCO.

Záložní lokalita představuje řešení, které minimalizuje ztráty v případě rychlých, nenadálých havárií. Aby bylo vůbec možné řešení záložní lokality vytvořit, je zapotřebí vybudovat dobré základy IT prostředí, které to umožní. Technologie Hitachi jsou těmi pravými nosnými základy vašeho IT prostředí.

Radim Petržela

Neriskujte nedostupnost e-mailů!

V současné době již budeme jen obtížně hledat společnost nebo úřad, který by si bez ICT dokázal představit svůj provoz. Convenio Consulting vypracovala celou řadu analýz potřeb u svých zákazníků a u celé řady z nich vytvořila disaster recovery plány. Jednou z nejdůležitějších služeb poskytovaných ICT oddělením uživatelům se ukazuje být e-mail. Takové zjištění pro nás není nijak překvapivé; právě naopak – potvrzuje naše odhady ohledně vnímání důležitosti jednotlivých aplikací uživateli.

Běžně se setkáváme s požadavky na dostupnost e-mailové služby v řádech jednotek hodin nebo i desítek minut. Zajistit tuto dostupnost pro větší počet e-mailových schránek již není možné běžně používanými postupy. U klasického řešení, kdy je e-mailový server umístěn na jednom, byť výkonném serveru a v nočních hodinách probíhají zálohy na pásku, se čas obnovy po havárii může pohybovat i v řádu desítek hodin. Na první pohled může tento odhad vypadat až příliš pesimisticky, ale pojďme si spočítat čas obnovy, který by byl spojen s větší závadou pouze tohoto jednoho serveru:

- Dodání nového serveru, případně jeho oprava – minimálně 8 hodin
- Instalace operačního systému a jeho nastavení – 3 hodiny
- Instalace aplikací a jejich nastavení – 3 hodiny
- Obnova dat z pásek – 4 hodiny

Uvedli jsme příklad, kdy dojde k výpadku jen jednoho serveru a veškerá ostatní infrastruktura je plně funkční. Pokud by došlo k závadě rozsáhlejší, například k vyhoření jednoho racku, kde by byly i další komponenty potřebné pro chod sítě, začnou časy dramaticky narůstat. Pokud je tedy pro vaši společnost důležitá dostupnost e-mailů za každých okolností, je nezbytně nutné vybudovat podstatně robustnější architekturu celé e-mailové služby.

Pro splnění požadavku organizace na vysokou dostupnost e-mailové komunikace se nabízí několik řešení. Tyto varianty vycházejí ze skutečně potřebné dostupnosti, z možností organizace (lokální, geografické, transkontinentální clustery) a v neposlední řadě z finančních možností. Zvýšená dostupnost e-mailu v prostředí Microsoft Exchange vychází ze zdvojování či vícenásobení jednotlivých komponent potřebných pro běh Exchange. Pokud se podíváme na potřebné komponenty ze strany perimetru sítě, tak to jsou:

- Firewall
- Front-end Exchange Server
- Back-end Exchange Server
- DNS server
- Active Directory server
- Diskový prostor
- Backup server
- Monitorovací server

První komponentou celé infrastruktury na „hraně“ podniku je firewall. Pokud se budeme zabývat vysokou dostupností, nesmíme zapomenout také na samotnou bezpečnost celého e-mailového řešení. Bezpečnost jsme schopni zajistit firewally, ať v podobě Microsoft ISA serveru nebo s využitím zařízení jiných výrobců, jakými jsou např. Check Point, Cisco… I zde platí, že by měla být zachována redundance. Z pohledu ochrany sítě proti napadení je vhodné zkombinovat různé druhy, nejlépe různé výrobce těchto zařízení, čímž se zabrání stavu, kdy případná chyba v softwaru umožňující napadení sítě si vynutí vypnutí provozu na vstupním perimetru sítě a způsobí nedostupnost e-mailových služeb.

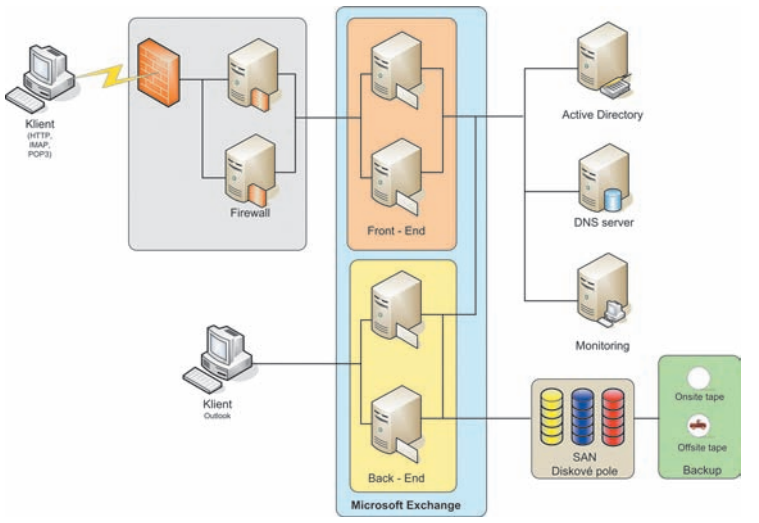


Schéma řešení vysoce dostupné Exchange infrastruktury.

