

Udržte svůj byznys

Je škoda přijít o rozjeté podnikání kvůli nějaké živelní katastrofě nebo krizové události způsobené lidskou činností. Jak se tomu dá zabránit?

VÁCLAV MOLÍK

Mluvíme-li o krizových plánech, kontinuitě provozu a obnově po havárii, každému se vybaví buď měsíce práce podle složitých metodik, například PAS 56, ISO/IEC 25999, nebo stohy papíru v trezoru, ve kterých se nevyzná. Proč se zabývat plány kontinuity podnikání, havarijními plány nebo plány obnovy? Vulkán v Čechách nemáme, pořádné zemětřesení tu nezažili ani prarodiče našich prarodičů, o blizardu s vichřicí jsme četli naposledy jako sedmnáctiletí v rodokapsu a pořádný meteorit spadl na Zemi před 65 miliony let...

Pouze malý zlomek populace ČR se setkal se živelní pohromou, která by vážně poškodila jím vlastněný majetek. I to je důvod, proč u vedení firem převládají názory: „Nemáme dost zdrojů (peníze, čas, lidi) na pře-

pravu nějakých alternativních plánů. Je malá pravděpodobnost, že se něco vážného přihodí, a když, pak budeme reagovat operativně podle situace.“

V některých odvětvích je zavedení krizových plánů vyžadováno ze zákona (energetika, teplárenství, nebezpečné látky, rozvody vody, energie, telekomunikace, zdravotnictví, požární ochrana atd.). Dává smysl zabývat se kontinuitou provozu i v běžné firmě, když do uvedených kategorií nespadá a zákon to u ní nevyžaduje?

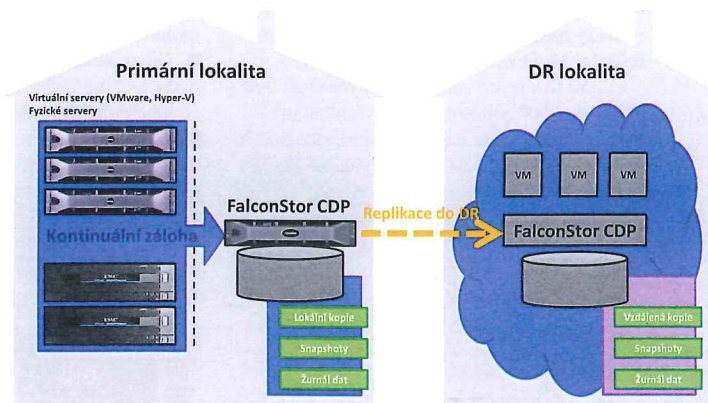
Je třeba si uvědomit, že mezi největší hrozby nepatří nutně živelní katastrofy nebo krizové události způsobené lidskou činností. I když jejich dopad může být velký, jsou málo pravděpodobné. Je to spíš množství menších problémů, jako jsou prodloužené výpadky elektřiny, výpadky počítačových sítí nebo ztráta klíčových zaměstnanců či kombinace všeho. Například respondenti EMC Corporation's 2011 European Disaster Recovery Survey uvádějí, že přerušeni provozu firmy jsou častěji spojena se selháním IT zařízení (61 %), selháním napájení (42 %) nebo ztrátou či znehodnocením dat (35 %).

Poznátky ze života

Uvedu dvě situace, se kterými jsem se osobně setkal.

Situace 1: Útok hackera do interní sítě zastavil provoz podniku a plná obnova kritických systémů trvala několik dnů.

Situace 2: Zdánilivě malá porucha v budově hrozí vyřadit celé datové centrum. Jde o springler, který nebylo možné odstranit ze serverovny kvůli požárním předpisům. Serverovna je totiž postavena z původní kanceláře a pro zhášení in-



Typová varianta: Primární lokalita (serverovna zákazníka), záložní/DR lokalita (GTS datacenterum)

terním plynem by bylo nutné vybudovat oddělenou požární sekci, a to je příliš drahé.

