Data v péči

ČÍSLO 11 | ZÁŘÍ 2008 | MHM COMPUTER A. S.



TECHNOLOGIE SAS
pro Enterprise storage systémy

Zázrak zvaný **SAS**

INFORMAČNÍ BEZPEČNOST
a její hrozby

ZÁLOHOVÁNÍ POBOČKOVÝCH SERVERŮ
- aneb jak na centrální backup

Zápisky z dovolené

Vedoucí příjmu zakázek a servisní technik v jedné osobě mi nabídl občerstvení a začal úřadovat. Zkontroloval technický průkaz, pas a pro něj v češtině nečitelný řidičský průkaz. Pak jsem podepsal, že souhlasím s namontováním nových dílů na svou motorku. Vše probíhalo docela svižně, bez prodlev a bez jakýchkoliv problémů.

„Za rohem je čekárna a kuchyňka, je tam televize, nějaké časopisy, kafe a automat na pití," upozornil mě technik a odmlčel se.

Po chvíli řekl, jakoby pro sebe „… je to dost práce, to budeme dělat docela dlouho, nejmíň čtyři hodiny," a pak se obrátil přímo ke mně: „Máte dost času?"

Jestli jsem měl něčeho málo, tak to byl čas.

„Tedy víte, dost spěchám, ale kdybyste chtěl, mohu vám pomáhat, tak by to bylo možná hotové rychleji," řekl jsem a usmál se na něj.

Technik se také usmál a odvětil: „To byste si ale musel hodně připlatit."

Poznámce jsem nerozuměl, ale pak jsem si řekl, že to není podstatné, a neřešil jsem to. V tu chvíli bylo důležité, že jsem pochopil, že moje pomoc byla s díky odmítnuta a budu dlouho čekat.

Jak praví český klasik JW v jedné ze svých pohádek: „Zdálo by se, že příběh končí, ale nekončí."

Zůstal jsem sedět v kanceláři, čekal jsem a nudil jsem se. Z dlouhé chvíle jsem si proto začal prohlížet podrobněji zařízení a vybavení kanceláře – a najednou jsem si všiml tabulky, která stála na skříňce:

CENÍK PRACÍ
Cena práce..... 75 dolarů / hod
Cena práce s možností sledovat technika ..... 85 dolarů / hod
Cena práce s možností pomáhat technikovi ..... 120 dolarů / hod

V první chvíli jsem si pomyslel, že jde o „opravdu dobrý" vtip, něco jako nápisy typu „Odešel jsem na přesnídávku, nevrátím-li se do jedné, zůstal jsem i na oběd," ale po chvíli jsem si vzpomněl na jeho poznámku „To byste si ale musel hodně připlatit" a vše jsem pochopil.

Z důvodů nedostatku jiné činnosti jsem začal nad ceníkem rozjímat. A hned mě napadlo: Ti Američané! Ti dokážou vydělat na všem!

Seděl jsem v křesle, čekal a rozjímal dál.

Základní sazba je jasná, školený technik provede práci a já mu hradím jeho odborný výkon. Pokud může někdo sledovat práci technika, tak získává teoretické znalosti o postupech, o vhodném nářadí a o způsobech řešení. A pokud dokonce někdo bude technikovi pomáhat, lze říci, že se účastní jakéhosi neformálního školení včetně praktického cvičení dovedností (a navíc svého školitele – servisního technika – zdržuje od práce).

Takže platit za služby – to je vlastně docela fér, pomyslel jsem si už v polospánku.

„Pane, vzbuďte se prosím, vaše motorka je už hotová. A odkud jste říkal, že jste? Z České republiky? Aha, a kde to je?"

Martin Miloschewsky

Best Training Partner Award of the year 2007

V minulých dnech udělila společnost Hitachi Data Systems (HDS) společnosti MHM computer cenu „Best Training Partner Award of the year 2007" za nejlepší školicí středisko v regionu EMEA. Toto ocenění bylo uděleno zejména za poskytování odborného školení v oblasti podnikových i modulárních paměťových systémů a softwaru společnosti HDS i za výborné znalosti a zkušenosti instruktorů.

Společnost MHM computer působí jako Hitachi Authorized Education Delivery Partner a její školicí centrum nabízí rozmanité kurzy v rámci výukového programu Hitachi Data Systems Certified Professional. Tento program účastníkům umožňuje dosahovat profesního růstu, zlepšit výkonnost a zvýšit důvěryhodnost. Školení jsou určena pro partnery a zákazníky HDS a jsou plně kompatibilní s požadavky výukových programů na podnikové paměťové systémy společnosti Sun Microsystems. Výuku zajišťují HDS certifikovaní instruktoři v plně vybaveném školicím centru.

V roce 2007 se školení zúčastnili posluchači z více než deseti zemí Evropy i Asie. Školení jsou obvykle v angličtině. Informace o jejich aktuální nabídce, registrační údaje a popisy kurzů naleznete na www.mhm.cz/skoleni nebo na *https://learning-center.hds.com*.

Další informace o školicím centru najdete také na *www.hdscc.cz*.

Vyhrajte s MHM!

TAŠKA NA DOKUMENTY OD SPOLEČNOSTI HITACHI ČEKÁ NA ŠŤASTNÉHO VÝHERCE.
PODROBNOSTI A SOUTĚŽNÍ OTÁZKU HLEDEJTE NA STRANĚ 15.



Data v péči MHM

Občasník
Vydáno: září 2008
Neprodejné
Vydává:
MHM computer a. s.
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

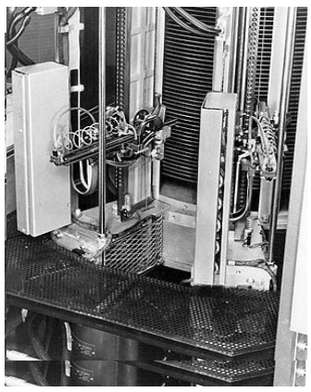
Připomínky a náměty pište na
redakce@datavpeci.cz, případně na adresu vydavatele.

A jakže je to vlastně v té bedýnce pospojované, pane kolego?

Pokud bychom chtěli provést fundovaný marketingový výzkum a veřejnosti položit poměrně jednoduchou otázku „Dokázali byste říct, co je diskové pole?“, dobrali bychom se nejspíš stejných výsledků jako nejmenovaný televizní bavič ve své večerní show. Pokud bychom tedy vybrali jako cílovou skupinu IT odborníky a položili jim tento dotaz, dokázaly by správně odpovědět více než tři čtvrtiny respondentů. Následná otázka ve stylu „Dokázali byste popsat SAS rozhraní použité v nejnovějších polích?“, by ale patrně vykouzlila bezradný úsměv na tváři i jim.

…A VY NEVÍTE, CO JE TO SCSI? ANEB TROCHA HISTORIE

Na začátku všeho byla tma a ticho. Pak se ze tmy nevědomí odněkud vynořila logická úroveň nula a jedna. Aby nuly a jedničky žily déle než jako impulzy v registru klopných obvodů, vyrazila děrovačka první dírku v děrném štítku. A bylo po tichu. Stohy stránek děrných štítků nahradily cívky děrných pásek a papír posléze magnetická páska. Koncem padesátých let se u mainframů roztočila první bubnová paměť a chvíli nato i první disk. Paměťová úložiště, pokud se jim tak dá říkat, byla k CPU připojena napřímo sběrnicí. Technické řešení přístupu k datům se lišilo výrobce od výrobce a s notnou dávkou nadsázky bychom mohli říci – co rodina zařízení, to originál. Jako nazýváme devatenácté století stoletím páry, tak šedesátá a sedmdesátá léta století minulého můžeme označit desetiletím sběrnic.



Začátkem let osmdesátých nastoupila na scénu jako zázrak architektura IBM PC, spásná myšlenka standardizace a celkové kompatibility. Zde byla zcela jasně definována úloha diskového prostoru, a bylo tedy nutné najít nějaký standardizovaný způsob přístupu k datům.

PANÍ STANDARDIZACE JE STEJNĚ SLEPÁ JAKO PANÍ SPRAVEDLNOST

Směr vývoje ukazuje vždy ta miska, na kterou se víc nasype.

V roce 1980 vyvinula firma Shugart Technologies rozhraní ST 506/412, častěji nazývané **ST506**. Propojení (mezi diskem a řadičem) tohoto rozhraní bylo zajišťováno 20vodičovým kabelem pro data a 34vodičovým kabelem pro řídící signály. Toto rozhraní bylo citlivé na šum. Řadič umožnil připojit celé dva disky přenosovou rychlostí 625 kB/s. Než se ocitlo koncem osmdesátých let v propadlišti dějin, používala ho firma Seagate u svých disků v IBM PC kompatibilních strojích. Tedy skoro ve všech.

V roce 1986 firmy Compaq a Western Digital představily nové rozhraní mezi diskovou jednotkou a řadičem (host adaptérem) nazvané **IDE** (Integrated Drive Electronics). Pevný disk IDE je připojen 40vodičovým kabelem k řadiči IDE. Toto rozhraní se velmi brzy stalo standardním díky své dostupnosti, jednoduchosti a faktu, že v PC-AT byla standardizována podpora rozhraní IDE v BIOSu (1983). Paralelní rozhraní IDE dovolilo připojit na jeden čtyřicetižilový kabel dvě zařízení. Od původních 3,3 MB/s se do dnešních dnů podařilo dosáhnout přenosové rychlosti 133 MB/s (jeden přenos). Zcela zásadní nevýhodou bylo, že rozhraní IDE čekalo na dokončení jednotlivých příkazů a ostatní řadilo do fronty.

Pokusem nahradit ideologicky již ne zcela mladé ST506 byl v roce 1980 počin **ESDI.** Do elektroniky disku byla implementována jistá inteligence, disk například sdělil svoji geometrii řadiči. Rozhraní ESDI firmy Maxtor, používající stejné kabely jako ST506, můžeme právem považovat za dědečka SCSI.