Další, ne však poslední komponentou v e-mailovém řešení je samotný Exchange server. Pro větší počet uživatelů a zajištění vysoké dostupnosti se rozděluje na front-end a back-end servery. Front-end servery zajišťují sběr a vyřízení požadavků od všech autentizovaných uživatelů. Tyto servery jsou clusterovány do Network Load Balancing (NLB) clusteru. Back-end servery mají za úkol zajištění dostupnosti a konzistence uživatelských dat. Na těchto serverech jsou uloženy všechny e-mailové schránky uživatelů. Tyto servery jsou clusterovány do „share-nothing“ clusteru. Výkonnost back-end serverů je hodně závislá na datových úložištích, na kterých jsou data Exchange (mailboxy, logy…) provozována.

Dalšími dvěma nepostradatelnými komponentami celého Exchange řešení jsou DNS server a doménový controller Active Directory server. U těchto dvou částí nikdo nepochybuje, že je nutné je mít v clusteru, protože z hlediska služeb založených na technologiích Microsoftu jde o dvě klíčové služby, bez kterých neběží nic ostatního.

Velmi důležitou součástí je diskový systém. Je nutné, aby byl schopen zaručit dostatečnou ochranu dat i výkon, a tím i odezvu back-end serverům. Diskovým systémem u většiny vysoce dostupných instalací Exchange rozumíme diskové pole připojené na SAN (Storage Area Network). U diskového pole je nutné zaručit komunikaci mezi polem a Ex-

change serverem i v případě vzdáleného zrcadlení dat mezi dvěma geograficky oddělenými lokalitami. Exchange je stejně jako každá jiná databáze náchylná na chyby v konzistenci dat. V některých případech daleko náchylnější než Oracle nebo SQL. Proto pro některé dodavatele storage systémů může být problém zaručit konzistentní kopie Exchange databází na dvou či více oddělených lokalitách.

Po diskovém poli nesmíme zapomenout ani na backup. Zálohování může být prováděno do diskových nebo páskových prostor. Nejvhodnější je kombinace obou, kdy diskové zálohy jsou využívány pro rychlou obnovu uživatelských mailboxů nebo samotných e-mailů. Tato úroveň zálohování závisí na možnostech softwaru používaného pro backup. Uvedené zálohy jsou používány pro opravu uživatelských chyb. Druhým typem zálohy, tedy na pásky, je archivace pro účely disaster recovery všech středisek a nutnosti jejich obnovy.

Celkový výkon a způsob řešení vysoce dostupného Exchange řešení nezávisí pouze na počtu serverů, ale také na konfiguraci domény celé organizace. Doména organizace může být typu „single forest“, tedy jeden les pro celou organizaci. V tomto případě jsou mailboxy i uživatelé v jednom doménovém lese. Dalším modelem je „dedicated Exchange forest“, kde je vytvořen jeden doménový les pro běh Exchange včetně hostování mailboxů a jiný, oddělený les, je určen pro uživatelské účty, které jsou s mailboxy propojeny. Posledním modelem, který je využíván ve velkých nadnárodních organizacích, je několik lesů, kde každý má vlastní Exchange služby a tyto lesy jsou vzájemně propojeny.

Architektura ICT je vysoce individuální záležitost. Výše uvedená řešení nemají obecnou platnost a není možné je implementovat stejně v každé společnosti. Vždy je zapotřebí zvážit konkrétní požadavky dané organizace, její současnou ICT infrastrukturu, návazné aplikace nebo i lokalitu, možná rizika s ní spojená a případně potřebu vybudování záložní lokality.

Convenio Consulting vám nabízí služby zkušených konzultantů, pro které jsou tato řešení „denním chlebem“ a kteří vás dokáží provést rychle celým procesem. Významnou přidanou hodnotou nabízených konzultačních služeb může být i přesná specifikace potřebných komponent, která vám výrazným způsobem pomůže při organizaci výběrového řízení.

Pokud vás tato problematika zaujala, můžete se již nyní přihlásit na workshop „Jak komunikovat e-maily za každé situace?“, který se bude konat 20. 9. 2007. Bližší informace najdete na www.convenio.cz. Přihlášky, stejně tak jako dotazy k této problematice, posílejte na e-mail office@convenio.cz.

Miroslav Teichman, Michal Hrdlička

Convenio Consulting poskytuje analýzy, technologické testy, konzultace, školení, workshopy.

1. Plány obnovy po havárii (Disaster Recovery plány, Business Continuity, Risk Management)
2. Sladění požadavků organizace a ICT infrastruktury
3. Návrh architektury vysoce dostupných systémů
4. Návrh optimalizace zálohování dat
5. Vypracování ICT strategie organizace
6. Tvorba zadání a vyhodnocení výběrových řízení
7. Optimalizace nákladů na ICT infrastrukturu
8. Ochrana osobních údajů

Semináře:

- 20. 9. 2007 Jak komunikovat e-maily za každé situace?
- 2. 10. 2007 Business Continuity

Registrujte si své místo včas, počet míst je omezen!

