

Hrozby bezpečnému provozu IT

Bezpečný provoz datových center nám zajišťuje kritická síťová infrastruktura (NCPI – Network Critical Physical Infrastructure). Jak je to s bezpečností jí samotné?

V následujících odstavcích se budeme zabývat kritickou fyzickou infrastrukturou datových center v její vazbě na bezpečnost IT systémů. Podíváme se na používané technologie a uvedeme jejich vazbu na funkci a bezpečnost. Závěrem se seznámíme s modely fungování technologického dohledu těchto technologií a jejich významem pro provoz datových center.

KRITICKÁ SÍŤOVÁ INFRASTRUKTURA DATOVÉHO CENTRA

V datových centrech nejčastěji řešíme bezpečnostní problémy související se zajištěním bezproblémového chodu hardwarových prostředků. Tyto prostředky mají zcela zásadní vliv na dostupnost aplikací a dat, neboť tvoří základní podmínky pro chod samotné výkonné části IT. Pro uvedené prostředky

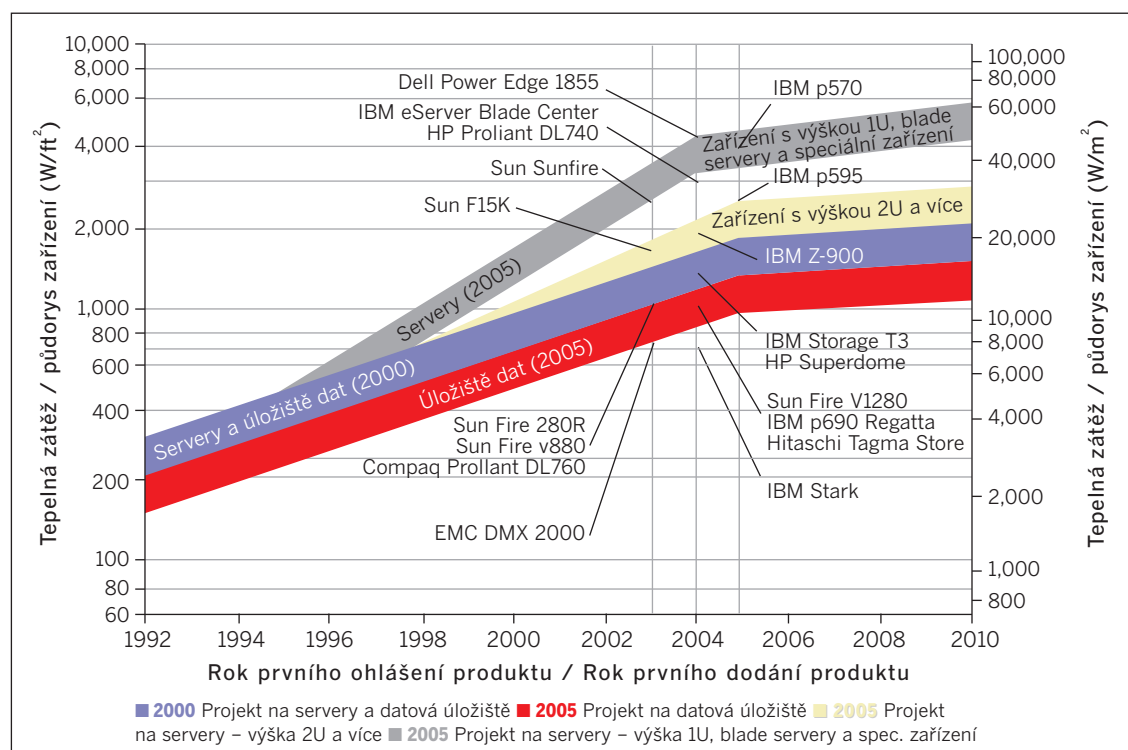
se používá souhrnné označení NCPI (Network Critical Physical Infrastructure).

Za nejdůležitější je v této oblasti považován systém napájení. Vztah mezi fungováním hardwaru pro IT aplikace (např. serveru nebo diskového pole) ve vztahu k jeho napájení elektrickou energií je zcela zřejmý. Tento faktor je také často vnímán jako bezpečnostní hrozba pro IT aplikace a podílí se značnou měrou na těchto rizicích.

