

## ROZHOVOR

## Virtualizace klade zcela nové nároky na bezpečnost

MARTIN NOSKA

O požadavcích na bezpečnost, které souvisejí s aktuálními změnami v IT infrastruktuře, s námi hovořil Jan Dymáček, ředitel společnosti Comguard.

## Co je podle vás největším rizikem při nasazení virtualizace?

U datových center jsme do značné míry přišli o možnost fyzického oddělení síťových segmentů. Virtualizovány jsou nejen interní aplikační servery, databáze a zálohovací systémy, ale mnohem častěji i uživatelský front-end spojený i s B2B nebo B2C a občas se setkáme i s virtualizovaným desktopem. To je zásadně jiné prostředí, než jaké ve firmách doposud panovalo a na jaké jsou naše bezpečnostní opatření připravena. Nyní mnohem více záleží na zapojení systémů Risk&Compliance.

## Risk&amp;Compliance, co konkrétně si má uživatel pod tímto pojmem představit?

Jedná se především o aplikační a vníro systémovou bezpečnost. Převáděno do praktických řešení například McAfee nabízí čtyři klíčové prvky: Integrity Monitor, Application Control, Change Control a Vulnerability Scanner. Integrity Monitor pro virtuální servery a databáze zajišťuje ochrany a monitorování změn souborů, práv a oprávnění včetně informací, kdo byl zalogován na systém, jaký proces nebo systém (editor) změnu provedl a zda změna byla provedena autorizovaným nebo neautorizovaným programem (malware aplikací). Integrity Monitor dále pokrývá komponenty jako databáze, síťové prvky a hlavně jednotný pohled na celé prostředí od virtuálního po fyzické.



U datových center jsme díky virtualizaci do značné míry přišli o možnost fyzického oddělení síťových segmentů.

JAN DYMÁČEK  
Executive Director,  
Comguard

## Zmínili jste monitor na úrovni databází, co všechno by měl sledovat?

Jedná se o komplexní přehled od aktivit (přihlášení/odhlášení, vytvoření uživatele a jeho role, změny hesel) přes změny návrhu (vytvoření/změna tabulky, indexy, uložené dotazy či procedury apod.) až po samotnou změnu dat (vlození, update, vymazání). Neměl bych zapomenout zmínit, že vše musí být centrálně nasaditelné, spravovatelné a reportovatelné. Centrální management (ePO) pak řídí i ostatní bezpečnostní prvky, jako jsou koncové stanice, DLP, Encryption a další.

## Monitoring ovšem často nestačí, lze změnám zabránit?

Ano, zde se uplatňuje právě již zmíněné řešení Application Control a Change Control. Application Control najde uplatnění na portálech typu B2C, B2B, ATM, core systémech a jinde, kde je jasně stanovený soubor běžících aplikací a jejich změn (ty lze řídit pomocí nástroje Change Control). Application Control nabízí aplikační audit serveru s možností vynucení spuštění jen autorizovaných aplikací, Change Control pak navazuje na obě předchozí řešení a nabízí preventivní ochranu a blokování. Pro doplnění bych zmínil ještě Vulnerability Scanning a manažer, který je důležitý zejména při pronájmu aplikací, serverů nebo outsourcingu jejich správy, jako kontrola jejich stavu od úrovně zranitelnosti OS, aplikací, databází až po uživatelské prostředí. Ve fyzic-

kém světě jsou pak kontrolovány aktivní prvky, firewally, proxy apod. Vysokou relevantnost zajišťují korelační moduly, které oznamují s vyšší prioritou jen uplatnitelná rizika – např. zranitelnosti u běžících služeb.

(mar) 10 0212

## ROZHOVOR

## Hostingové služby ve světle aktuálních požadavků

MARTIN NOSKA

O tom, jakými proměnami procházejí hostingové služby a před jakými požadavky a výzvami stojí, s námi hovořil Filip Špaček ze společnosti Master Internet.

## Co považujete za největší změnu v oblasti hostingu v posledních letech?

Co pozorujeme i na poptávce, je jednoznačný trend outsourcingu hostingových služeb. Firmy čím dál více preferují kompletní pronájem technologií včetně správy a případně i softwaru. Dalším výrazným odvětvím je samozřejmě virtualizace a obecně snaha o co nejefektivnější využití hardwarových prostředků. Tyto trendy samozřejmě ovlivnily i nabídku našich služeb.

## Jaké chyby nejčastěji firmy dělají při výběru hostingových služeb a podle kterých kritérií se obvykle rozhodují?

Často je to chyba v návrhu hardwarové konfigurace. Management firmy požaduje přesný návrh systému po vlastních IT kapacitách a nevyužije poradenství housingové společnosti, která s tím má mnohem bohatší zkušenosti z praxe. Stává se pak, že firma nakoupí technologie zbytečně předražené nebo naopak problémové z hlediska výkonu, kompatibility, servisu a celkové spolehlivosti.

## Které typy služeb v oblasti hostingu jsou mezi firmami v ČR nejoblíbenější?

Pomineme-li webhosting, který stále pokrývá široké spektrum zákazníků, tak je nejžádanější

službou housing vlastního hardwaru. Stále častěji se však do popředí zájmu dostává outsourcing služby, tzn. komplexní řešení pronájmu serveru včetně softwaru, administrace, zálohování, monitoringu a dalších doplňkových služeb.

## Jak se díváte na možnost zvládnutí přechodu na IPv6 a co jej nejvíce brzdí?

Přechod na IPv6 má své specifikum v tom, že k němu prostě musí dojít. Není tu jiná alternativa. Odhaduje se, že adresy IPv4 dojdou někdy koncem roku 2011. Proces přechodu už je delší dobu nastartovaný. Kde mohou nastat problémy, je například oblast ISP pro koncové uživatele, kde běžně používaná zařízení mívají stále firmware s podporou pouze pro IPv4. Co se týče naší sítě, přechod na IPv6 máme prakticky za sebou.

## Co jsou podle vás v dnešních datových centrech nejužší hrdla z hlediska jejich výkonu (efektivity)?

Jak již naznačuje často skloňovaná „zelená energie“, spotřeba elektrické energie je tím nejzákladnějším limitem. Lze sledovat, že prakticky všechna datová centra řeší především otázku dostatečného příkonu, od kterého se následně odvíjejí prostorové parametry a chladicí výkony datacenter. Dnes jsou již známé technologie pro chlazení vysokozátěžových racků a serverů, stejně tak umíme pracovat s minimem prostoru. Limitem však vždy zůstává elektrická energie, která tvoří významnou nákladovou položku jak provozně, tak investičně.

(mar) 10 0213



Nežádanější službou je housing vlastního hardwaru, do popředí se ale dostává i outsourcing služeb.

FILIP ŠPAČEK  
provozní ředitel,  
Master Internet