Convenio Consulting ‣ odštěpný závod MHM computer s.r.o. ‣ U Pekáren 4/1309
102 00 Praha 10 - Hostivař ‣ telefon: +420 267 209 111 ‣ fax: +420 267 209 222
e-mail: office@convenio.cz ‣ www.convenio.cz

CONVENIO CONSULTING

Roadshow

Data v péči LIVE

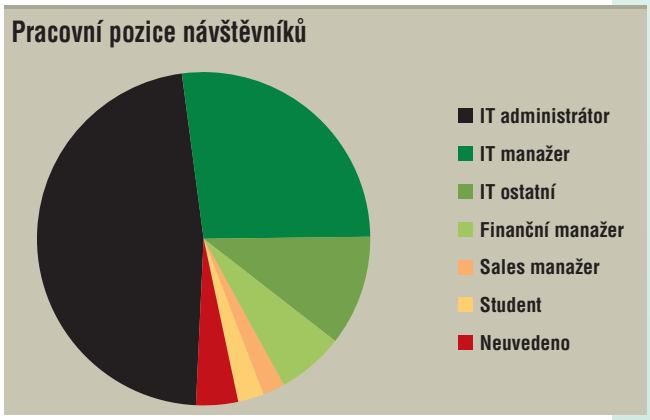
Vybraná města České republiky hostila v průběhu června roadshow Data v péči LIVE. Tento seriál přednášek představil moderní trendy v oblasti ukládání dat a péče o ně. Obsah každého dne roadshow byl rozdělen na tři hlavní části. V té první jsme se věnovali ukládání dat teoreticky. Přednášející vysvětlovali, proč ukládání dat působí problémy, a popisovali důsledky podcenění tzv. datového problému. Druhá část byla zaměřena na ekonomiku péče o data. Zásadním mottem této části byla diskuse o různých způsobech snížení nákladů na výstavbu datové infrastruktury podniku tak, aby optimálně sloužila organizaci. Třetí, poslední část byla věnována výhradně technologickým postupům. Názorně – v podobě živých ukázek konsolidace dat, rychlého obnovení dat a kompletního geografického clusterového disaster řešení – zde bylo předvedeno, jak správně pečovat o data. Zlatým hřebem této praktické části byla destrukce produkční roadshow lokality a následný automatický přesun (tzv. failover) všech produkčních systémů, aplikací a dat do záložní roadshow lokality. Pragmaticky bylo vysvětleno, že pokud o svá data pečovat nebudeme, tak o ně dříve nebo později přijdeme!

Management podniku chce vždy vědět, kolik ho budou stát informační technologie. Zároveň má o nich a o jejich možnostech často jen zkreslené představy. U typických IT profesionálů je tomu však přesně naopak. Roadshow dala oběma stranám možnost pochopit význam IT procesů a jejich „cenu“.

Klíčovou roli hrálo v rámci roadshow spojení know-how s technologiemi. Nutnou součástí proto byly racky obsahující disková pole, servery, switche apod., které putovaly po České republice a sloužily k praktickým ukázkám konsolidace, zálohování dat a clusterového řešení. Každý z racků vážil více než 200 kilogramů, a proto pro ně bylo nutné zajistit speciální přepravu. Díky technologickým partnerům akce, společnostem MHM computer, Hitachi a Bull, bylo možné přímo na místě demonstrovat přínosy vyspělých produktů.

Poděkování patří všem partnerům akce, technologickým i mediálním, kteří přispěli nejen k náplni setkání, ale také pro účastníky zajistili doplňující informační materiály.

Zájem o přednášky byl značný. Účastnili se jich jak odborníci z nejrůznějších pozic s převažující IT specializací, tak i finanční nebo provozní manažeři. Logicky největší účast přineslo setkání v Praze a v Brně, příjemná komorní atmosféra provázela prezentaci v Plzni. Celkem se zúčastnilo téměř 200 posluchačů.



Velký zájem a nepochybný úspěch je pro nás zavazující pro nadcházející rok. Roadshow zamíří nejen do tradičních měst, jako tomu bylo letos, ale nezapomene ani na místa nová. Obsahově se rozšíří o příspěvky technologických partnerů, které vhodně doplní její bohatý program. Těšíme se tedy na setkání v příštím roce!

Naďa Barešová

Fakta o MPIO Microsoftu

Nedílnou součástí všech prostředí zaručujících vysokou dostupnost dat (někdy také označovanou jako „pětidevítkovou“ – 99,999%) jsou řešení Multi Path I/O, zkráceně MPIO. MPIO řešení znamená, že aplikační část systému může své read/write operace posílat do datového úložiště po více datových cestách. Při výpadku používané datové cesty dochází k automatickému přesměrování (tzv. failoveru) I/O operací na další dostupnou datovou cestu, a tím k zachování dostupnosti dat. Moderní řešení MPIO umožňují také rozložit celkovou zátěž vstupně/výstupních operací na všechny datové cesty (loadbalancing), a tím zvýšit celkovou propustnost systému. Funkce failoveru a loadbalancingu spolu vzájemně spolupracují tak, aby byla vždy zaručena maximální dostupnost a propustnost dat v závislosti na počtu funkčních datových cest.

Kompletní MPIO řešení se skládá z hardwarové a softwarové části. Hardwarová část představuje fyzické datové cesty a tvoří ji redundantní hardwarové komponenty (adaptéry HBA, switche, kabely), které propojují aplikační část systému s datovým úložištěm. Softwarová část konsoliduje všechny fyzické datové cesty do jedné virtuální datové cesty a stará se o loadbalancing a failover. Programová část je buď přímo implementována do operačního systému, nebo se o ni stará software třetích stran. Bohužel ani jedna z těchto implementací softwarové části MPIO není ideální.