Systém napájení se skládá z jednoho nebo více přívodů napájení z rozvodné soustavy (u větších datových center i přímo z vysokonapěťové), soustavy rozvaděčů, náhradních zdrojů elektrické energie, střídavých i stejnosměrných záložních systémů a kabelových propojení. Ne-

dílnou součástí je dále řídicí systém, který zajišťuje správnou distribuci elektrické energie. Denní praxe dále ukazuje, že velice důležitou součástí návrhu systému napájení jsou nejenom správně použité komponenty a jejich vhodné kombinace, ale i topologie celého systému.

Nevhodné topologie systému napájení obsahují zbytečné neredundantní body (Single Point of Failure – SPoF), které nejenom snižují dostupnost systému, ale zhoršují také jeho možnosti servisu za provozu. Jako příklad může sloužit právě zmiňovaný řídicí systém. V mnoha systémech napájení je použit řídicí systém na bázi jediného PLC (Programmable Logic Controller – programovatelný logický automat), který řídí napájení datového centra ve dvou větvích napájení.



OBR. 1:
NÁRŮST POŽADAVKŮ
NA CHLAZENÍ
V DATOVÉM CENTRU
V ZÁVISLOSTI NA DOBĚ
NASAZENÍ
NEJZNAMĚJŠÍCH TYPŮ
SERVERŮ.

© 2004 - 2006
ALTRON

monitoring nonIT technologií datového centra

Neuzavřené poplachi Všechny poplachi Uzávěrečné záznamy Nový záznam Všechny záznamy On-line dohled Konfigurace jističů Odnímat

Všechny poplachi

Čas	Vložit	Zařízení	Poplach	Uzavřeno	Uzavřel	Text
0 0	16.10.2007 20:14:54	SYSTEM SMS_server	9902	16.10.2007 20:14:54	SYSTEM	STL_CIRMAN se odhlásil ze systému rozeslání alarmu.
1 0	16.10.2007 14:20:32	SYSTEM VYTAH_2	3101	16.10.2007 21:08:23	STL_BROZEK	porucha
0 0	16.10.2007 06:35:20	SYSTEM SMS_server	9901	16.10.2007 06:35:20	SYSTEM	STL_CIRMAN se přihlásil do systému rozeslání alarmu.
1 1	16.10.2007 03:49:14	SYSTEM KLIMA_1.12	2101	16.10.2007 21:06:49	STL_BROZEK	porucha
1 1	16.10.2007 01:50:34	SYSTEM KLIMA_1.2	2101	16.10.2007 21:07:04	STL_BROZEK	porucha
1 1	16.10.2007 00:33:55	SYSTEM KLIMA_1.8	2101	16.10.2007 21:07:12	STL_BROZEK	porucha
1 1	15.10.2007 21:41:07	SYSTEM KLIMA_1.9	2101	16.10.2007 21:07:29	STL_BROZEK	porucha
0 0	15.10.2007 20:24:20	SYSTEM SMS_server	9902	15.10.2007 20:24:20	SYSTEM	STL_CIRMAN se odhlásil ze systému rozeslání alarmu.
1 1	15.10.2007 18:38:47	SYSTEM KLIMA_1.3	2101	16.10.2007 21:07:31	STL_BROZEK	porucha
1 1	15.10.2007 16:36:56	SYSTEM KLIMA_1.11	2101	16.10.2007 21:07:32	STL_BROZEK	porucha
7 0	15.10.2007 11:05:29	SYSTEM VYTAH_2	3101	15.10.2007 21:43:05	STL_BROZEK	porucha
4 + 0	15.10.2007 08:44:46	SYSTEM RU1	1801			poloha nikerého prvku neodpovídá požadavku
2 + 0	15.10.2007 08:33:56	SYSTEM RNA1.8	1601			poloha nikerého prvku neodpovídá požadavku
0 0	15.10.2007 07:57:30	SYSTEM SMS_server	9901	15.10.2007 07:57:30	SYSTEM	STL_CIRMAN se přihlásil do systému rozeslání alarmu.
1 + 0	15.10.2007 07:15:36	SYSTEM RNA1.4	1601			poloha nikerého prvku neodpovídá požadavku
0 0	15.10.2007 06:18:53	SYSTEM SMS_server	9902	15.10.2007 06:18:53	SYSTEM	STL_LEBL se odhlásil ze systému rozeslání alarmu.
1 + 0	14.10.2007 23:13:23	SYSTEM RNA1.2	1601			poloha nikerého prvku neodpovídá požadavku
4 + 0	14.10.2007 01:23:42	SYSTEM RU3	1801			poloha nikerého prvku neodpovídá požadavku
0 0	14.10.2007 00:14:50	SYSTEM SMS_server	9902	14.10.2007 00:14:50	SYSTEM	STL_KOLLAR se odhlásil ze systému rozeslání alarmu.
1 2	14.10.2007 00:08:47	SYSTEM KLIMA_1.1	2101	16.10.2007 21:07:52	STL_BROZEK	porucha
1 + 1	13.10.2007 23:31:25	SYSTEM KLIMA_3.3	2101			porucha