SCSI

Rozhraní SCSI (Small Computer System Interface) je na světě již poměrně dlouho, a to konkrétně od roku 1981. Bylo představeno jako osmibitové univerzální rozhraní, které umožní připojit k PC periférie jako pevný disk či jinou datovou „popelnici“ pomocí vcelku jednoduchého komunikačního protokolu podporujícího multitasking. Na rozdíl od všech předchozích je skoro veškerá inteligence integrována v zařízení (HOST) připojeném na SCSI sběrnici (BUS), která je od interní sběrnice počítače oddělena řadičem (Host Bus Adapter). Obsluha datového toku je prostřednictvím SCSI příkazů. Od roku 1981 se leccos změnilo a původních 50 žil se nám rozrostlo na 68, v případě konektoru SCA, kterým jsou vybaveny hot-plug disky, dokonce na 80. Každá nová generace přinášela zhruba dvojnásobné zvýšení výkonu oproti generaci původní se zachováním zpětné kompatibilty.

Původní **SCSI** disponovalo závratnou rychlostí 4 MB/s, 8bitovým paralelním přenosem po 50žilovém kabelu a možností adresovat celkem osm zařízení na jedné sběrnici. Není to, pravda, příliš mnoho, nicméně v těchto dřevních dobách i jiní nejme-

novaní velikáni hlásali, že ***„640 kB is enough for anyone“***. Od té doby informační technologie prošly mohutným vývojem. Rychlosti strojů se zvyšují lineárním trendem, obsluhované kapacity exponenciálně a na vlně pokroku se zákonitě muselo svézt i SCSI rozhraní. Již v roce 1986 spatřila světlo světa zázračná formule ANSI X3.131 – 1986, což není nic jiného než definovaný průmyslový standard **SCSI-1**. Šířka sběrnice: 8 bitů, počet zařízení: max. 8, takt. 5 MHz, přenos 5 MB/s, max. délka kabelů: 6 m. Koncem osmdesátých let jsme mohli obdivovat **SCSI-2**, které přineslo rozšíření množiny příkazů – i pro vyměnitelná média, frontování příkazů (command queuing) a aktivní terminaci. Díky rozšíření sběrnice na 16 bitů dosáhlo zvýšení datové propustnosti dvojnásobku, nazvané – **Wide SCSI**. Šířka sběrnice: 16 bitů, počet zařízení: max. 16, takt. 5 MHz, přenos 10 MB/s, max. délka kabelů: 6 m. Následovalo zvýšení taktu na 10 MHz – **Fast SCSI** – 10 MB/s, Fast Wide SCSI – 20 MB/s, délka kabelů 6, resp. 3 m. V roce 1994 bylo standardizováno **SCSI-3,** které přineslo opětovné zvýšení taktu na dvojnásobek, takže rozhraní Ultra SCSI (narrow) nyní dosahuje výkonu 20 MB/s, UltraWide SCSI 40 MB/s ruku v ruce s opětovným zkrácením aktivní délky kabelů na 3, resp. 1,5 m. To vše platí do roku 1996, kdy byla uvedena specifikace **Ultra 2 SCSI.** Překvapivě již nikoli jako standard SCSI-4. Ano, už i sběrnice SCSI ztrácejí svou erudovanost skrytou za standardizační komisí ANSI a výrobci pevných disků, kteří ji navrhují (v tomto případě Seagate a Quantum) její název upravují ke svým obchodním účelům. Místo logických úrovní 0 a 5V se začaly používat jejich rozdíly LVD (Low Voltage Differential), to znamená, že hodnota signálu je měřena vůči sobě. Pro aktivní přenos se začaly využívat nejen náběžné, ale i sestupné hrany signálů a QAS (arbitrace) – výsledek je 80 MB/s na 12 m dlouhém 68vodičovém kabelu. Plochý kabel přestal stačit, a proto se začaly, z důvodů rušení a přeslechů, používat ploché kabely lepené z párů kroucených dvoulinek. V roce 1998 přichází Quantum s **Ultra 160 SCSI**, který přidává podporu CRC a paketizaci. Po 68 žílách nyní svištělo 160 MB/s. Konečnou stanicí paralelního šílenství bylo **Ultra 320 SCSI** z roku 2000, které taktované na 80 MHz s propustností 320 MB/s představovalo technologický strop a bylo na hranici materiálu i fyzikálních zákonů. Co nás tedy čeká dál?

A CO TO TEDY ZKUSIT SÉRIOVĚ? ANEB PŘICHÁZÍ DOBA SÉRIOVÁ

SSA – Serial Storage Architecture

SSA představuje zajímavý pokus firmy IBM z roku 1990 o vlastní sériové SCSI řešení. Se svými 640 Mb/s a celkem 192 adresovatelnými zařízeními s podporou RAID technologie a dalšími zajímavými funkcemi. Firma si nechala řešení patentovat, čímž jej odsoudila k zániku a jednání s ostatními probíhalo zhruba v duchu:

10 Prodáme vám nové skvělé sériové rozhraní
20 Děkujeme, my si počkáme na Fibre Channel
30 END

FIREWIRE

V roce 1993 začala i firma Apple tušit, že šířka a takt paralelní sběrnice nelze zvyšovat donekonečna, a přišla s rozhraním FireWire postaveném na komunikačním protokolu SCSI-2. Ovšem s tolika odlišnostmi, že i samotná organizace IEEE FireWire přidělila rozhraní číslo 1394 a standard byl v roce 1996 na světě. Se svými 400 Mb/s, možností řetězení a podporou plug & play skončilo toto rozhraní jako spojovací článek mezi PC a spotřební elektronikou. FireWire odmítli výrobci pevných disků.

FIBRE CHANNEL

Od roku 1986 se připravovala specifikace vysokorychlostního rozhraní, které by bylo schopné přenést velké objemy dat vysokou rychlostí. V roce 1994 bylo rozhraní standardizováno, protokol FCP zde byl použit jako transportní protokol pro SCSI příkazy po FC síti. Přenosová rychlost od 1,0625 Gb/s, maximální počet připojitelných zařízení na jedné smyčce je 127. Existuje možnost propojit zařízení systémem „každý s každým“ pomocí switchů a celkový počet možných připojení může činit až **2^{24},** tedy 16 777 216**.** Fibre Channel u výrobců pevně zapustil kořeny a dnes FC disky najdeme v každém diskovém poli třídy Enterprise a v lepších modulárních polích. Fibre Channel se používá pro propojení diskových polí a knihoven k serverům. Jeho přenosová rychlost dnes činí 8,5 Gb/s FC8.

Jak Fibre Channel, tak FireWire a koneckonců i SATA (Serial attached ATA) ukázaly, že sériově je dnes správně, a výrobci disků začali hledat cestu, jak SCSI rozhraní na svých výrobcích, když FC je příliš drahé, SATA příliš pomalé a konektor SCA příliš široký (80 pinů, které Wide SCSI používá, se na moderní 2,5palcové disky jaksi nevejde), nahradit něčím jiným. Pak se dalo pár chytrých hlav dohromady a v roce 2003 se stal malý zázrak. Bylo standardizováno rozhraní SAS, které kombinuje nejlepší vlastnosti různých předchozích řešení, používá již vyráběné konektory a má navíc jednu zásadní vlastnost – je kompatibilní se SATA-2 disky.

Těžko říci, jestli labutí písní paralelních rozhraní byla rychlost, zvyšující se cena mědi nebo prostý fakt, že dětské prstíky v čínské manufaktuře dokáží za jednotku času zapojit mnohem více krátkých šestižilových kabelů než splést 68žilových vodičů do úhledných copánků a ty protahovat šasi značkových serverů. Budoucnost, jak se zdá, patří sériovému přenosu. Technické novinky vznikají v zásadě ze dvou důvodů. Prvním je snaha o technické zlepšení stávajícího řešení, druhou a dnes bohužel podstatně častější, je úsilí jednoho konglomerátu firem zašlapat do země ostatní konglomeráty (kokurenci) tím, že se vytvoří technické řešení v zásadě podobné, jako je konkurenční. Aplikuje se na ně tým marketingových specialistů, vybraným skládačům (skládač = sestavovatel finálního výrobku) se pošle nějaký ten kontejner vzorků zdarma a po určitém čase se řešení nechá uznat za standard.

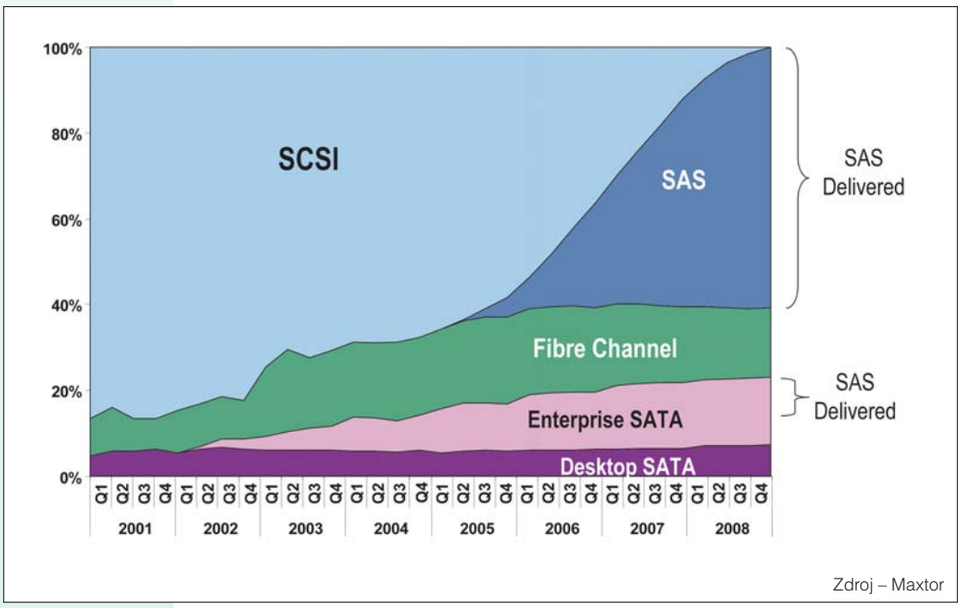
ZÁZRAK ZVANÝ SAS

I zlobři mají vrstvy

Stejně jako Fibre Channel používá architektura SAS vrstvovou architekturu. Je poněkud složitější, neboť

v sobě kombinuje dva vzájemně historicky ne zcela kompatibilní protokoly. Standardem je definováno celkem šest vrstev. Pojďme si je pojmenovat a v krátkosti popsat.

