

# Bezpečnost fyzické síťové infrastruktury

Na bezpečnost IT můžeme pohlížet jako na míru neohroženosti funkce technologií – tedy na dostupnost aplikací a dat. Bezpečnostní hrozby, které jejich chod ohrožují, lze rozdělit na tři základní oblasti.

Petr Ding

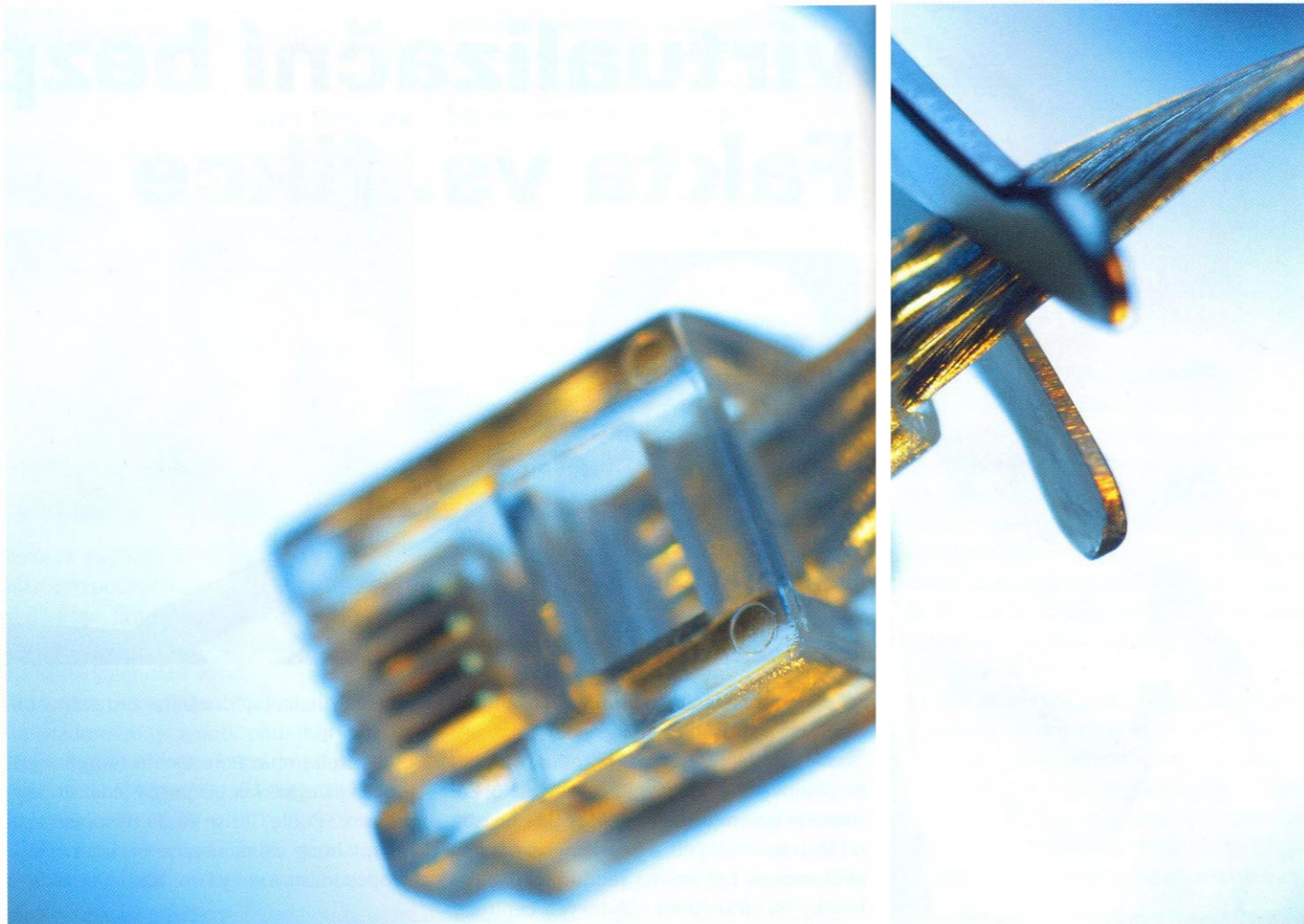
**T**ou první je datová a softwarová doména – nejčastější zdroj hrozeb, kam patří spam, počítačové viry, softwarové chyby, chyby LAN a WAN, vnější nepovolený přístup nebo například zneužití dat. Fyzická bezpečnost (Physical Security) hardwarových prostředků nebývá obvykle vnímána jako hlavní zdroj hrozeb – sem patří poruchy hardwaru, chyba obsluhy, krádež zařízení nebo dat, vnitřní nepovolený přístup, zneužití zařízení, přírodní katastrofa, požár a další (tedy narušení hardwarových prostředků v místě jejich instalace, obvykle v datovém centru nebo v serverovně). Třetí oblastí jsou technologie, zajišťující bezproblémový chod hardwarových prostředků IT. Tyto technologie mají zcela zásadní vliv na dostupnost aplikací a dat, neboť tvoří základní podmínky pro chod samotné výkonné části IT. Pro tyto prostředky se používá souhrnné označení NCPI (Network Critical Physical Infrastructure).