Pokud software pro MPIO pochází přímo od dodavatele diskového pole, máme zaručenu maximální kompatibilitu a výkonnost s dodávaným diskovým polem, ale jen velmi křehkou kompatibilitu s použitým operačním systémem. Tato subtilní kompatibilita je dána velice povrchní znalostí o fungování operačního systému a může být kdykoliv narušena rutinními úkony, jako jsou například instalace bezpečnostních oprav nebo service packů. Jejich další nevýhodou je, že nutí zákazníka zůstat pouze u jednoho dodavatele technologií SAN (Storage Area Network), protože heterogenní prostředí není a kvůli kompatibilitě ani nemůže být podporováno.

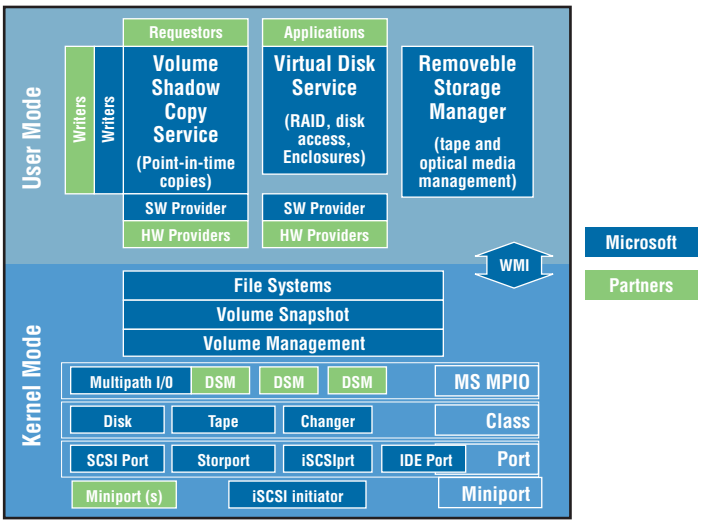
Na druhé straně software pro MPIO, který se nachází v jádru operačního systému, zaručuje jeho maximální stabilitu a funkčnost, ale neumí efektivně využívat všech dostupných funkcí připojeného diskového pole. Je to opět dáno pouze orientační znalostí funkčnosti použitého diskového pole.

Společnost Microsoft si uvědomovala výše uvedené nedostatky i jejich negativní dopady na uživatele a přišla s myšlenkou rozdělit softwarovou součást MPIO na dvě části. První představuje rozhraní MPIO, které je implementováno přímo v jádru operačního systému Windows. Toto rozhraní se vyvíjí spolu s operačním systémem Windows, čímž je zaručena jeho maximální stabilita. Komunikačním protějškem rozhraní MPIO jsou tzv. Device Specific Moduly (DSM), které dodají výrobci diskových polí tak, aby se maximálně využila funkcionalita použitého diskového systému. Aby Microsoft usnadnil výrobcům diskových polí práci, vytvořil „obecný“ DSM, který výrobce diskového pole pouze upraví podle svých potřeb a poskytovaných služeb. Obecný modul není součástí standardní instalace operačního systému Windows, ale výrobce diskových polí ho dostane v tzv. MPIO Diver Development Kitu (DDK).

POPIS ŘEŠENÍ

MPIO řešení postavené na modelu společnosti Microsoft zaručuje nejen maximální stabilitu operačního systému a využití všech specifických vlastností použitého diskového systému, ale také umožňuje administrátorům bezpečně pracovat v heterogenním prostředí. Jedno rozhraní MPIO může komunikovat s více DSM moduly, které reprezentují storage technologie různých výrobců.

MS Windows Server 2003 Storage Stack



Rozhraní MPIO je plně podporováno operačními systémy Windows 2000 Server, Windows Server 2003 a Windows Server 2003 R2. Rozhraní navržené Microsoftem rozhodně nezastává celou funkci MPIO řešení, ale je pouze jeho polovinou. Vždy musí být dodán správný DSM modul. Pouze potom je řešení MPIO úplné. Kompletní MPIO řešení tedy nedodává Microsoft, ale výrobce diskových systémů. To, že dodávané MPIO řešení využívá MPIO Microsoftu, zaručuje jeho certifikace a logo. V případě technologií Hitachi Microsoft certifikoval aplikaci Hitachi Dynamic Link Manager (HDLM), kterou lze použít ve spojení s diskovými poli Hitachi i EMC.

Detailní struktura kompletního MS Windows Storage Stacku je zobrazena na schématu. Modře jsou znázorněny komponenty spravované a vyvíjené společností Microsoft. Zeleně jsou vyobrazeny součásti dodávané třetími stranami. Všechny tyto kom-

ponenty musejí splňovat certifikační podmínky stanovené Microsoftem. Základní komponenty jádra a jejich funkce jsou následující:

- **Port Driver** – vytváří tzv. Physical Device objekty (PDO), které představují propojení příslušného zařízení s jeho sběrnicí. Spolu s class driverem zaručuje funkci PnP (Plug-and-Play). V prostředí Windows se můžeme setkat se dvěma typy těchto ovladačů: starší je SCSIport driver, novější se jmenuje storport driver a byl představen ve Windows Serveru 2003.
- **Miniport Driver** – každý storage adaptér je asociován se svým miniport driverem, který zastává pouze nezbytné operace, specifické pro daný hardware. Miniport Driver nevyvíjí Microsoft, ale je dodáván třetí stranou.
- **Class Driver** – vytváří tzv. Function Device objekty (FDO), které jsou prezentovány jako funkční celky vyšším vrstvám, uvedeným v modelu. Podílí se také na zajištění funkce PnP. Class Driver stejně jako Miniport Driver a Port Driver nejsou součástí rozhraní MPIO.
- **MPIO Drivers** – kolekce tří driverů pracujících na úrovni rozhraní MPIO. Tyto ovladače tvoří Multipath Port Filter Driver (mpspfltr), Multipath Disk Driver Replacement (mpdev.sys) a Multipath Bus Driver (mpio.sys).
- **Multipath Port Filter Driver** (mpspfltr) – transformuje standardní diskové identifikátory na jednoznačné identifikátory MPIO.
- **Multipath Disk Driver Replacement** (mpdev.sys) – Class Driver, který má za úkol „uzamknout“ vzniklý objekt PDO, převzít jeho vlastnictví a zabránit tak jeho vícenásobné interpretaci v systému. Absence tohoto driveru je zřejmá všem administrátorům Windows bez softwaru pro MPIO, kde je instance daného disku prezentována tolikrát, kolik existuje datových cest.
- **Multipath Bus Driver** (mpio.sys) – zajišťuje spojení tzv. root bus zařízení s hostitelským počítačem. Stará se také o funkci PnP a umožňuje monitorování a řízení asociovaných modulů DSM.
- **DSM** – poslední součástí MPIO jsou DSM moduly. Jejich úkolem je správně inicializovat připojená zařízení, loadbalancing, failover, opětovné zasílání I/O, které nemohly být v důsledku výpadku cesty správně doručeny. Každý DSM modul implementuje i monitorovací a řídicí funkci. Jako komunikační rozhraní se používá Windows Management Instrumentation (WMI).

Radim Petržela

Trocha počítačové historie

Začátek éry praktického využívání počítačů u nás spadá do konce 50. let minulého století. Od té doby se toho ve světě počítačů změnilo tolik, že si dnes už jen velmi málo lidí dokáže představit, jak tehdejší počítače vypadaly a jak se s nimi pracovalo. Pamětníků počítačových začátků pomalu ubývá a na druhé straně přibývá historek, které se k tomuto období sice vážou; někdy ale mají k realitě dosti daleko. Pokusme se tedy alespoň v kostce si tu dobu přiblížit.

Typickým představitelem tohoto počátečního období byly v Československu sovětské počítače Ural 1 a Ural 2. První Ural 1 k nám byl dovezen v roce 1958 a byl nainstalován na pracovišti Ústavu teorie informace a automatizace Československé akademie věd. Toto pracoviště také posloužilo jako hlavní zdroj informací o počítačích Ural a o jejich provozu pro tento článek.

Z dnešního pohledu se tehdejší počítače dodávaly jako „holé železo“. Nebyly vybaveny vůbec žádnými nástroji, které by usnadnily programování, tedy žádnými programovacími jazyky ani standardními podprogramy, natož pak operačním systémem. Nedokázaly zpracovávat abecední ani zvláštní znaky s výjimkou znaků plus a minus, uměly pracovat pouze s dvojkovými čísly, která se v psané formě kódovala osmičkově. Jediným programovým vybavením těchto počítačů byly testovací programy, které sloužily technikům údržby pro ověření základních funkcí počítače.

JAK URAL FUNGOVAL

Ural 1 pracoval s výjimkou operací s periferními zařízeními rychlostí 100 operací za sekundu. Bylo to dáno zejména jeho velmi neobvyklou operační pamětí – magnetickým bubnem, který se otáčel rychlostí 100 ot./s. Buben byl masivní válec, jehož poloměr měřil odhadem téměř 15 cm a výška činila kolem 6 cm. Za těchto podmínek neměli konstruktéři počítače prakticky žádný prostor pro podstatnější zvýšení otáček bubnu, a tím ani pro zásadnější zvýšení operační rychlosti počítače. I při těchto otáčkách byl buben jedním z nejzranitelnějších míst počítače. Kladl značné nároky na přesnost výroby, životnost ložisek a přesnost nastavení čtecích a zapisovacích hlav, které tvořily jeden kompaktní celek. Porucha ložisek nebo nastavení hlav znamenala totální havárii bubnu. Jakmile se v důsledku nějaké poruchy blok hlav dotkl povrchu bubnu, začaly hlavy působit jako tupý soustružnický nůž, který strhl magnetickou vrstvu a zakousl se do vlastního tělesa bubnu. Buben se zastavil, jeho motor shořel a bylo nutné obě součásti vyměnit. U Uralu 1, který k nám byl dovezen jako první, nastala popsaná havárie za dobu jeho provozu jednou.

Bubnová paměť měla kapacitu 2 048 samostatně adresovatelných 18bitových slov. Slova o délce 18 bitů byla určena pro uložení jednoadresových instrukcí. Aritmetické a logické operace však pracovaly s operandy, které měly dvojnásobnou délku 36 bitů. Takový operand byl uložen do dvou 18bitových slov na dvou po sobě jdoucích adresách. Aritmetické operace probíhaly v režimu s pevnou řádovou čárkou, která byla umístěna před nejvyšším dvojkovým řádem. Absolutní hodnota všech zobrazených čísel byla tedy menší než jedna. Pro praktické použití není zobrazení s pevnou řádovou čárkou vyhovující, takže si uživatelé Uralu 1 museli sami vypracovat podprogramy, které jim umožnily pracovat s čísly ve tvaru s pohyblivou řádovou čárkou (mantisa a exponent).