Physical Layer
Základem budiž fyzická vrstva **(Physical Layer)** – zde jsou definovány mechanické (jaké že to používáme konektory?) a elektrické (a kolik že voltů vlastně je ta logická jednička?) charakteristiky. Z pohledu mechanicky zdatné nezúčastněné osoby konektor SAS (SFF8482) disku vypadá skoro úplně stejně jako konektor SATA disku, jenom je na něm o jeden nálitek (klíč) víc. Obdobně vypadá konektor SFF8484, který umožňuje připojit dvě zařízení. K externímu propojení se používají konektory SFF847, známé též jako konektory Infiniband. Aby svět nebyl až tak jednoduchý, do hry vstupují i čtyřportové MiniSAS – SFF8087 a 8088. To jsou konektory, které můžete znát pod označením iPASS. Délka jednoho SAS kabelu může činit až osm metrů.

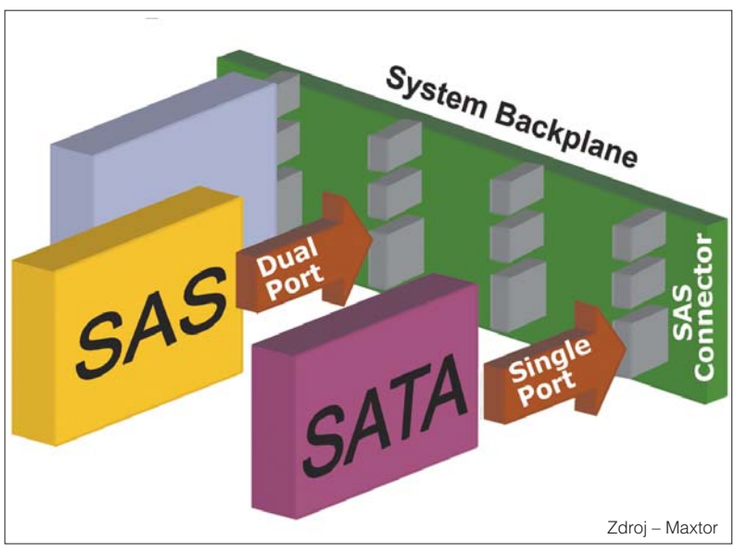


Zdroj – Maxtor

PHYLayer
Nad ní leží vrstva PHY, brouci, švábi či jiná elektronická havěť **(PHY Layer)** – čipy komunikují mezi sebou, provádějí překódování z 8 bitů na formát 10 bitů. Představme si to jako doručenky ke každému balíku dat. Najdeme zde OOB (out of band) signál, který je velmi důležitý z hlediska synchronizace různě rychlými protokoly – SAS vs. SATA elektronika cyklicky testuje a resetuje kabel a ptá se zařízení, jak rychle budou vzájemně komunikovat a zda pojede náš balík s doručenkou, vlakem, nebo letecky.

SAS Link Layer
Další vrstvou je linková vrstva (**SAS Link Layer**) – která ovládá tři nadvrstvy: SSP (pro Serial SCSI protokol), STP (pro SATA tunneling protokol) a SMP (pro serial management protokol). Na linkové vrstvě se vytváří spojení a přenášejí se data. Přečte se doručenka (primitive) a na základě jejího obsahu se rozhoduje, co bude s balíkem dat dál. Primitives mohou být jak společné pro všechny tři protokoly, např.: ERROR, HARD_RESET, BREAK,OPEN_ACCEPT…, tak přísně specifické pro daný protokol, například SATA_ERROR, SATA_HOLD. Na linkové vrstvě je řešen i power management STP. Používá příkazy: ATA IDLE, IDLE IMMEDIATE, STANDBY, STANDBY IMMEDIATE, zatímco SSP si vystačí s jednoduchým SCSI příkazem: START, STOP, UNIT.

Port Layer
O stupeň výš leží portová vrstva **(Port Layer)** – na této vrstvě zpracovává množina konečných automatů tyto funkce: Vytváří pár PHY-PHY, vybírá se PHY, které bude vysílat, otevírá a zavírá se spojení. V naší poštovní analogii skupina pošťáků čte stále dokola doručenky a rozhoduje, jakým způ-



Zdroj – Maxtor

sobem s balíkem naloží, zda mají volný vozík na balíky, dostatek doručovatelů a domlouvají komunikaci s ostatními poštami.

Transport Layer
Předposlední vrstva je transportní **(Transport Layer)** – tato vrstva je jakýmsi interfejsem mezi vrstvou

aplikační a portovou vrstvou. Tady se balí naše datové balíky. Transportní protokoly SSP (pro SAS zařízení), STP (pro SATA zařízení) a protokol STP se používá k řízení expanderů.

Application Layer
A zcela nejvýše leží aplikační vrstva (**Application Layer**) – s tou si povídá náš operační systém.

Á PROPOS – VY NEVÍTE, CO JE TO EXPANDER?

Ze smyčky do hvězdičky
Topologie bus není z hlediska škálování zcela optimální. Klasické SCSI mělo, jak jsme si říkali, klasický kabel, na který se nechalo umístit maximálně 16 zařízení včetně řadiče adresovaných jako SCSI ID 0–31. Víc se nedalo uadresovat, ani kdyby z nebe padaly trakaře obsedlané kočkami a psy v poměru 1:1. Prostě nedalo.

Naproti tomu smyčka Fibre Channel dovede naadresovat až 127 zařízení. Zásadní nevýhodou smyčky je to, že výpadek jednoho zařízení ve smyčce způsobí její zastavení a rozpad – algoritmus řízení nemá jak přeskočit vadné zařízení a zůstane stát jako slaměný panák v poli. Tuto relativní nevýhodu odstraňují různé obvody PBC, huby, případně fabric switche. Nicméně na backplanu diskových polí naleznete vždy smyčky. Na FC zařízení najdete WWN adresu (64bitové číslo) jako jeho jednoznačný a světově unikátní identifikátor. FC používá WWN pouze při logování do FC sítě pro generování 24bitové Fabric Address, případně z těchto 24 bitů posledních 8 bitů jako adresu na smyčce. Představme si v naší poštovní analogii např. P. O. Box, kterým maskujeme svoji skutečnou adresu.

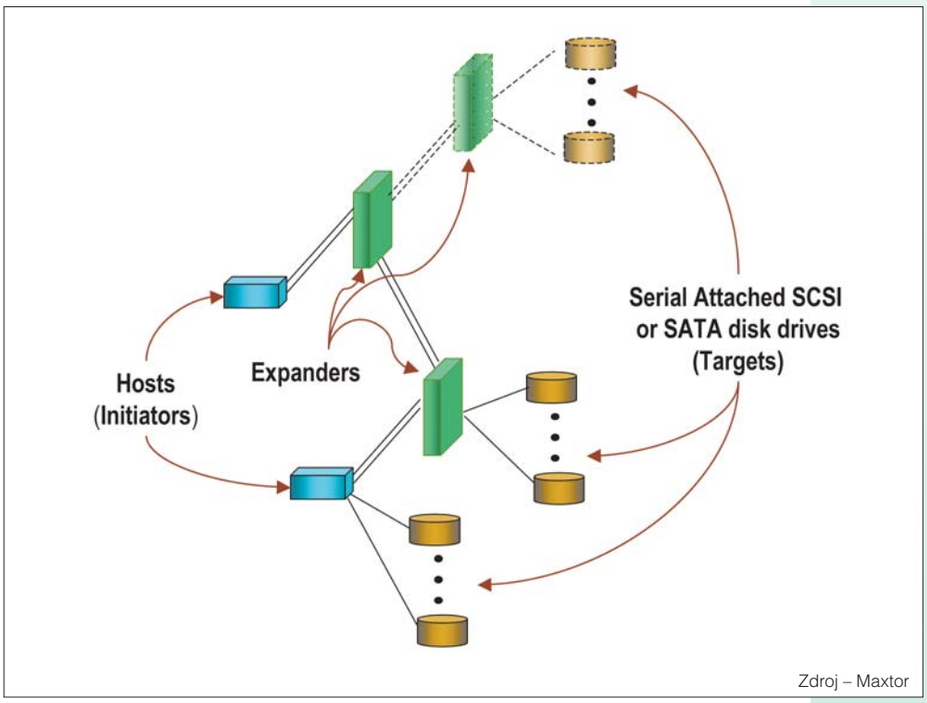
SAS používá též WWN (někdy nazývané SAS ADDRESS), ovšem s tím rozdílem, že v síti adresuje přímo na WWN. SAS je tzv. Point-to-point rozhraní, vždy spolu komunikují jeden initiator a jeden target. To je však dvojice a standard nám slibuje až 16 384 vzájemně komunikujících zařízení v jedné SAS doméně. Zde přichází ke slovu expandery, které se dále dělí na Edge Expandery a Fanout Expandery. Expander si můžeme představit jako síťový hub, který spojuje PHYs jednotlivých SAS zažízení mezi sebou. Edge Expander dovoluje propojit 128 zařízení mezi sebou a může být zapojen k jednomu dalšímu Edge Expanderu. Potřebujeme-li propojit více Edge Expanderů, musíme použít Fanout Expander, který si můžeme představit jako síťový switch, neboť do systému vnáší jistou inteligenci – jako například routovací tabulky. V jedné SAS doméně můžeme vzájemně propojit 128 Edge Expanderů se 128 Fanout Expandery, proto 128 * 128 = 16 384 zařízení. Porty a za nimi ležící elektronika PHY se nechají multiplikovat – zdvojovat, nebo zčtyřnásobit, a tím vytvoří tzv. Wide port. Protože vzniká spojení PHY – PHY a kabel se s nikým nesdílí, využívá se vždy celá šířka pásma.