OBR. 2: UKÁZKA VÝPISU Z MONITORINGU DATOVÉHO CENTRA.

Při selhání řídicího centra nebo jeho systému napájení dojde k selhání funkce obou větví napájení. Jedná se tedy o klasický SPoF. Návrhem vhodné topologie s modulárním ŘS s decentralizovanou funkcí tento SPoF eliminujeme.

Je zřejmé, že díky vhodné zvolené topologii zajistíme nejenom vysokou dostupnost napájení, ale také možnost opravy a údržby těchto částí za provozu, což je vzhledem ke stále se rozšiřujícímu požadavku na provoz IT v režimu 7x24x365 stále významnější.

Systém napájení není však zdaleka jedinou technologií NCPI v datových centrech. Druhým systémem, který zásadně ovlivňuje dostupnost a tudíž se stává hrozbou v případě poruchy nebo selhání, je systém chlazení. V minulých letech se tento systém nepovažoval za přímou hrozbu, neboť jeho dopad na funkci v případě selhání nebyl okamžitý. Moderní hardware se však vyznačuje výrazně vyšší výkonovou hustotou v datových stojanech (rack), která se obvykle posuzuje v kW/rack nebo v kW/m², a ta vyvolává zvýšenou potřebu chlazení celého zařízení – viz obr. 1.

V praxi graf z obr. 1 znamená, že reálně osazené stojany technologií 2RU a vyšší mohou dnes dosahovat výkonové hustoty 6–10 kW/rack, technologie 1RU 12–15 kW/rack, Blade & Custom dokonce 15–22 kW/rack. Při těchto výkonových hustotách se při ztrátě funkce chladičového výkonu dosahuje přehřátí tohoto hardwaru v řádu i jednotek minut.

V takto krátkém čase není možno na situaci adekvátně reagovat a důsledek může být stejný jako při výpadku napájení. V lepším případě dojde k regulárnímu odstavení serveru (shutdown), v horším dokonce k odpojení zdroje z důvodu přehřátí. Je totiž třeba mít na paměti, že prakticky veškerá dodaná elektrická energie se mění v teplo, a to se odvádí nucenou výměnou vzduchu. I zde je důležité nejen použití vhodných komponentů chlazení a jejich správná kombinace, ale také topologie chladičového systému analogicky odpovídající systému napájení. Opět je důležitá eliminace SPoF v systému chlazení. Systém chlazení se tak z pohledu NCPI integrátora stává stejně důležitou – kritickou – částí z hlediska dostupnosti služeb IT jako systém napájení.