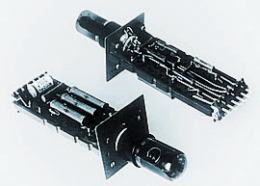
Prakticky každý uživatel počítače se musel naučit programovat. Některé programy pro řešení obecnějších problémů se objevily až později, např. v oboru výpočtů strojírenských nebo stavebních konstrukcí, ale i tak je většinou využíval poměrně úzký okruh spolupracovníků autora programu. Jak už bylo řečeno, s počítačem se nedodávaly žádné pomůcky pro programování, takže sestavit program znamenalo napsat do programového formuláře řádek po řádku posloupnost strojových instrukcí v absolutních adresách. Počítače Ural měly jednoadresovou koncepci instrukční sítě, takže každý řádek programu měl tvar šestimístného osmičkového čísla. Na prvních dvou místech byl zapsán kód operace, na dalších čtyřech adresa operandu. Většina aritmetických a logických operací však potřebuje dva operandy. Princip jednoadresového počítače je takový, že v počítači existuje zvláštní registr – střádač, jehož obsah slouží jako druhý operand, a po skončení operace se do střádače ukládá výsledek.

Pro ladění programů byl k dispozici prakticky jediný nástroj, a to byl ovládací pult počítače. Byl vybaven tlačítky, která umožňovala počítač spustit, zastavit a vkládat do počítače čísla i instrukce, a dále displejem, na němž doutnavky zobrazovaly obsah všech důležitých registrů počítače. Při ladění programátor procházel program z ovládacího pultu po blocích nebo i po jednotlivých instrukcích a kontroloval, co se v jednotlivých krocích děje.

Ural 1 byl počítač elektronkový. Základní počítačové obvody byly konstruovány s použitím elektronek a dalších prvků tehdejší klasické radiotechniky, odporů a kondenzátorů, které byly vzájemně propojeny letovanými drátovými spoji. Jedinými polovodičovými součástkami počítače byly hrotové a plošné diody, které tvořily hlavní stavební kámen logických obvodů. Vnitřek elektronkového počítače se tedy podobal vnitřku rozhlasového nebo televizního přijímače té doby. Rozdíl byl jedině v počtu použitých elektronek a ostatních radiotechnických součástek. Počet elektronek v Uralu 1 už byl v řádu stovek, počty ostatních součástek šly do tisíců; Ural 2 jich měl ještě mnohem víc. To samozřejmě vyžadovalo dát elektrickým obvodům nějaký konstrukční řád.

KONSTRUKCE POČÍTAČE

Konstrukční uspořádání počítače bylo skříňové, Ural 1 se skládal z pěti skříní vysokých asi dva metry. Ve spodní části skříní byly uloženy napájecí zdroje, před prostřední skříní byl umístěn ovládací pult. V horní části skříní byly vestavěny konektory, do nichž se po vodicích lištách zasunovaly typové elektronické obvody, umístěné na standardizované desce. Na přední části desky byl umístěn malý panel, jehož rovina byly kolmá k rovině desky a do něhož byla vestavěna patice pro zasazení elektronky.



Rozvod hlavních řídicích signálů, které musely být k dispozici ve všech skříních, se uskutečňoval soustavou sběrnic (měděných vodičů) natažených v nejhornější části každé skříně. Když se při instalaci počítače usadily jednotlivé skříně vedle sebe, propojovaly se sběrnice mezi skříněmi drátěnými spojkami, které se ke sběrnicím připájely.

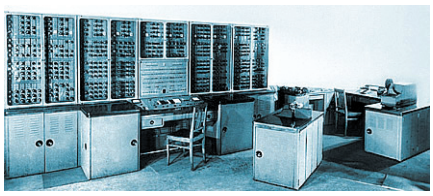
Pro vstup dat se u počítačů Ural používal snímač děrné pásky. Jako páska sloužil klasický černý perforovaný kinofilm 35 mm, do něhož se děrovaly obdélníkové otvory podobně jako do děrného štítku. Páska se nakonec slepila do nekonečné smyčky. Data se snímala po blocích, každý blok byl na pásce vyznačen vyděrovaným číslem bloku. Manipulace s děrnou páskou, zejména opravy chyb, nebyla ničím příjemným. Uměním bylo už jen vadné políčko na dlouhé pásce najít. Nalezená chyba se pak opravovala tak, že se chybějící otvor doděroval ručním děrovačem, kdežto otvor navíc se pečlivě zalepil jedním z okének, která vznikala při děrování pásky.

Funkci vnější paměti plnila magnetopásková jednotka. Samotná páska – jako médium – byla opět tvořena perforovaným kinofilmem, tentokrát potaženým magnetickou vrstvou a slepeným opět do nekonečné smyčky. Tato nekonečné smyčka se vkládala do magnetopáskové jednotky, která byla téměř identická se snímačem děrné pásky. Rozdíl byl pouze v tom, že fotodiody děrnopáskového snímače byly až na jednu výjimku nahrazeny blokem magnetických hlav. Poněkud kuriózním důvodem zmíněné výjimky byl fakt, že i vnější pásková paměť pracovala s daty uspořádanými do bloků, číslo bloku se však na pásku nezaznamenávalo magneticky, ale děrovalo se do ní. Aby se přečetlo, nějaká fotodioda tam zůstat musela.