NEVĚSTA ZE SATA ANEB NÁVOD JAK POSKLÁDAT MIX DISKŮ V JEDNÉ KRABICI

SAS Disky mají dva target porty. SATA disky mají však pouze jeden port. Musí se tedy použít 2port to single port adapter, kterým nejen odstraníme handicap SATA spočívající v neexistenci druhého portu, ale zároveň přidáme i WWN. Odtud je již jen krůček k tomu navrhnout a poskládat diskové pole, ve kterém můžeme v jedné řadě kombinovat rychlé a výkonné SAS disky s jejich levnějšími, pomalejšími, ale co do kapacity většími sourozenci. Pro ty, kteří by chtěli radostně zavýsknout a použít SAS disky se SATA řadičem, mám doplňující informaci, že kompatibilita je jaksi jednosměrná. SAS disk k SATA řadiči nepřipojíte (ani násilím).

A CO BUDE DÁL?

Začátkem května letošního roku oznámila společnost Hitachi společně s PMC-Sierra, že společným úsilím dosáhly reality přenosu dat rychlostí 6 Gb/s na SAS rozhraní. Zrodilo se SAS-2 zpětně kompatibilní s SAS. V demonstraci bylo použito čipsetů PMC-Sierra, jmenovitě protokolového řadiče Tachyon SPC 8x6G, RAIDového řadiče SRC 8x6G a rozšiřujících switchů (expanderů) maxSAS SXP 36/24x6GSec. Společnost Hitachi pak dodala vzorky pevných disků, které disponovaly právě 6Gb SAS rozhraním.



Zdroj – Maxtor

Čekají nás tedy světlé, rychlé a sériové zítřky.

Jan Kerber, MHM computer

Technologie SAS
pro Enterprise storage systémy

Vytížení datových center zaznamenalo v posledních letech exponenciální růst. IT manažeři jsou proto nuceni hledat nové možnosti jak zdroje pro ukládání podnikových dat rozšířit, a to pokud možno velmi spolehlivým a současně cenově úsporným způsobem. Díky zavedení technologií komplementárních sériových rozhraní se nyní mohou pružně rozhodnout, zda použít vysoce výkonné disky SAS, nebo cenově úsporné disky Serial ATA (SATA) v prostředí pro úschovu dat používajícím sériovou sběrnici **(SAS – Serial Attached SCSI)**. Kompatibilita hardwaru mezi novými rozhraními přitom při volbě serverů a subsystémů pro ukládání dat nabízí nebývalou flexibilitu.

Technologie SAS byla navržena jako nástupce paralelního SCSI, které bylo coby rozhraní pro ukládání podnikových dat úspěšně používáno přes 20 let. SAS podporuje sadu příkazů a protokol SCSI, takže udržuje kompatibilitu s aplikačním softwarem, do nějž podniky investovaly v posledních 20 letech mnoho prostředků. SAS umožňuje vyšší rychlost přenosu dat, větší počet zařízení na řadič, snižuje počet kabelů i konektorů a zjednodušuje jejich propojení (čímž umožňuje použití menších diskových polí s větší hustotou uložených dat).

SAS představuje point-to-point sériovou architekturu, což znamená, že každý disk má přidělené připojení k hostitelskému zařízení. Při celkově vyšším výkonu odstraňuje kritická místa sdílené (paralelní) sběrnice, protože hostitelské zařízení přenáší data na každý pevný disk v celé šířce pásma. Tato přidělená point-to-point připojení zajišťují prvotřídní výkon pomocí plně duplexního připojení rychlostí 3 Gb/s.

SAS je dualportové rozhraní, které vytváří dvě oddělené datové cesty k disku. Tím je dosažena vyšší úroveň výkonu a je odstraněno kritické místo, které je nevýhodou současných paralelních rozhraní SCSI. Specifikace SAS předznamenává průběžné zvyšování přenosové rychlosti na 6 Gb/s a poté až na 12 Gb/s, což zaručuje vysoký výkon v dlouhodobém časovém horizontu. Společnosti PMC-Sierra a Hitachi Global Storage Technologies (Hitachi GST) v dubnu 2008 oznámily, že úspěšně dosáhly end-to-end interoperability mezi 6Gb/s čipsety SAS společnosti PMC-Sierra a prototypem 6Gb/s pevných disků (HDD) SAS společnosti Hitachi. Díky vyššímu výkonu, který 6Gb/s pevné disky SAS poskytují, jsou systémy SAS-2 lépe rozšiřitelné, dostupné a spolehlivější. V důsledku předvedení úspěšné interoperability 6Gb/s SAS mezi čipsety PMC-Sierra a pevnými disky Hitachi mohou výrobci serverových systémů a zařízení pro úschovu dat navrhnout architekturu SAS-2, která bude bez jakýchkoli problémů uceleně fungovat při přenosové rychlosti 6 Gb/s. Pevné disky SAS s 6 Gb/s a další součásti infrastruktury budou zpětně plně kompatibilní se stávajícími 3Gb/s zařízeními. Zákazníci tak získají výjimečnou flexibilitu v oblasti konfigurace a ochranu svých investic.

VĚTŠÍ PODPORA ZAŘÍZENÍ

Jedním z hlavních omezení paralelního rozhraní SCSI je skutečnost, že podporuje nejvýše 15 disků na jedné sběrnici. SAS zlepšuje adresovatelnost a konektivitu disku pomocí Fanout a Edge Expanderů. Fanout Expandery mohou adresovat až 128 Edge Expanderů a každý Edge Expander může adresovat až 128 zařízení SAS, takže celková konektivita představuje 16 384 zařízení SAS. Tímto způsobem je možné přes vícečetné spoje SAS seskupit velké množství uskládaných dat.

Díky této dobře rozšiřitelné metodě propojení pevných disků SAS do systému mohou IT manažeři vyvíjet řešení pro ukládání dat, která podporují vytváření víceuzlových clusterů a dynamický load balancing. (Dynamický load balancing je aplikace, která rozkládá zátěž na větší počet řadičů a datových cest, čímž odstraňuje kritická místa a zvyšuje průchodnost.)

KOMPATIBILITA SÉRIOVÉHO ROZHRANÍ

Technologie SAS a SATA sdílejí stejné fyzické rozhraní. IT manažeři tak mohou používat oba typy disků v jednom úložišti. To představuje významnou výhodu pro ty z nich, kteří zajišťují víceúrovňové ukládání dat, což je metoda klasifikace a úschovy dat na základě hodnoty, kterou podnik datům přisuzuje. Použití vysokokapacitních a cenově dostupných disků SATA pro ukládání referenčních dat, k nimž není třeba častý přístup, umožňuje IT manažerům minimalizovat náklady a zjednodušit správu dat. Primární data, běžně používaná při zpracování on-line transakcí a v dalších aplikacích, které jsou pro podnik zásadní, je pak vhodné uschovávat na výkonnějších pevných discích SAS.

Kompatibilita mezi backplany, konektory a kabe-



Hitachi Simple Modular Storage 100: diskové pole používající technologii SAS

láží sníží náklady a složitost, ale také zjednoduší proces výměny „mixu“ disků v úložišti. Možnost vyměnit disk SATA za disk SAS, nebo naopak, odstraní nutnost vyměňovat celé systémy v případě, že je potřeba vyšší výkon nebo větší kapacita.

Pro firemní zákazníky, kteří požadují flexibilitu a rozšiřitelnost z důvodu zvyšování pracovního vytížení datových center, budou pevné disky SAS představovat významný krok kupředu. S celosvětovými požadavky na úschovu dat, které se budou v nadcházejících letech značně zvyšovat, budou mít flexibilita a rozšiřitelnost pro tvůrce systémů a jejich zákazníky prvořadý význam.

MEZNÍK V OBLASTI SCSI

Za posledních dvacet let prošla technologie radikální proměnou. Dramatický pokrok v rychlosti procesorů (2 000× rychlejší), velikosti RAM (1 000× větší) a rychlosti RAM (2 000× rychlejší) zvýšil výkon systému na úroveň, která by ještě před několika málo lety byla nemyslitelná, nemluvě o době před dvaceti lety. Jeden aspekt výkonnosti systému se ale nápadně opožďuje: výkon disku paralelního SCSI. Pozoruhodný pokrok v oblasti plošné hustoty samozřejmě přinesl exponenciální růst v ***kapacitě*** disků (3 600× větší), ale rychlosti přenosu u paralelního SCSI dosáhly pouze skromných přírůstků (32×). Tyto přírůstky navíc přišly jen zdráhavě, protože základní omezení paralelní sdílené sběrnicové architektury jsou příčinou toho, že každé další zvýšení rychlosti je stále problematičtější a nákladnější.

Zatímco paralelní SCSI se jasně blíží limitům svého praktického výkonu, sériová rozhraní chytila díky nedávným průlomům v technologii Very Large Scale Integration (VLSI) a vysokorychlostním sériovým kombinovaným vysílačům-přijímačům druhý dech. Technologie SCSI nyní dosáhla zásadního bodu obratu, kdy omezení paralelních rozhraní odrazují od dalšího vývoje v této oblasti, zatímco klíčící potenciál sériových rozhraní již předvedl pozoruhodný výkon a přínosy ve smyslu rozšiřitelnosti. Pro lepší porozumění významu tohoto mezníku, konkrétním výzvám, které představuje paralelní SCSI, a odpovídajícím výhodám Serial Attached SCSI (SAS) níže uvádíme shrnující tabulku.

Technologie Serial Attached SCSI byla plánována jako ***nejmodernější*** řešení pro ukládání dat – zachovává si osvědčenou sadu příkazů SCSI předcházející technologie a spojuje ji s nejnovějšími dostupnými sériovými technologiemi. Výsledkem je rozhraní vyvinuté pro potřeby Enterprise zákazníků, které v sobě spojuje čtyři podmanivé rysy (výkon, rozšiřitelnost, kompatibilitu a SCSI integraci) a tvoří ucelené a komplexní řešení. Pokročilý design Serial Attached SCSI zaručuje, že SAS splní nároky na ukládání podnikových dat nejen dnes, ale i v budoucnu.