Vztah fungování hardwaru pro aplikace IT (např. serveru nebo diskového pole) vůči jeho napájení elektrickou energií je zřejmý a je často vnímán jako jedna z největších bezpečnostních hrozeb pro IT aplikace, protože se na nich často podílí. Systém napájení se skládá z jednoho nebo více přívodů napájení z rozvodné soustavy (u větších DC se používá vn připojení), soustavy rozvaděčů, náhradních zdrojů elektrické energie, záložních systémů střídavých (AC) a stejnosměrných (DC) a kabelových propojení. Nedílnou součástí je řídicí systém zajišťující správnou distribuci elektrické energie. Důležitou součástí návrhu systému napájení jsou nejen správně užití komponenty a jejich vhodné kombinace, ale také topologie celého systému. Vhodně zvolenou topologií zajistíme jak vysokou dostupnost napájení, tak možnost opravy a údržby těchto částí za provozu, což je vzhledem k stále se zvětšující nutnosti provozovat IT v režimu „24x7x365“ stále důležitější.

Systém napájení není však zdaleka jedinou technologií NCPI v datových centrech. Druhým systémem, který zásadně ovlivňuje

V takto krátkém čase není možno na situaci dostatečně rychle reagovat a důsledek může být stejný jako při výpadku napájení. Buď dojde k regulárnímu odstavení serveru, nebo k odpojení zdroje z důvodu přehřátí. Proto i zde je nutné nejen použití vhodných

podružné systémy. Prakticky u všech těchto systémů můžeme nalézt vazbu mezi jejich funkcí a funkcí IT, a jsou tedy také potenciální hrozbou pro IT provoz. Zde je zcela klíčový správný návrh těchto technologií také s ohledem na vliv na samotný pro-



dostupnost, a tudíž se stává hrozbou v případě poruchy nebo selhání, je systém chlazení. V minulých letech nebyl považován za přímou hrozbu, neboť jeho dopad na funkci v případě selhání nebyl okamžitý. Se zmenšováním hardwaru v IT se však zvyšuje výkonová hustota v datových stojanech (rack), která se obvykle vyjadřuje v kW/rack nebo v kW/m<sup>2</sup>.

Při současných výkonových hustotách, které se pohybují u technologií 2RU, respektive technologií 1RU okolo 12–15 kW/rack, u žiletkových (blade) a speciálních řešení dokonce 15–22 kW/rack, dojde při selhání chlazení k přehřátí zařízení v řádu minut.

komponent chlazení a jejich správná kombinace, ale také topologie chladicího systému odpovídající k systému napájení. 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 hasicího zařízení (SHZ), přístupové systémy – Access System (ACS), elektronický zabezpečovací systém (EVS), elektrická požární signalizace (EPS) včetně detekce požáru, datová kabeláž, systémy fyzické infrastruktury (rakové stojany, zdvojená podlaha) a další

voz IT v přímém kontextu s provozními a bezpečnostními opatřeními, stejně jako analýzou rizik v dané lokalitě.