Ural 1 disponoval číslicovou tiskárnou, která tiskla na každý řádek jedno osmičkové nebo desítkové číslo. Tisklo se na úzký pruh papíru pomocí typových lišt. Každý číselný řád měl v tiskárně svou typovou lištu, na níž byly umístěny typy číslic od 0 do 9. V klidu byly lišty zasunuty do výchozí polohy. Při operaci tisku se každá lišta vysunula tak, aby se na úroveň tištěného řádku dostal typ číslice, která se měla na daném řádu vytisknout. Operace skončila úderem kladívek, které typy nastavené v jednotlivých řádech otiskly přes barvicí pásku na papír. Rychlost tisku dosahovala 100 řádek za minutu. U tiskárny Ural 2 nahradil typové lišty rotující typový váleček, jehož osa byla rovnoběžná s tištěnou řádkou a číslicové typy byly rozmístěny po obvodu válečku. I zde se tisk uskutečňoval úderem kladívka. Použitím typového válečku se rychlost tisku zvýšila zhruba na desetinásobek, ale tisk měl horší kvalitu, řádky byly často roztřesené.

URAL PŘI PRÁCI

V ČSAV byl počítač v provozu nepřetržitě na tři směny od pondělního rána až do sobotního večera. Přestávka byla pouze v neděli. Ve dvou denních směnách se zpravidla ladily programy, noční směny sloužily převážně k výpočtům podle odladěných programů. Ranní směna začínala profylaktickou údržbou, během níž se pouštěly testy a opravovaly běžné závady. Po obě denní směny byli k dispozici technici, kteří průběžně odstraňovali běžné chyby. Čas od času se opravovalo v jednom kuse i několik hodin. Noční směna se techniky neobsazovala, přítomen byl jen noční hlídač, jehož úkolem bylo napsat na závěr směny do deníku stručný zápis o jejím průběhu. Zápisy o noční směně četli všichni s velkým zájmem, protože se mohli například dozvědět, že proběhla bez technické poruchovosti, ale nepočítalo se, protože počítač počítal, co sám chtěl. Je třeba říct, že zápisy tohoto typu nebyly příliš časté, protože na noční směny chodili počítat ostřílení harcovníci a navíc velcí fandové počítačů, kteří si s řadou běžných chyb dokázali sami poradit. Ne snad tím, že by je přímo opravili, ale dokázali na místě modifikovat svůj program tak, aby se alespoň některým problémům vyhnuli.



Údržba nebyla jednoduchá už proto, že konstrukční prvky neměly stabilní parametry. Elektronky s narůstajícím počtem odpracovaných hodin měnily své charakteristiky, polovodičové diody byly zase značně závislé na teplotě. Příkonem 10 kVA představoval Ural 1 slušná kamínka, a protože neměl klimatizaci, v horkých letních dnech někdy nezbylo než ho vypnout. Zákeřným nepřítelem byly tzv. studené spoje vzniklé při pájení, kdy se spoj dostatečně neprohřál. K odhalení takových spojů sloužilo proklepávání gumovou paličkou. Omezená životnost elektronek se začala projevovat prudkým nárůstem jejich poruch. V ČSAV se to řešilo tím, že zhruba jednou za rok se udělala během jednoho víkendu generální oprava. Celý počítač se při ní důkladně vyčistil, proměřily se všechny elektronky a ty, jejichž parametry nevyhovovaly, se vyměnily.

Některé chyby počítače byly opravdu záludné. Jednou testy neustále signalizovaly chybu, ale závadu se nedařilo odkrýt ani při pečlivém zkoumání signálů osciloskopem; až si jeden technik všiml, že při připojeném osciloskopu závada zmizí a při jeho odpojení se opět objeví. Nechat k počítači připojený osciloskop nebylo dost dobře možné, ale vše se vyřešilo tím, že se mezi místo, kam byl osciloskop připojen, a mezi uzemnění počítače připojil malý kondenzátor, který simuloval vstupní kapacitu připojeného osciloskopu.

Ještě stručně k Uralu 2. Konstrukčně převzal koncepci Uralu 1, tj. byl postaven na stejných prvcích (elektronky, odpory, kondenzátory, polovodičové diody), používal podobné typové elektrické obvody a i vzhledově vypadal téměř stejně, jen počet skříní se rozrostl téměř na trojnásobek. Úměrně vzrostl i příkon, na 30 kVA. Mezi hlavní odlišnosti Uralu 2 patřila feritová operační paměť, instrukce pro aritmetické operace s pohyblivou řádovou čárkou a bubnová paměť ve funkci vnější paměti.

Spolu se zavedením aritmetických operací v pohyblivé řádové čárce se zvýšila délka operandu ze 36 na 40 bitů a délka instrukce z 18 na 20 bitů. Kapacita feritové paměti stoupla prakticky na dvojnásobek. Feritová paměť také výrazně zvýšila operační rychlost počítače, zhruba na 5 až 6 tisíc operací za sekundu. Ke zvýšení operační rychlosti přispěly i bubnové paměti ve funkci vnějších pamětí. Kapacita jedné bubnové paměti činila 8 192 40bitových slov; celkem bylo možné k počítači připojit osm takových pamětí.

Ruské prameny udávají, že počítačový závod v Penze vyrobil celkem 183 počítačů Ural 1 a 139 kusů Uralu 2. Historie počítačů Ural skončila roku 1969, kdy byl vyroben jediný kus posledního modelu Ural 16.

Miroslav Kříž

Aktualita: MHM VIP Enterprise partnerem VMware

Společnost MHM computer s. r. o. rozšířila spolupráci se společností SOFT-TRONIK a stala se VIP Enterprise partnerem společnosti VMware. Může tak poskytnout lepší podporu stávajícím i novým zákazníkům po stránce technické i obchodní.