Hitachi Data Systems

Mezník v oblasti SCSI: Přechod od paralelního SCSI k Serial Attached SCSI (SAS)

	Paralelní SCSI	SAS
Architektura	Paralelní, všechna zařízení jsou připojena ke sdílené sběrnici	Sériová, point-to-point, oddělené cesty signálu
Výkon	320 MB/s (Ultra320 SCSI); výkon se snižuje, když jsou zařízení připojována ke sdílené sběrnici	3,0 Gb/s, plánováno je až 12,0 Gb/s; výkon zůstává, i když je připojováno více disků
Rozšiřitelnost	15 disků	Více než 16 000 disků
Kompatibilita	Nekompatibilní s ostatními rozhraními disků	Kompatibilní se Serial ATA (SATA) rozhraním
Max. délka kabelu	12 metrů celkem (nutné sečíst délky všech kabelů použitých na sběrnici)	8 metrů na jedno oddělené připojení; celková kabeláž pro doménu stovky metrů
Kabeláž	Množství vodičů znamená další objem i náklady	Kompaktní vodiče a kabeláž šetří prostor a náklady
Hot Plug	Ne	Ano
Identifikace zařízení	Nastavuje se manuálně, uživatel musí zajistit, aby na sběrnici nekolidovalo žádné ID	V době výroby celosvětově nastaveno jedinečné ID; není nutný žádný krok ze strany uživatele
Terminace	Nastavuje se manuálně, uživatel musí zajistit řádnou instalaci a funkčnost terminátorů	Oddělené cesty signálu umožňují, aby zařízení obsahovala terminaci defaultně, není nutný žádný krok ze strany uživatele



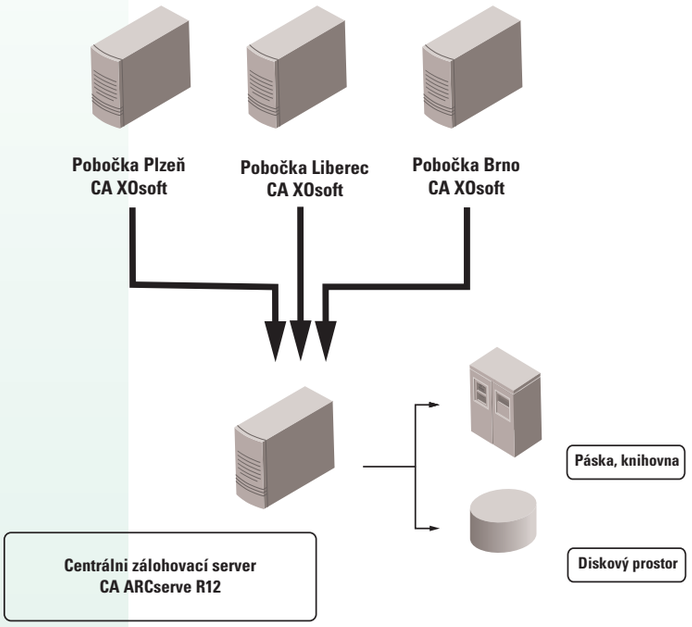
Zálohování pobočkových serverů

ANEB JAK NA CENTRÁLNÍ BACKUP

Při běžném provozu firmy se často setkáváme s potřebou zazálohovat data na malých pobočkových serverech. Firmy postupně rostou a zřizují pobočky na různých místech. Byť se zdá být otázka backupu jednoduchá, lze se při návrhu zálohovacího procesu setkat s řadou záludností.

PRVNÍ OTÁZKA: KAM ZÁLOHOVAT?

Poměrně častým řešením bývá zálohovací páska. Dnes se ovšem již v odpovědích uživatelů na tuto otázku často objevuje i externí disk nebo diskové pole. Uvědomíme-li si, že další zařízení znamená další náklady, proč tedy nevyužít zařízení instalované na centrále? Ve většině případů není na malých pobočkách žádný odborník. Nemyslím IT experta, ale alespoň člověka, který je schopen zvládnout kontrolu zálohy a případně výměnu nějakého média. Jeho přítomnost obvykle není možné zaručit.



OTÁZKA DRUHÁ: MŮŽEME ZÁLOHOVAT CENTRÁLNĚ?

Jednoduchá odpověď: Ano, můžeme. Centrálním zálohováním odstraníme potřebu dalších zálohovacích zařízení. Navíc i obsluha bude řešena centrálně z jednoho místa, kde je odborný personál. Spojení mezi pobočkami také existuje, obvykle je každá pobočka připojená k internetu.

TAK JDEME NA TO

Vypadá to jednoduše, ale mohou se objevit nečekané problémy. Princip je jednoduchý, data přesuneme na centrálu a tam zálohu vyřešíme. Ale vtip je právě v tom přesunu.

Je potřeba si uvědomit, jak velké množství dat přesouváme a jak dlouho to bude trvat. Například u linky s propustností 2 Mb/s bude trvat kopie 60 GB více než 60 hodin, což je z pohledu zálohování velmi neefektivní. Navíc by celá kapacita musela být reálně vyhrazena jen pro přesun dat skoro tři dny.

Mimochodem, když započítáte běžné použití asynchronních linek ADSL s prostupností uploadu řekněme 256 kb/s, tak můžete na centrální zálohování téměř zapomenout. Délka procesu bude časově naprosto neúnosná. V běžném prostředí by to trvalo celý týden.

EXISTUJE ŘEŠENÍ?

Není sice jednoduché, ale přesto existuje. Celé „kouzlo“ spočívá v technologii synchronizace a replikace.

SYNCHRONIZACE

Nejdříve krátké vysvětlení, co si pod pojmem synchronizace představit. Princip je velmi jednoduchý. Předpokládáme, že obsah pobočkového serveru máme zkopírovaný na serveru centrálním a je téměř shodný. Synchronizace nalezne rozdíly a zajistí jejich „předání“ mezi pobočkovým serverem a serverem centrálním. Vtip je v tom, že rozdíly v datech jsou z pohledu velikosti násobně menší než celý jejich obsah, který bychom museli přenášet při klasické plné záloze (full backup).

Zkuste si představit celý obsah o kapacitě 60 GB a rozdíl dosažený během jednoho pracovního dne – například 100 MB. Těch 100 MB už přenášet lze!

JAK ZAJISTIT SHODU?

Jednou variantou je vzít jeden ze serverů, dovézt ke druhému a překopírovat obsah. Druhou variantou je udělat kopii dat na externí médium, třeba na externí disk, a přenést ji na druhý server. Nic složitějšího v tom není. Neznamená to, že byste museli kopírovat data pravidelně. Postup použijete jen jednou na začátku pro ustavení první synchronizace, abyste množství dat přenášených po internetové lince co nejvíce snížili.

Výsledkem inteligentní synchronizace je komplentní záložní kopie v době synchronizace s malými nároky na přenos dat.

REPLIKACE

Zkusme koncept ještě rozšířit. Synchronizace pouze srovnává dva obsahy. Když si uvědomíte, že změny postupně vznikají při práci uživatelů, tak by bylo fajn je kopírovat ihned a nečekat na synchronizaci. Potom by množství přenášených změn bylo zcela minimální a bylo by rozprostřené do celého dne, podle toho, jak je potřeba.

Replikace zajistí přenos změn okamžitě, a tak sníží množství změn přenášených po lince v jednom okamžiku na minimum. Určitě počítáme s tím, že replikace je rovněž „inteligentní“ a přenáší reálné změny souborů a ne soubory celé. To znamená, že při změně části textu v rozsáhlém dokumentu se přenese pouze změna a ne soubor celý.

POJĎME TO DÁT DOHROMADY

Jak by mohl vypadat celý proces s využitím technologií synchronizace, replikace a zálohování? V úvahu přichází řešení dvěma navzájem integrovanými produkty CA ARCserve a CA XOsoft Replication.

CA XOsoft zařídí synchronizaci a replikaci mezi pobočkovými servery a CA ARCserve následně data zazálohuje. Celý proces je řízen automaticky, oba produkty spolu vzájemně komunikují. Samozřejmě se předpokládá, že linky jsou internetové a navíc CA XOsoft vám umožní i nastavovat dynamicky propustnost a rychlost přenášených dat tak, abyste v pracovní době nebyli omezováni.

Proces synchronizace, replikace a zálohy řídí konzole CA XOsoft. Pokud se rozhodnete obnovit data, potom vám konzole CA ARCserve nabídne data k obnově.

A MÁME ZAZÁLOHOVÁNO

Kombinací produktů CA ARCserve a CA XOsoft zajistíte elegantní řešení centrálního zálohování poboček s využitím internetových linek. Řešení zajišťuje dlouhodobou zálohu, správu médií i zabezpečení dat šifrováním. Můžete tak stále používat zálohovací zařízení na centrále a z poboček data pouze přetahovat k centrálnímu zálohovacímu serveru. Není třeba dalších zálohovacích zařízení, ani dalšího odborného personálu.

Michal Opatřil, CA

Hyper-V prakticky v MHM

Hyper-V, název nové virtualizační technologie od společnosti Microsoft, se v poslední době skloňuje na každém kroku. Není týdne, aby o ní nevyšel nějaký komentář. V našem časopisu jste se s Hyper-V mohli setkat již v dubnovém čísle, kde vás autor Martin Pavlis seznámil se základním konceptem Hyper-V virtualizace. To bylo ještě v prenatálním období, kdy byl Hyper-V dostupný pouze v beta verzi. Dnes je však všechno jinak. Hyper-V je hotov, oficiální přestavení a uvedení na trh proběhlo 26. června, a řada zákazníků zvažuje jeho nasazení. My jsme okamžitě po uvolnění ostré verze Hyper-V vyzkoušeli a o praktické zkušenosti se s vámi rádi podělíme v tomto článku.