Dalšími systémy, které se zahrnují do NCPI, jsou:

- **systém stabilního hasičího zařízení (SHZ)**, zajišťující automatizované hašení požáru v prostoru datového sálu a dalších kritických prostorech (např. Power room – místnost záložního napájení). Patří sem systémy na bázi inertních plynů, chemických plynů, vodní mlhy a některé další zhašecí systémy;
- **přístupové systémy (Access System – ACS)**, kamerové systémy (CCTV) sloužící ke sledování přístupu osob do prostor s IT zařízeními a infrastrukturou datového centra;
- **elektrický zabezpečovací systém (EZS)**, sledující narušení chráněných prostor datového centra;

- **elektrická požární signalizace (EPS)** včetně detekce požáru, sloužící k ochraně osob a technologií datového centra, spolupracuje úzce se systémem SHZ;
- **datová kabeláž** (optická, metalická, patch panely, optické vany);
- **systémy fyzické infrastruktury** (stojany, zdvojená podlaha, stínící systémy, atd.);
- **další podružné systémy.**

Prakticky u všech těchto systémů můžeme nalézt vazbu mezi jejich funkcí a funkcí IT a jsou tedy rovněž potenciální hrozbou pro IT provoz. Například při spuštění systému SHZ, a to i plánem, dochází zpravidla i k vypnutí všech systémů napájených elektrickou energií (převažující většina požárního nebezpečí datového centra vyplývá ze systému napájení nebo systémů distribuce). Nastává tedy přímé ohrožení funkce IT v souvislosti s funkcí SHZ. Zde je zcela klíčové provést správný návrh projektu těchto technologií také s ohledem na vliv na samotný provoz IT v přímém kontextu s provozními a bezpečnostními opatřeními, resp. analýzou rizik v dané lokalitě.

Dalším příkladem může být nesprávné stavební řešení s ohledem na hmotnost instalovaných zařízení. Dalším důsledkem miniaturizace a zahušťování výkonu v hardwarových prostředcích IT je stále se zvyšující hmotnost stojanů osazených serverovou a další aktivní IT technikou (v minulosti cca 500 kg, dnes běžně 1 000 kg i více). Zde hrozí riziko překročení původně projektovaných únosností podlah a poškození nebo zničení instalované techniky IT.

SYSTÉM MONITORINGU

V neposlední řadě NCPI zahrnuje systémy monitoringu (technologického dohledu) výše uvedených technologií. Je zcela pochopitelné, že pokud považujeme výše uvedené technologie za kritické pro provoz datového centra a při nesprávné funkci jsou hrozbou pro samotný provoz, klademe také velký důraz na monitorování jejich stavu. Důsledné monitorování umožňuje v mnoha případech předejít selhání funkce a vzniku havárie. Pokud již k selhání dojde, systém monitoringu umožní rychlejší a efektivnější analýzu situace a výrazně tak zkrátí dobu opravy technologie. Přidanou hodnotou monitorování provozu je také možnost provádět analýzy provozu ve vztahu k provozním nákladům, servisu, opravám a efektivitě provozu – viz obr. 2.

Monitoring v oblasti NCPI se dělí na dvě základní oblasti. Tou první je sledování samotných technologií (systémy napájení – motorgenerátory, UPS, napájení, rozvaděče, systémy chlazení – sálové jednotky přesné klimatizace, vnější jednotky, chillery¹, SHZ, EZS, EPS, ACS atd.). Zde se systém monitoringu zaměřuje na sledování a logování provozních veličin jednotlivých technologií, provozních a poruchových stavů a jejich vyhodnocování v kontextu ostatních technologií nebo jejich částí.

Druhou částí je monitoring prostředí datového centra. Zde se v souladu s instalovanými technologiemi sledují parametry technologií tak, jak působí na instalované IT. Výčet parametrů je poměrně dlouhý, k základní patří: teplota, vlhkost a prašnost vzduchu ve více místech datového sálu, parametry elektrické energie napájející IT, přítomnost vody, tlaková diference sálů atd.

