Výpadek elektrického proudu může přijít draho

Virová napadení nejsou hlavní hrozbou podnikových počítačových sítí. Ačkoliv je zjevné, že jsou stále fenoménem dnešní doby, stojí nyní IT pracovníci před daleko závažnějším problémem.

Podle Průzkumu stavu informační bezpečnosti v ČR 2007, provedeném společností Ernst & Young od května do července loňského roku, jsou v ČR výpadky proudu druhým nejčastějším bezpečnostním incidentem po nevyžádané elektronické poště (SPAM). V České republice postihují 86% organizací.

Z publikovaného grafu bezpečnostních incidentů s nejzávažnějším dopadem – (k nimiž patří porucha hardware, chyba programového vybavení, nevyžádaná elektronická pošta, selhání sítí, chyba administrátora nebo obsluhy, počítačový virus, chyba uživatele, přírodní katastrofa, nepovolený přístup k datům, krádež zařízení a podobně) – vyplývá, že ze všech případů, které představovali incident s největší finanční škodou pro organizaci, šlo ve 35% o výpadek proudu (obr. 1).

Kolik to firmy stojí?

Pokud vznikla škoda, tak průměrný finanční dopad každého výpadku proudu vyčíslili organizace na 260 000 Kč. To v rozpočtu zejména menších organizací, institucí či podniků není zanedbatelný údaj. Ve statistických údajích předstihly tak krádeže zařízení (v průměru 225 000 Kč), poruchy hardware (200 000 Kč) a selhání sítí LAN (80 000 Kč).

Spam zůstává bezkonkurenčně nejčastěji se vyskytujícím bezpečnostním incidentem. Dokonce zaznamenal nárůst celých 5 procentních bodů oproti roku 2005, kdy byla tato kategorie v rámci citovaného průzkumu poprvé sledována. V posledních dvou letech se s ním u nás – opět podle citovaného průzkumu – setkalo 92% společností.

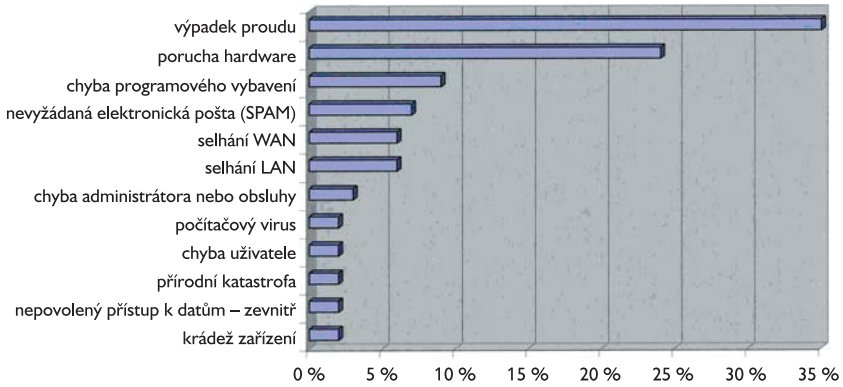
Je ale pozoruhodné, že výskyt počítačových virů se dostal na hranici 50% (pokles o 22 procentních bodů oproti roku 2005), kde byl naposledy v roce 1999. Lze jen spekulovat o „dospělosti", širokém nasazení antivirových technologií, standardizaci virových útoků a dalších faktorech, které tento dramatický pokles mohou, ale nemusí, mít na svědomí. Bude zajímavé sledovat, zda se tento trend za dva roky potvrdí.

Jak v této souvislosti konstatuje Country manager společnosti APC-MGE pro Českou republiku, Slovensko a Polsko, Ivan Hábovčík, *„ústup virů ze slávy je zřetelný. Viry se, obrazně řečeno, propadly z vedoucí skupinky pomyslného pelotonu. Naopak výpadek proudu a porucha hardware zůstávají stálicemi a jsou nyní na vrcholu bezpečnostních incidentů s nejzávažnějším dopadem"*.

Přesto, že se tato situace v České republice rok od roku zlepšuje – například organizací, které nikdy neprováděly analýzu rizik, s každým dalším ročníkem průzkumu ubývá – není toto zjištění nijak povzbudivé. Naprostá většina (80%) společností nemá na informační bezpečnost vyhrazen finanční rozpočet. Pětina společností nikdy neprovedla analýzu rizik informačních systémů, což je překvapující.

Přitom účinným zabezpečením klíčových datových center může být instalace energocentra, které v případě výpadku elektrického proudu bezprostředně zajistí náhradní dodávku elektřiny. Ideální je jeho naplánování už v projekční fázi výstavby nového sídla.

„Vhodné zálohování pomocí energocentra s UPS ve větších institucích dokáže zabránit až řádově miliónovým škodám," říká Ivan Habovčík. *„Ne náhodou se proto zajištění náhradní dodávky elektrické energie v případě jejího výpadku v datových centrech, který ještě poměrně nedávno nebyl zcela stěžejním, stává nyní ústředním motivem diskusí na mnoha odborných seminářích a konferencích. Od jeho úspěšného řešení - více, než si mnohdy myslíme – odvisí ekonomický úspěch nejednoho podniku"*.



Obr.1 Graf bezpečnostních incidentů s nejzávažnějším dopadem

Asi 80% případů přerušení dodávek proudu trvá od zlomku sekundy do 30 minut. Takovou dobu podpory jsou napájecí zdroje schopny zajistit bez potřeby instalace a spuštění dieselového agregátu vyrábějícího proud.

UPS lze dnes celosvětově najít jak v podnicích vyrábějících elektrotechnické výrobky nebo komponenty automobilů, tak v továrnách těžkého průmyslu, v chemickém, palivovém i stavebním oboru a také v hutích. Důležitou roli hrají samozřejmě rovněž v sektoru bankovnictví, financí a telekomunikací.

Manažeři jsou neustále pod tlakem, aby snižovali náklady. Krátkodobé úspory však často přinášejí vpravdě Pyrrhova vítězství. Ztráty v případech IT zařízení nebo třeba jen přechodné ztráty napájení se mohou ukázat jako zdrcující. V případě ztráty napájení může dojít nejen ke ztrátě dat, ale také k úplnému zastavení výrobního procesu. Zahraniční i naše zkušenosti prokázaly, že zastavení počítači řízené výrobní linky třeba jen na několik sekund může způsobit významný pokles parametrů celé série výrobků, které se vzhledem k nesplnění jakostních norem stanou neprodejnými.

V případě nejhoršího scénáře může výpadek či porucha počítačů dozorujících výrobu způsobit poškození strojů a dokonce – v důsledku ztráty jejich stability – vystavit pracovní personál nebezpečí. Například výpadek proudu v automobilovém průmyslu může způsobit vysoké škody u naprogramovaných svářecích či dalších robotů.

Nové technologie tedy umožňují účinnou ochranu a neustálý provoz počítačů – a v souvislosti s tím také výrobních linek, které jsou jimi řízeny. Klíčovým se zdá uvědomit si podnikatelské riziko, které nesou majitelé průmyslových podniků v souvislosti se zastavením výroby. Výdaje na systémy zabezpečení IT musí být dobře promyšlené, ale je to důležitá investice, která by se neměla odkládat.

Ing. Ivan Habovčík

Country Manager
Czech Republic, Poland, Slovakia
e-mail: Ivan.Habovcik@apcc.com