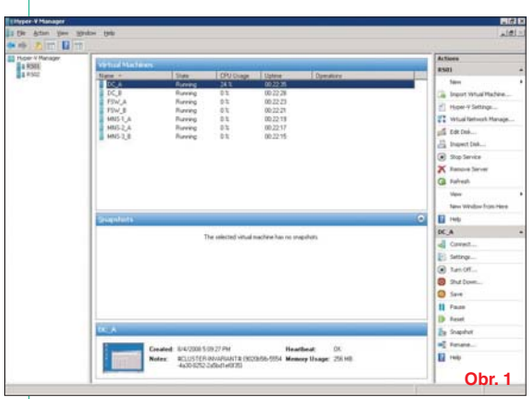
Prvním důležitým krokem nasazení Hyper-V je volba vhodné edice operačního systému MS Windows Server 2008. Hyper-V je volitelnou rolí tohoto nového operačního systému a běží pouze na verzi x64bit. K dispozici jsou celkem tři edice Windows Serveru 2008: Standard, Enterprise a Datacenter. Datacenter je nejvýkonnější edicí, se kterou se v našich končinách prakticky nesetkáme. Zato edice Standard a Enterprise jsou u nás hojně rozšířeny. Kterou tedy vybrat, požadujeme-li funkce Hyper-V? Klíčovou otázkou je, zda budeme chtít vybudovat Hyper-V prostředí s vysokou dostupností. Pokud ano, budeme potřebovat funkci tzv. failover clusteringu (lidově cluster), a ta je dostupná pouze v edici Enterprise. Z pohledu licencí dává Enterprise edice zákazníkovi možnost provozovat Windows Server 2008 1× na fyzickém stroji a 4× ve virtuálním prostředí na tomto stroji. U edice Standard je licenční model 1× a 1×. Licenční model edice Datacenter je 1× a neomezeno. Windows Server 2008 se také ve všech edicích nabízí ve verzi Core. Verze Core znamená, že operační systém nemá Graphical User Interface (GUI) pro správu systému; ta se kompletně provádí v příkazové řádce (CLI). Verze Core tak zaručuje větší stabilitu systému, má menší provozní režii, a tudíž je velice vhodným kandidátem pro hostování role Hyper-V.

Druhým podstatným krokem je volba správného hardwaru. Hyper-V vyžaduje 64bitovou architekturu, hardwarovou podporu pro virtualizaci Intel VT nebo AMD-V a funkci Data Execution Protection (DEP). Bez nich nebude Hyper-V fungovat. Funkce DEP se v podání Intelu nazývá Execute Disable (XD), u AMD je to No Execute bit (NX). Hardwarová podpora virtualizace i DPE se nastavují v BIOSu fyzického serveru. Obě tyto technologie od Intelu i od AMD jsou na trhu již delší dobu, cca tři roky, proto nasazení Hyper-V nemusí nutně znamenat pořízení nového serveru. Někdy stačí flashnout BIOS, jako tomu bylo v našem případě. V případě rozhodnutí koupit nový server doporučuji navštívit stránky Windows Server Katalogu (http://www.windowsservercatalog.net), kde najdete celou řadu serverů certifikovaných pro běh Hyper-V od renomovaných výrobců, jako jsou Hitachi, Bull, Fujitsu Siemens a další.

MHM se specializuje na běh systémů s vysokou dostupností, proto byla naše volba konfigurace Hyper-V prostředí jasná. Musí to být High Availability (HA)! Proto jsme zvolili Windows Server 2008 EE (Enterprise Edition) v anglické verzi. Hyper-V umí i češtinu, ale ta ve světě IT přináší jen nedorozumění. Abychom mohli tento článek proložit nasbíranými screenshoty, tak jsme záměrně nepoužili Core verzi. Jako hardwarový základ nám posloužily naše tři starší servery Bull Novascale 460, u kterých jsme updatovali BIOS. Instalace operačního sytému Windows Server 2008 na všechny tři servery proběhla naprosto hladce bez nutnosti dodávat další ovladače i přesto, že servery byly vybaveny řadičem RAID a adaptéry HBA. Velikým překvapením bylo, když instalátor Windows Serveru 2008 rozeznal i LUNy, které byly namapované z diskového pole, a nabídl je pro instalaci operačního systému.

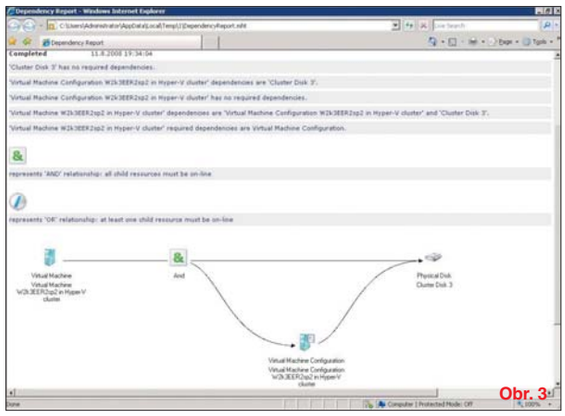
ZPROVOZNĚNÍ MS CLUSTERU

Pro realizaci prostředí MS clusteru je nezbytné mít funkční MS doménu. Proto jsme jeden ze serverů vyčlenili pro funkci doménového kontroleru a do této role jsme ho povýšili. Zbylé dva servery jsme do této domény začlenili a přidali jim roli Hyper-V. Instalace role Hyper-V je velice jednoduchým „klikacím“ úkonem, ale vyžaduje reboot serveru. Po rebootu, pokud je vše správně nastaveno v BIOSu, se spustí Hyper-V-Hypervisor spolu se službami: Hyper-V Image Management, Hyper-V Networking Management a Hyper-V Virtual Machine Management. Pro management Hyper-V má Windows Server 2008 vlastní MMC Hyper-V Manager snap-in modul, který lze spustit přímo z Administrative Tools nebo ze Server Management konzole. Ta se spouští automaticky po přihlášení uživatele a obsahuje všechny důležité snap-in moduly pro správu. Hyper-V Manager umožňuje kompletní správu lokálního i vzdáleného virtuálního prostředí (obr. 1). Práce s Hyper-V Managerem je velice intuitivní a celé jeho prostředí je velmi dobře ergonomicky navržené. Užitečnou funkcí Hyper-V Manageru je Export a Import virtuálních strojů z jednoho Hyper-V prostředí do druhého. Zajímavostí je také podpora provozu virtuálních „ne-Microsoftích“ operačních systémů. Seznam podporovaných virtuálních systémů můžete nalézt zde: http://www.microsoft.com/windowsserver2008/en/us/hyperv-supported-guest-os.aspx.

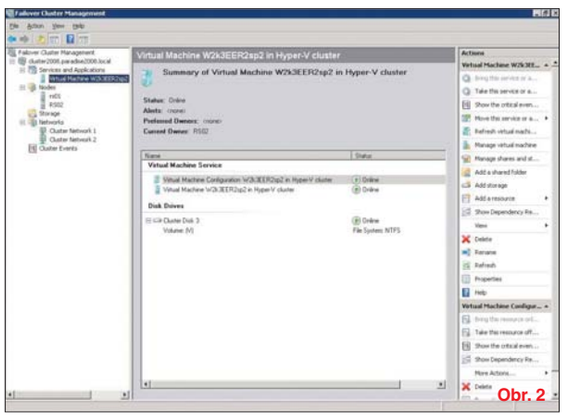


Obr. 1

V Hyper-V Manageru jsme vytvořili virtuální stroj s operačním systémem Windows Server 2003. Instalace tohoto virtuálního stroje proběhla naprosto běžným způsobem. Po dokončení instalace je možné do virtuálního stroje doinstalovat tzv. Integration Services (obdoba Virtual Machines Additions), které umožní zejména automatické přepínání ovládání myši. V případě vzdáleného přístupu (Remote Desktop) k Hyper-V Manageru je instalace Integration Services nutností, bez níž myš v otevřené virtuální stanici nebude fungovat. Pro úplnost této části musím dodat, že data instalovaného virtuálního stroje byla umístěna na diskovém poli, konkrétně Hitachi AMS500, které má certifikaci Windows Server 2008.


Obr. 3

Nainstalovaná virtuální stanice zatím neběží v HA prostředí. V případě výpadku Hyper-V serveru dojde k zastavení i tohoto virtuálního stroje. HA prostředí nám zaručí funkce Failover Clusteringu (po staru MSCS Microsoft Cluster Service). Tato funkce doznala v novém Windows Serveru podstatných změn jak v managementu, tak i v možnostech konfigurace. O těchto novinkách připravuji samostatný

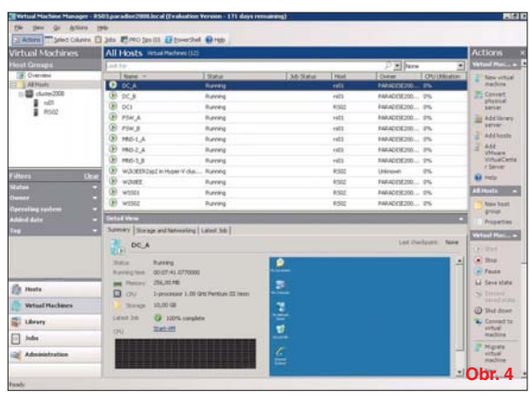

Obr. 2

článek, takže je teď nebudu popisovat. Pro naše prostředí, doménový kontroler, dva nody a jedno diskové pole, jsme vybrali konfiguraci clusteru s Node and Disk Majority kvórem. Jakmile byl cluster nainstalován, spustili jsme průvodce vytvořením nové clusterové aplikace. Specifikovali jsme typ clusterové aplikace, zvolili jsme Virtual Machine a průvodce zobrazil seznam dostupných virtuálních strojů, kde jsme si jednoduše vybrali a klikli na tlačítko Finish. Tímto se náš virtuální stroj stal HA stojem, který se v případě výpadku jednoho Hyper-V serveru automaticky přesune na druhý Hyper-V server a pokračuje v činnosti. Měřený výpadek při manuálním přesunu znamenal ztrátu tří pingů, skutečný výpadek (vytržení napájecího kabelu) potom sedm. Konfiguračním předpokladem HA prostředí je, že data virtuální stroje jsou uložena na LUNu diskového pole a oba Hyper-V servery mají k tomuto LUNu přístup. Tento LUN je potom diskovým zdrojem v prostředí clusteru. Nastavení clusterové aplikace virtuální stroje je znázorněno na obr. 2. Na obr. 3. si potom můžete prohlédnout mapu závislostí zdrojů clusterové aplikace virtuálního stroje.

Výše popsané HA prostředí řeší výpadek Hyper-V serveru, ale nikoli výpadek celé lokality. Ten řeší geografické HA prostředí, neboli existují nejméně dvě geograficky vzdálené lokality (produkční a záložní), které jsou vzájemně redundantní. Hyper-V spolu s Hitachi Storage Clusterem (HSC) umožňuje takové geografické prostředí vytvořit.