Poslední dobou se ve firmě GTS Czech setkáváme stále častěji se zástupci vedení firem, kteří si uvedená rizika uvědomují. Při snaze je řešit ale narážejí na složité metodiky, nedostatek kvalifikovaného personálu a vysoké náklady na implementaci. Proto jsme vytvořili pracovní skupinu složenou z odborníků společností GTS Czech, Logica a GAPP System a společně jsme připravili pracovní rámec nasazení BCM/DRP pro malé a střední podniky. Součástí rámce je jak metodika, tak technické řešení v oblasti IT a telekomunikací včetně následného provozu a péče o uvedenou oblast.

Zjednodušenou metodiku BCM pro SME je vám připravena představit Logica na workshopu, během kterého proskočí ve vašem podniku zaměstnanci v požadovaných rolích a zajistí jejich podporu při přípravě a nasazení kontinuity provozu ve firmě. Vaši pracovníci pod naším vedením se sami naučí řešit danou problematiku, a díky tomu nebudete závislí na dodavateli. Výsledkem práce vašich zaměstnanců pak budou dokumenty potřebné pro další krok.

Při návrhu cílového technického řešení vyjdeme z několika připravených typových variant.

Podstatou je správné zálohování kritických dat (kombinace CDP a časových snímků) do záložního datového centra a správný design datové sítě, který umožní efektivně překloupat provoz systémů ze serverů na primární lokalitě na servery v záložní lokalitě. Jedna z typových variant je na příložených schématech.

V záložním datacentru lze umístit jak vaše servery, tak pronajmout výpočetní výkon. Je možné použít jak vaše vlastní, tak i námi pronajaté dedikované servery. Jako výhodnější řešení lze využít pronájem virtuálních serverů, protože výhodné vlastnosti virtualizace umožní obsluhu záložních serverů zjednodušit a náklady na provoz i řešení havarijních situací podstatně snížit. V nekrizovém stavu běží typicky jen virtuální servery zajišťující replikaci dat, ostatní virtuální servery jsou hibernované. Vy platíte pouze za to, co skutečně používáte. Ani my, jako váš dodavatel, totiž nemusíme platit za elektrickou energii, licence, náklady na chlazení a další náklady za hibernované stroje.

Skutečně zálohujete?

Obligátní tvrzení, že zálohují všichni, ale obnoví pouze někteří, není vhodné brát na lehkou váhu. Pravidelné provádění testů, během kterých ověříme dostupnost kritických dat a plnou funkci systémů, je součástí naší služby pro vás, ovšem předpokládá také vaši spolupráci. Připravili jsme takové řešení, které umožní dělat testy bez vlivu na běžný provoz vaší firmy, tzn. paralelně s ostrými, běžícími systémy vašeho IT.

Funkční systém, sestavený z jednotlivých IT zařízení a telekomunikačních služeb, musí podporovat přechod do krizového režimu a zpět do běžného provozu, s minimálním vlivem na kritické procesy (například výroba, prodej, servis...), které jsou nutné pro zajištění základních funkcí podniku. Samozřejmě nesmí dojít ke ztrátě vašich kritických dat. Zeptejte se našich zákazníků, zda jsme schopni takové řešení navrhnout, realizovat a provozovat. Kontaktujte nás. Jsme schopni vám předběžně spočítat, zda se vám taková řešení vyplatí nebo ne. Podle toho se můžete sami rozhodnout, jestli je pro vás užitečné řešit tuto problematiku s námi či nikoliv.

Další informace naleznete na stránkách www.gts.cz/ict.



Autor ing. Václav Molík pracuje ve společnosti GTS Czech. Spoluautoři: Doc. RNDr. Milan Berka, CSc., Michal Trnka, M.A. (Logica Czech Republic), ing. Petr Dvořák (GAPP System).