VMware je software, díky kterému je možné na jednom počítači provozovat několik virtuálních počítačů současně – od desktopů až po velké databázové systémy – a umožňuje tak zákazníkům konsolidovat serverové prostředí. Usnadňuje správu i přidělování a poskytování zdrojů serverů, umožňuje jednoduše a přímočaře vyvíjet distribuované aplikace a rapidně urychlit celý proces vývoje a testování.

Firma VMware je tvůrcem standardů v této oblasti a je vnímána jako absolutní světový lídr. Mezi spokojenými zákazníky používajícími její řešení najdete firmy ze všech oborů – např. Volvo, American Express, Ernst & Young, a mnoho dalších.

vmware®

Soutěž

V této rubrice přinášíme soutěžní otázky a jsme zvědavi na vaše odpovědi.
Hlavním tématem minulého čísla byla problematika konsolidace dat. Zejména jsme se věnovali řešení iSCSI, které je analogií technologie FC (Fibre Channel) a je určeno primárně pro malé a střední podniky.
Toto řešení je založeno na robustním diskovém úložišti, garantujícím spolehlivé a bezpečné uložení dat. Pro přenos dat z úložiště ke kterémukoliv aplikačnímu serveru, počítači či notebooku firmy využívá běžnou LAN. Není potřeba pořizovat žádné hardwarové nebo softwarové komponenty.

DNEŠNÍ OTÁZKA ZNÍ:
Co znamená v angličtině zkratka iSCSI?

Z mnoha správných odpovědí na otázku z minulého čísla byl vylosován pan Zbyněk Šotek z Brna

Gratulujeme a zasíláme malou pozornost od společnosti MHM.

OTÁZKA Z MINULÉHO ČÍSLA ZNĚLA:
Co je zobrazeno na obrázku?

Správná odpověď zní:
Feritová paměť
Tvořila ji malá feritová jádra protkaná soustavou vodičů sloužících k adresaci a ke čtení nebo k zápisu. Tato jádra byla uspořádána do tzv. paměťových matic. Dva vodiče, provlečené jádry kolmo na sebe, sloužily k magnetizaci (překlopení) jádra, jeden pak ke čtení a zápisu. Kolmými dráty (vlastně souřadnicemi) protékal pulzní proud – každým vždy poloviční, než byl zapotřebí k překlopení jádra. Jádro, kde se potkaly dva „půlproudy“, se překlopilo. V případě, že jádro bylo ve stavu „1“, naindukovalo do čtecího vodiče napěťovou „odezvu“. Každé z jader představovalo 1 bit. Čtení bylo destruktivní, takže po čtecím cyklu musel následovat zápisový. Tato operační paměť byla používána v 60. a 70. letech minulého století.

ODPOVĚDI PROSÍM PIŠTE DO ODPOVĚDNÍHO FORMULÁŘE NA WWW.MHM.CZ V SEKCI ČASOPIS. ODPOVĚĎ NA SOUTĚŽNÍ OTÁZKU NAJDETE V PŘÍŠTÍM ČÍSLE. NA VÝHERCE, KTERÝ BUDE VYLOSOVÁN ZE SPRÁVNÝCH ODPOVĚDÍ DNE 30. 11. 2007, ČEKÁ JAKO OBVYKLE MALÝ DÁREK.

Projekt EuroChamber Praha vám pomůže vyhledat vhodného obchodního partnera v zahraničí

Podnikáte na území hlavního města Prahy a máte zájem proniknout – formou exportu zboží a služeb nebo formou expanze své firmy – na zahraniční trhy? Potom se obraťte na Hospodářskou komoru hlavního města Prahy, která realizuje projekt JPD 3 EuroChamber Praha zaměřený na pomoc podnikatelům při navazování mezinárodní spolupráce.

Mnoha podnikatelům, zejména malým a středním, brání v rozšíření na nové trhy především komplikovanost pravidel, kterými se musejí řídit. Projekt EuroChamber Praha nabízí pražským firmám možnost vstoupit na zahraniční trhy jedněmi dveřmi, a to včetně získání osobních kontaktů v jednotlivých regionech i v celostátních obchodních komorách. Ty výrazně zjednoduší jejich zapojení do mezinárodního obchodu a zvýší jejich konkurenceschopnost v evropském měřítku. Hlavní cílovou destinací projektu jsou státy Evropské unie, i když know-how, které Hospodářská komora hlavního města Prahy v rámci projektu vytvoří, je využitelné také pro vstup na trhy mimo Unii.

Pracovníci Hospodářské komory hlavního města Prahy nejdříve seznámí zájemce o spolupráci se zahraničními partnery a s možnostmi, které jim projekt nabízí. Následně přijdou na řadu jednání přímo se zástupci zahraniční obchodní komory. Podnikatel, který má doporučení pražské hospodářské komory a do ciziny přijíždí prostřednictvím kontaktu s partnerskou zahraniční institucí, má mnohem větší šanci uspět se svou nabídkou.

Pražské firmy mohou výhody projektu využít zcela zdarma; projekt EuroChamber Praha je financován Evropským sociálním fondem a státním rozpočtem České republiky.

Ing. Petr Petřík
Hospodářská komora hlavního města Prahy

Changing the Way We Live And Work

www.cisco.cz

welcome to
the human network.

CISCO