Éru MS virtualizace můžeme slovy klasika rozdělit na dobu před Hyper-V a po Hyper-V. Informace o nové virtualizační technologii Hyper-V zní na poslech dobře, ale teprve praktické vyzkoušení přinese nefalšovaný úžas nad rychlým a ladným během Hyper-V virtuálních strojů. Přitom je Hyper-V za hubičku. Cena Windows Serveru 2008 s a bez Hyper-V je liší o 28 amerických dolarů! Navíc bezplatné funkce clusteringu, možnost on-line konzistentního zálohovaní prostřednictvím služby VSS (Volume Shadow Copy Service), Import/Export virtuálních strojů, management konzole a další jsou hozenou rukavicí konkurenčním technologiím. Microsoft dále nabízí řadu pokročilých nástrojů pro management a backup Hyper-V prostředí z rodiny MS System Center. Zde stojí za zmínku MS System Center Virtual Machine Manager 2008 (SCVMM), který umožňuje konverzi virtuálních strojů konkurenčních technologií nebo pokročilou správu a monitorování nejen Hyper-V, ale i VMware virtuálního prostředí. Uvolněné SCVMM 2008 je očekáváno koncem srpna (o SCVMM 2008 připravuji také samostatný článek), ale malou ochutnávku jeho beta verze si můžete prohlédnout na obr. 4.

Radim Petržela, MHM computer


Obr. 4

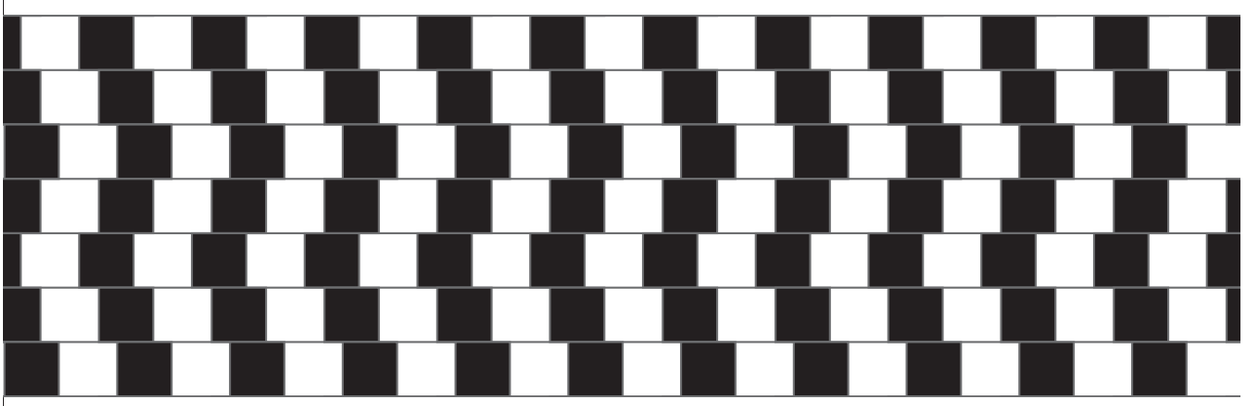
Informační bezpečnost a její hrozby

Informační bezpečnost je nepřetržitým úsilím o ochranu jednoho z nejcennějších aktiv každé společnosti – informací. Pro stále větší počet společností jsou informace a data klíčovým faktorem jejich podnikání a s tím také roste důležitost jejich ochrany. Uvádí se, že i ty největší a nejlépe kapitalizované banky by zkrachovaly, pokud by nebyly schopny své klienty obsluhovat během tří po sobě jdoucích dnů. Nastalý „run na banku" a výběr hotovosti znepokojených klientů by pak způsobil její insolventnost, a to i tehdy, pokud by po odstranění výpadku provoz obnovila. Protože každá banka disponuje větším množstvím kamenných poboček a většinou rovněž systémem internetového bankovnictví, nejpravděpodobnější událostí, která by banku na tři dny vyřadila z provozu, je ztráta dat a tedy informací o klientských účtech.

Vedle zajištění dostupnosti dat je dalším důležitým aspektem informační bezpečnosti zabezpečení informací proti neautorizovanému přístupu a jejich zneužití. Pro příklad vyzrazení citlivých informací nemusíme chodit daleko. Na jaře letošního roku došlo u atlantského zpracovatele plateb pro banky a obchodníky CardSystems Solutions ke krádeži informací o 40 milionech platebních karet. Několik set platebních karet byly v důsledku této události nuceny zablokovat i české banky. Ke zcizení čísel karet, dat expirace a bezpečnostních kódů karet z databáze použil útočník počítačový virus.

S rozvojem informační a komunikační techniky na jednu stranu roste tempo a objem zpracovávaných informací, které pohánějí motor ekonomiky. Z druhé strany však s sebou tento rozvoj přináší nová ohrožení, kterým je nutno čelit. Komplexnost informačních a komunikačních systémů i celé IT infrastruktury, ve které se stále více prosazují virtualizační techniky, dosáhla bodu, kdy zajištění vysoké bezpečnosti a dostupnosti dat stojí stále více úsilí a prostředků. Podobně s nástupem nových technologií a způsobů komunikace vyrostla celá plejáda nových bezpečnostních rizik v oblasti počítačové bezpečnosti, jako jsou phishing, pharming či spyware, které připravily odborníkům v počítačové bezpečnosti nejednu horkou chvilku (viz přehled soudobých hrozeb počítačové bezpečnosti). Četnost aktualizace antivirových a antispamových programů se z řádu měsíců a let posunula do řádu hodin a dní. Boj za bezpečnost informací se rozho-

UKÁŽEME VÁM SPRÁVNÝ ÚHEL POHLEDU



www.convenio.cz

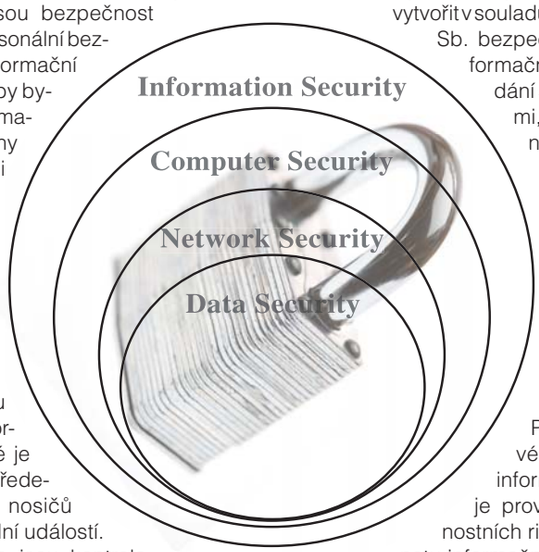
Nezávislé konzultační služby
Další infmormace Vám poskytneme na e-mailu: offce@convenio.cz
CONVENIO CONSULTING

Soudobé hrozby počítačové a internetové bezpečnosti	
Název hrozby	**Popis hrozby**
Hacking	Hacking spočívá v úsilí o narušení soukromí uživatele počítačových sítí či poškození počítačových entit, jako jsou soubory, programy či webové stránky, útočníkem (hackerem). Stupeň nebezpečnosti hackingu sahá od pouhého znepříjemňování činnosti uživatelů až k nelegálním aktivitám, jako je krádež souboru dat.
Phishing	Phishing (někdy překládán do češtiny jako rhybaření) je podvodná technika používaná na internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) od obětí útoku. Jejím principem je rozesílání e-mailových zpráv, které se tváří jako oficiální žádost banky či jiné podobné instituce a vyzývají adresáta k zadání jeho údajů na odkazovanou stránku. Tato stránka může například napodobovat přihlašovací okno internetového bankovnictví a uživatel do něj zadá své přihlašovací jméno a heslo. Tím tyto údaje prozradí útočníkům, kteří jsou poté schopni mu z účtu vykrást peníze.
Pharming	Pharming se snaží přesměrovat provoz legitimních webových stránek na stránky falešné, ale podobně vypadající, na kterých se pokusí vylákat od návštěvníka citlivé údaje jako například přihlašovací údaje do internetového bankovnictví. Jednou z metod pharmingu je napadení DNS serveru, který udržuje seznam internetových domén a příslušných DNS adres. Druhá metoda je založena na útoku proti jednotlivým počítačům. Počítače s operačními systémy Windows obsahují takzvaný soubor hosts, který funguje obdobně jako DNS server. Jestliže se útočníkovi podaří do tohoto souboru zapsat adresu své podvodné stránky, pak je efekt pro uživatele stejný jako v předchozím případě.
Malware	Malware je obecný termín pro škodlivý programový kód či software, který se bez vědomí uživatele snaží proniknout do počítačového systému a poškodit jej nebo z něj zcizit citlivé údaje. Malware zahrnuje širokou škálu škodlivých programových kódů zahrnující počítačové viry, červy, trojany, rootkity, spyware a další.
Spyware	Spyware je program, který využívá internetu k odesílání dat z počítače bez vědomí jeho uživatele. Někdy odesílá pouze data typu přehledu navštívených stránek či nainstalovaných programů za účelem zjištění potřeb nebo zájmů uživatele. Existuje ale i spyware odesílající hesla a čísla kreditních karet nebo spyware fungující jako zadní vrátka. Spyware se často šíří jako součást sharewaru. K druhům spywaru patří adware (obtěžující reklama), browser helper object (změna parametrů prohlížeče), hijacker (změna domovské stránky), dialer (přesměrování volání modemu), keystroke logger (odpozorování stisků tlačítek klávesnice) a remote administration (vzdálená správa počítače neautorizovanou osobou).
Ransomware	Ransomware je druh malwaru, který má formu kryptoviru, kryptotrojanu nebo kryptočerva. Útočník prostřednictvím ransomwaru zakóduje určité soubory uživatele a poté požaduje výkupné za poskytnutí klíče k jejich odkódování.
Počítačový virus	Virus je škodlivý počítačový kód, který se připojí k programu nebo k souboru a může poškodit software, hardware i soubory. Počítačový virus se šíří z počítače na počítač. Skutečný virus se však nebude rozšiřovat bez zásahu člověka. Někdo musí nastavit sdílení souboru nebo poslat e-mail, aby se virus rozšířil. Viry zpravidla infikují takzvané proveditelné soubory (nejčastěji s příponou .exe), jejichž spuštěním dojde k rozmnožení virového kódu.
Worm	Worm (červ) se šíří z počítače na počítač, ale na rozdíl od viru má možnost se šířit bez jakéhokoli přičinění člověka. Worm převezme kontrolu nad funkcemi v počítači, které mohou přenášet soubory nebo informace, a může se tak přenášet samostatně. Vysokým nebezpečím červů je jejich schopnost replikace. Červ může například rozesílat kopie sebe sama všem členům e-mailového adresáře, jejichž počítače poté provedou to samé, což způsobí dominový efekt. Worm může neúměrně zatěžovat operační paměť nebo přenosovou kapacitu sítě a vést tak k zahlcení či zhroucení počítačového systému či sítě.
Trojan	Trojský kůň je počítačový program, který se jeví jako užitečný, ale ve skutečnosti působí škody. Trojští koně se šíří tím, že jsou uživatelé zlákáni k otevření programu, protože si myslí, že pochází z legitimního zdroje. Některé trojany jsou pouze obtěžující, jiné mohou vážně poškodit systém či vymazat důležitá data. Na rozdíl od virů a červů se samy nereprodukují infikováním dalších souborů ani samy sebe nereplikují.
Rootkit	Rootkit je sada počítačových programů a technologií, pomocí kterých lze maskovat přítomnost zákeřného softwaru v počítači (například přítomnost virů, trojských koňů, spywaru a podobně). Rootkity umožňují skrývat běžící procesy, soubory a systémové údaje, takže pomáhají útočníkovi zůstat skrytý.
Spam	Spam je nevyžádané masově šířené sdělení (nejčastěji reklamní) šířené internetem. Původně se používalo především pro nevyžádané reklamní e-maily, postupem času tento fenomén postihl i ostatní druhy internetové komunikace – např. diskuzní fóra, komentáře nebo instant messaging.