Tato oblast je velice důležitou součástí monitorovacího systému, neboť sleduje dopady instalovaných NCPI technologií na samotnou techniku. Zde se předpokládá, že tyto vlivy jsou předmětem již samotného návrhu. Praxe nás však stále přesvědčuje, že ne vždy odpovídají podmínky uvažované při návrhu datového centra reálně použitým řešením. Jednoduchý příklad: datový sál, posta-

vený před třemi lety, je navržen na maximální příkon 5 kW/rack, což odpovídá podmínkám v tomto období. Dnes se instalují servery a jiné aktivní prvky, které přináší hustotu 8 kW/rack a vyšší. Důsledkem toho dochází lokálně nebo globálně k nesprávné cirkulaci chladného vzduchu na datovém sále a tedy k přehřívání zařízení především v horních částech stojanů, čímž vzniká bezpečnostní incident. Při kvalitně provedeném monitoringu prostředí lze tuto špatnou cirkulaci odhalit pomocí měření teploty ve správně zvoleném místě datového sálu již s předstihem.

Ani ten nejlepší monitorovací systém nezajistí sám o sobě zvýšení dostupnosti a zároveň s tím snížení bezpečnostních hrozeb vyplývajících z nesprávné funkce technologií NCPI. Monitorovací systém poskytuje velké množství dat, které je třeba řádně interpretovat a především na ně odpovídajícím způsobem reagovat. K tomu je zapotřebí zajistit trvale obsazené dohledové pracoviště, a dále pak je nutná servisní organizace, která je schopna provést včas nezbytný zásah. Pouze dokonalá souhra monitorovacího systému a organizačních opatření umožňuje minimalizovat tato rizika.


MODELY PROVOZU

Existují dva modely úspěšného provozování datového centra, které naplňují předchozí podmínky. Ten první je vhodný pro datová centra se střední dostupností; v tomto případě provozovatel datového centra provozuje lokální monitorovací systém s vlastními operátory, kteří obvykle zabezpečují základní údržbu a provoz. Zároveň však servisní organizace periodicky provádí profylaktické prohlídky veškeré technologie a také veškerý poruchový servis v režimu offline – tj. při nahlášení poruchy operátory. V některých případech je tento provoz doplněn možností získání dat z monitorovacího systému servisní organizací za účelem vyhodnocení poruchového stavu pro zefektivnění a zrychlení oprav.

Druhým modelem je provozování datového centra specializovanou firmou, která plní funkci operátora i servisní orga-

nizace v režimu on-line. Tato organizace se stará o všechny provozní záležitosti datového centra a garantuje provozovateli parametry prostředí pro jeho chod. Tato poskytovaná komplexní služba se nazývá Technology Facility Management (TFM) a pro provozovatele zajišťuje nejvyšší míru dostupnosti a tedy eliminace bezpečnostních hrozeb v oblasti NCPI a nakonec i fyzické bezpečnosti.

ZÁVĚREM

V datových centrech se koncentruje nejen IT, ale i hrozby jeho bezpečnosti. Monitorovat je třeba dvě základní oblasti jeho provozu – provoz jednotlivých technologických prvků a provoz celkového prostředí. Zvláště náročné je monitorování celkového prostředí datového centra, protože se zde pracuje s velkým množstvím dat. To vede ke zvláštním požadavkům na personál schopný skloubit koncepční a organizační opatření s každodenním provozem monitorovacího systému. Je se rovněž třeba rozhodnout i pro model provozování datového centra, tj. zda použít vlastní operátory anebo i touto prací pověřit servisní organizaci. Neboli zde platí – jak pečlivě bude analýza přípravy chodu datového centra provedena, tak kvalitně pak bude vše ve finále fungovat. 

PETR DING
petr.ding@altron.net



ING. PETR DING

Absolvent ČVUT FEL, obor radioelektronika. Dříve pracoval ve společnostech ČKD Hořovice a KVR Technik, v současnosti je hlavním inženýrem pro datová centra u firmy Altron, a.s.

MANAGEMENT SUMMARY

Článek popisuje základní prvky kritické síťové infrastruktury datového centra, systém jeho monitoringu a základní modely provozu. Jsou zde popsány dvě základní oblasti monitoringu v oblasti NCPI a dva modely úspěšného provozování datového centra. Článek upozorňuje na nutnost pečlivé analýzy provozu datového centra a nezbytnost jeho obsluhy kvalitním personálem, schopným sladit organizační opatření s praktickými provozními otázkami.

¹ Vzduchové chladiče kapaliny, které se obvykle používají jako primární zdroje chladu pro klimatizační a chladicí jednotky v budovách.