V neposlední řadě NCPI zahrnuje systémy pro sledování výše uvedených technologií. Důsledný monitoring umožňuje v mnoha případech předcházet selhání a vzniku bezpečnostních incidentů. Pokud již k selhání dojde, systém monitoringu umožní rychlejší a efektivnější rozbor situace, a výrazně tak zkrátí dobu opravy technologie. Za další přidanou hodnotu monitorování provozu je považována možnost provádět analýzy provozu ve vztahu k provozním nákladům, servisu, opravám a efektivitě provozu.

Monitoring v oblasti NCPI se dělí na dvě základní oblasti. Tou první je monitorování samotných technologií (systémy napájení, systémy chlazení) – 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 oblastí je monitoring prostředí datového centra. Zde se sledují parametry technologií tak, jak působí na instalované IT. Výčet všech parametrů je poměrně dlouhý, proto zde uvedeme pouze základní sledované veličiny: teplota, vlhkost a prašnost vzduchu v datovém sálu v řadě umístění, parame-

pak zázemí servisní organizace, která je schopna provádět údržbu a opravy technologických systémů datového centra. Pouze dokonalá souhra monitorovacího systému a personálně-organizačních opatření umožňuje tato rizika minimalizovat.

Existují dva modely úspěšného provozování datového centra, které naplňují předchozí podmínky. Ten první je vhodný pro datová centra se střední dostupností. Provozovatel datového centra provozuje lokální monitorovací systém s vlastními operátory, kteří obvykle zabezpečují základní údržbu a provoz. Zároveň však je sjednána servisní organizace, která periodicky provádí profy-

„ Systémem, který zásadně ovlivňuje dostupnost, a tudíž se stává hrozbou v případě poruchy nebo selhání, je systém chlazení. “

try elektrické energie napájející IT, zaplavení technologických prostor, tlaková diference sálů atd. Tato oblast je velice důležitou částí monitorovacího systému, neboť sleduje dopady instalovaných NCPI technologií na samotnou IT. I tyto vlivy jsou předmětem samotného návrhu NCPI. Praxe nás však stále přesvědčuje, že ne vždy jsou podmínky uvažované při návrhu datového centra stejné s reálně použitým řešením v oblasti IT. Jednoduchý příklad: datový sál, postavený před třemi lety, je navržen na maximální výkon 5kW/rack, což odpovídá hustotě výkonu IT v tomto období. Dnes se však instalují servery a ostatní aktivní prvky, které vyžadují hustotu 8 kW/rack a více. Důsledkem toho dochází lokálně nebo globálně k nesprávné cirkulaci chladného vzduchu v datovém sále a k přehřívání IT zařízení v horních částech rackových stojanů. Při správně provedeném monitoringu prostředí je možno s předstihem tuto špatnou cirkulaci odhalit pomocí měření teploty ve správném místě datového sálu.

Monitorovací systém pochopitelně nezajistí zvýšení dostupnosti a tím snížení bezpečnostních hrozeb vyplývajících z nesprávné funkce technologií NCPI – poskytuje pouze velké množství dat, které je třeba více či méně interpretovat a odpovídajícím způsobem na ně reagovat. K tomu je zapotřebí personální obsazení dohledového pracoviště, kde je monitorovací systém prezentován, a dále

laktické prohlídky veškeré technologie a také veškerý poruchový servis v režimu off-line, tedy 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.

Dalším modelem je provozování datového centra specializovanou organizací, která plní funkci operátora i servisní organizace v režimu on-line. Tato organizace se stará o všechny provozní záležitosti DC a garantuje provozovateli parametry prostředí pro chod DC. 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 i Physical Security.

Rychlý rozvoj IT technologií s sebou přináší nové hrozby a překážky pro vlastní infrastrukturu – ty vyplývají z rostoucích nároků těchto technologií na vytvářené podmínky provozu. Datová centra jsou typickým příkladem místa, kde se tyto potenciální problémy mohou koncentrovat – proto je nezbytné dokonale zvládnout návrh a provoz těchto center.

Autor pracuje jako produktový manažer ve společnosti Altron.