řel a válečná vřava na bojové linii už asi, bohužel, nikdy neutichne.

ZÁKLADNÍ POJMY

Často se setkáváme s pojmy, jako je bezpečnost dat, bezpečnost sítí, počítačová bezpečnost a informační bezpečnost. Z těchto termínů je informační bezpečnost nejširším pojmem, neboť zahrnuje jak bezpečnost počítačovou, tak další druhy ochrany informací, jakými jsou bezpečnost personální a fyzická. Personální bezpečnost ve vztahu k informační bezpečnosti zajišťuje, aby byla osobám, které s informacemi nakládají, vymezeny pro práci s informacemi jasná pravidla, aby byly v dodržování těchto pravidel proškoleny a aby byla prověřena a kontrolována spolehlivost těchto osob. Fyzická bezpečnost si klade za cíl zamezit neoprávněnému přístupu k fyzickým nosičům informací a systémům, které je zpracovávají, ale také předejít poškození těchto nosičů a systémů např. při živelní události. Zahrnuje opatření, jako jsou kontrola vstupu a režimová opatření či instalace hlásičů požáru a elektronických zabezpečovacích systémů. Zajištění personální, fyzické i počítačové bezpečnosti vyžaduje zavedení důsledných procedurálních opatření, která budou v organizaci uvedena v život zpravidla prostřednictvím vnitřních organizačních směrnic.



Při realizaci projektů v oblasti informační bezpečnosti se využívá především metodika norem ISO 27001 a ISO 27002 a dále zákonné normy, které se vztahují k zabezpečení zvláště chráněných informací. Norma ISO 27002 je sbírkou nejlepších bezpečnostních praktik a může být využita jako kontrolní seznam všech bezpečnostních opatření, které je nutno pro bezpečnost informací v organizaci udělat. Norma ISO 27001 pak normu ISO 27002 doplňuje specifikací požadavků, jak v organizaci zavést efektivní systém řízení bezpečnosti informací (ISMS).

Pro určité typy informací je zákonem stanoven přísnější režim jejich ochrany. Patří sem např. zdravotní a jiné osobní a citlivé údaje, informace chráněné bankovním a obchodním tajemstvím či informace utajované podle zákona o ochraně utajovaných informací. V souladu se zákonnými požadavky je pak nutno zavést na jejich ochranu odpovídající bezpečnostní opatření, která jsou zanesena v bezpečnostní dokumentaci a směrnicích. V oblasti ochrany utajovaných informací je tak potřeba vytvořit v souladu se zákonem č. 412/2005 Sb. bezpečnostní dokumentaci informačního systému pro nakládání s utajovanými informacemi, v oblasti ochrany osobních údajů pak musí dojít k realizaci a zdokumentování technicko-organizačních opatření na ochranu osobních údajů podle zákona č. 101/2000 Sb.

SYSTÉMOVÉ ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

Předpokladem systémového řízení bezpečnosti informací v každé organizaci je provedení analýzy bezpečnostních rizik, která stanovuje hodnotu informačních aktiv, odhaluje slabá místa v organizaci a identifikuje i ohodnocuje hrozby, které v oblasti informační bezpečnosti existují. Analýza rizik je východiskem pro návrh bezpečnostních opatření. Tato opatření, jsou-li vhodně zobecněna, tvoří základ bezpečnostní politiky informací, která v obecné podobě stanovuje cíle a prostředky v oblasti ochrany informací organizace a definuje odpovědnosti, pravidla a postupy, jak jich dosáhnout.

Úkolem bezpečnostního projektu pak je praktická implementace bezpečnostní politiky v prostředí dané organizace. Bezpečnostní projekt zahrnuje plán realizace bezpečnostních opatření jak v oblasti personální a fyzické bezpečnosti, tak v oblasti bezpečnosti informačních a komunikačních systémů. Technická opatření k zajištění bezpečnostních opatření je potřeba promítnout do bezpečnostní architektury IT organizace, to znamená najít jednotlivé komponenty IT infrastruktury i vhodné aplikační programové vybavení a na ně navázat

CONVENIO CONSULTING

Nabídka konzultačních služeb Convenio Consulting v oblasti informační bezpečnosti má za cíl zajistit komplexní ochranu informací v dané organizaci a zahrnuje zpracování dokumentace a realizaci projektů v těchto oblastech:

- *Analýza bezpečnostních rizik a klasifikace informací*
- *Bezpečnostní politika informací*
- *Bezpečnostní projekt IS/IT a tvorba bezpečnostních směrnic*
- *Bezpečnostní audit IS/IT a penetrační testy*
- *Disaster Recovery plán*
- *Projekt ochrany osobních údajů*
- *Bezpečnostní dokumentace IS pro nakládání s utajovanými informacemi*

Soutěž

V této rubrice přinášíme soutěžní otázky a jsme zvědavi na vaše odpovědi.

Na obrázku vidíte hardwarovou komponentu z minulého století. Její dnešní podoba je díky neustálému vývoji jiná, ale tato komponenta je stále nezbytná.

Dnešní otázka zní:

Co je ukázáno na obrázku?



OTÁZKY Z MINULÉHO ČÍSLA ZNĚLY:

Jak byste definovali velikost IT svého podniku? Používáte ve svém podniku externí disková pole? Jak důležitá je při nákupu nového serveru nebo diskového pole pro váš podnik otázka úspory elektrické energie?

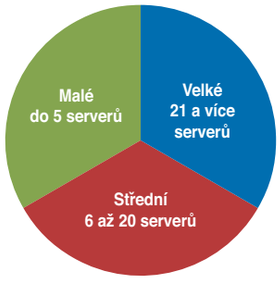
Všechny tři otázky se týkaly velikosti IT a ekologie. Z mnoha zaslaných odpovědí jsme pro vás připravili souhrnnou statistiku, která je pro přehlednost znázorněna grafy. Zřejmé je, že střední a velké podniky používají disková pole. Překvapivým výsledkem je zjištění, nezávislé na velikosti podniku, že stále více společností myslí i na úsporu elektrické energie. Děkujeme všem čtenářům, kteří obětovali svůj čas a díky nimž jsme získali hodnotné podklady.

Z mnoha odpovědí byl vylosován pan Radek Pohnán z Prahy. Gratulujeme a zasíláme malou pozornost od společnosti Tandberg Data.

Jak důležitá je při nákupu nového serveru nebo diskového pole pro váš podnik otázka úspory elektrické energie?



Jak byste definovali velikost IT svého podniku?



Používáte ve svém podniku externí disková pole?



ODPOVĚDI NA AKTUÁLNÍ OTÁZKU PROSÍM PIŠTE DO ODPOVĚDNÍHO FORMULÁŘE NA WWW.DATAVPECI.CZ. ODPOVĚĎ NA SOUTĚŽNÍ OTÁZKU NAJDETE V PŘÍŠTÍM ČÍSLE. NA VÝHERCE, KTERÝ BUDE VYLOSOVÁN ZE SPRÁVNÝCH ODPOVĚDÍ DNE 29. 10. 2008, ČEKÁ JAKO OBVYKLE DÁREK, TENTOKRÁT OD SPOLEČNOSTI HITACHI.

…dokončení ze str. 14

jednotlivá požadovaná bezpečnostní opatření. Netechnická (fyzická, personální a procedurální) opatření se zpracují a realizují v podobě bezpečnostních směrnic.

V oblasti krizového plánování se zpracovává Disaster Recovery plán, jehož cílem je zajistit obnovu funkčnosti IT systémů organizace v případě, že nastane havarijní situace, a zaručit tak požadovanou úroveň dostupnosti informací.

Důležitým nástrojem pro poznání objektivního stavu informační bezpečnosti v organizaci je bezpečnostní audit ICT, který identifikuje možné nedostatky v ICT infrastruktuře a v systému řízení bezpečnosti a je předpokladem zpracování komplexního řešení bezpečnosti informací. Pro zjištění úrovně zabezpečení počítačových sítí se pak provádějí penetrační testy.

Jaroslav Fojtík, Convenio Consulting



PARLAMENT
VLÁDA
SAMOSPRÁVA

Zpravodajský měsíčník
pro státní správu a podnikatele

Mějte skutečný rozhled

čtěte Parlament • vláda • samospráva

www.parlament-vlada.cz

E-mail:
info@parlament-vlada.cz
redakce@parlament-vlada.cz