ROZHOVOR

Dostatečné zabezpečení IT infrastruktury je pro firmy stále problémem

MARTIN NOSKA

Nedílnou součástí IT infrastruktury větších firem a menších organizací pracujících s citlivými daty je systém logického i fyzického zabezpečení. O tématu a osobních postřezích jsme hovořili s Martinem Petrovkou, ředitelem společnosti Complete CZ.

O době škrtů se mluví též jako o příležitosti – opravdu nějakou vidíte?

Určitě ano. Myslím, že obecně mají větší šanci inovativní a skutečně efektivní řešení. Když je prostředků méně, více se řeší, za co je utratit. Když se podíváme do oblasti fyzického zabezpečení ICT, tak vidíme zájem o modulární řešení, která lze koupit v menší konfiguraci a postupně rozšiřovat – konkrétně o zabezpečené racky, které v určité situaci mohou dokonce nahradit celou serverovnu. Z hlediska procesů může být v rizikové době tlak na větší automatizaci procedur klasifikace a ochrany dat.

Čím je dnešní doba rizikovější než před dvěma lety?

Je jasné, že v situaci zvýšených tlaků a nejistoty zaměstnanci uvažují o možnostech obohacení či získání přízně konkurence na úkor stávajícího zaměstnavatele. Podle průzkumu Data Loss Barometer společnosti KPMG již v první polovině loňského roku rostl počet úniků dat způsobených zaměstnanci meziročně o více než 50%. To žel platí dvojnásob ve státní správě – zde je nárůst incidentů podle KPMG ještě vyšší. Nic na tom nezmění průzkumem zjištěný fakt, že se hlásí stále menší počet úniků dat – přes uvedený růst incidentů jejich medializace poklesla o 30%. Problémy je však lepší řešit preventivně než pak „tutlat".

Podobná data najdeme i ve studii European Identity and Access Management od KPMG a Everettu. Tři čtvrtiny firem si uvědomují, že by měly pozornost a investice v této oblasti spíše zvýšit, ovšem čtvrtina jich provedla v roce 2009 až padesátiprocentní škrty v rozpočtech, dalších 13% dokonce ještě více a celá polovina firem omezila jejich rozsah.

Je podle vás problémem nedostatečná diskuze o možnostech zabezpečení?

Hovoří se o tom stále. Rovněž je pravdou, že v této oblasti organizace různého druhu plošně šetří, a to často bez předchozí analýzy možných dopadů a nastavení úsporných, ale funkčních postupů. Jinde zase řeší pouze nebezpečí zvenku a zálohovaná data jsou uvnitř organizace dostupná řadě lidí. Tato oblast se dá přirovnat k boji s korupcí. Metody jsou známé, je jich celá řada, ale klíčové je některé z nich zavést takovým způsobem, aby je bylo možné prosadit a ohlídat.

> Zajištění bezpečnosti musí prosazovat vedení firem, neobejde se přitom bez spojenců vevnitř či vně organizace.
>
> **MARTIN PETROVKA**
> ředitel, Complete CZ

Jak si myslíte, že je možné tento stav řešit?

Důležité je, aby si bezpečnost ohlídalo přímo vedení firem. K tomu potřebuje spolehlivé spojence vevnitř či vně organizace. Vedle adekvátní personální a bezpečnostní politiky organizace, se jeví jako klíčové automatizované systémy prosazující potřebné procesy a případné restrikce a dále fyzické zabezpečení technologií, dat i jejich záloh, např. datovým sejfem či zabezpečeným rackem.

(maj) 10 0149