

Bezpečnosť IT en milieu non-IT

alias IT prostredie, prostredie pre IT a ochrana prostredia

Pozn.: (en milieu [án milijö], franc. = v prostredí)

Na úvod urobme analýzu názvu článku. Pojem prostredie je nám asi najbližší, začneme malú exkurziu rôznymi druhmi prostredia, o ktorých sa v súvislosti s výpočtovou technikou najčastejšie hovorí. A aby sme tieto rôzne prostredia správne chápali v kontexte informačných technológií, uvedieme, čo všetko tento pojem zahŕňa. Informačné technológie (IT) podľa definície americkej ITAA (Information Technology Association of America) sú „štúdiom, návrhom, vývojom, implementáciou, podporou alebo manažmentom počítačových informačných systémov, zvlášť softvérových aplikácií a technických prostriedkov počítačov (hardvéru)“. Z tejto širokej definície vyplýva, že programátori a špecialisti IT oddelení budú ako prostredie často označovať platformu, ktorá sa viaže k vývoju a prevádzke ich softvérovej aplikácie. Hovorí o unixovom prostredí, prostredí Windows, grafickom prostredí, vývojom prostredí a pod.

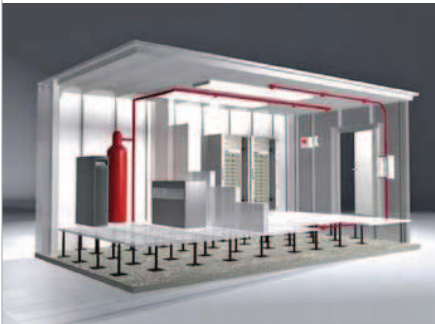
Druhú skupinu budú tvoriť ľudia, ktorí sa starajú o kvalitu prostredia, v ktorom sa IT zariadenia nachádzajú. V oblasti dátových centier to sú pracovníci technologického facility managementu, ktorí sa starajú o chod a údržbu kritickej podpornej infraštruktúry (non-IT), bez ktorej by sa IT zariadenia v dátových sálach a serverovniach prehriala a v tom lepšom prípade by riadnym spôsobom automaticky ukončili svoju činnosť. Prostredie, tak ako ho chápe kritickej facility management (Critical facility management, CFM), znamená zabezpečenie priestoru, v ktorom sú IT zariadenia umiestnené. Dokonca i pojem aplikácie má pre CFM celkom iný význam: aplikáciou rozumieme použitie vzduchotechnických filtrov na zaistenie bezprašnosti prostredia, klimatizačné a chladiace jednotky na zaistenie optimálnej teploty a vlhkosti chladiaceho vzduchu v mieste jeho nasávania IT zariadeniami, antistatické povrchy, odtienenie rušivých elektromagnetických javov, energeticky zabezpečený systém neprerušiteľného napájania pre kritickú záťaž, distribučné systémy na rozvod elektrickej energie a chladiacich médií, systémy na fyzické zabezpečenie majetku a kontrolu vstupu osôb a ďalšie systémy umiestnené v kritickej priestore i mimo neho (palivové hospodárstvo, motorgenerátory, vonkajšie chladiace jednotky).

V súvislosti s manažmentom dátových centier, ktorý okrem výkonu služieb CFM zahŕňa ešte riadenie ekonomických aspektov prevádzky, riadenie vykonávania zmien, vedenie dokumentácie skutočného stavu, vykonávanie prevádzkových auditov a ďalšie činnosti, sa objavuje ďalší rozmer pojmu prostredie, ktorý sa týka nielen jeho prevádzkovateľa, ale aj výrobcov IT, systémových integrátorov a najširšej verejnosti. Je ním vplyv IT zariadení na životné prostredie. Počnúc výrobou počítačov a počítačových komponentov cez optimalizáciu využitia výpočtového výkonu softvérovými aplikáciami, keď sa niektoré vý-

počtové operácie presúvajú do nočných hodín, keď je cena energie nižšia a systémy sú menej využité, až po virtualizáciu serverov a konsolidáciu podnikovej infraštruktúry, sú uplatňované opatrenia, ktoré majú jediný cieľ – znížiť prevádzkové náklady súvisiace s nákupom elektrickej energie a znížiť nepriame korporátne emisie CO₂. Veľkosť tzv. uhlíkovej stopy (carbon footprint) sa stáva parametrom, ktorého vývoj spoločnosti pozorne sledujú, pretože jeho znižovanie vedie jednak k ekonomickým úsporám, jednak k vyššej prestíži týchto spoločností, ak sú dosiahnuté úspechy správne komunikované verejnosti, napríklad v rámci výročných správ.

Bezpečnostné hrozby a ich členenie

Po nevyhnutnom objasnení pojmov IT, non-IT a CFM sa teraz podrobnejšie pozrieme na zaistenie fyzickej bezpečnosti dátového centra z pohľadu jeho každodennej prevádzky. Aby zvolené riešenie obstálo v dlhšom časovom horizonte, musíme vidieť bezpečnosť z vyššej perspektívy. Ak hovoríme v súvislosti s non-IT infraštruktúrou dátového centra o bezpečnosti, máme na mysli najmä jej existujúce či pripravované limity, spôsob riešenia kritickej stavov a udalostí a takisto fyzické zabezpečenie prístupu do jednotlivých technologických miestností a k technológiám umiestneným vo vonkajšom prostredí,



pripadne i registráciu fyzického prístupu k IT a non-IT zariadeniam tak vnútri, ako i mimo budovy, dátového centra. Ako súčasť bezpečnostných opatrení ďalej zaisťujeme pravidelné školenia a certifikáciu personálu, splnenie požiadaviek daných poistnými zmluvami atď. Na bezpečnosť prevádzky dátového centra sa môžeme pozeráť ako na mieru neohrozenosti chodu (funkcie) IT zariadení umiestnených v ňom, pričom chodom rozumieme dostupnosť IT aplikácií a dát. Bezpečné prostredie pre IT (služby a zariadenia) preto tvoria:

1. Technológie zaisťujúce chod IT zariadení – systém napájania, systém klimatizácie a chladienia, elektromagnetického odtienenia. Ich architektúra a topológia majú mimoriadne veľký význam.
2. Technológie, ktoré síce nezaisťujú chod IT zariadení, ale sú natoľko dôležité, že ich zlyhanie má fatálne dôsledky. Patrí sem napríklad

fyzická infraštruktúra a systémy protipožiarnej ochrany. Príkladom bezpečnostného incidentu môže byť zrútenie podlahy z dôvodu nedostatočnej nosnosti alebo bezdôvodné spustenie stabilného hasiaceho zariadenia (SHZ), pričom z bezpečnostných dôvodov príde k odpojeniu všetkých systémov od prívodu elektrickej energie, pretože ochrana života a zdravia osôb má vyššiu prioritu než ochrana životného prostredia a majetku. Vhodný návrh týchto ďalších kritickej systémov preto vzniká v kontexte s prevádzkovými a bezpečnostnými opatreniami a v úzkej nadväznosti na analýzu rizík v danej lokalite, buďto alebo časti objektu, kde je dátové centrum prevádzkované. Sledujeme mechanickú pevnosť konštrukcií, tesnosť a požiaru odolnosť, kapacitu trás pre silovú kabeláž, potrebné systémy, vzduchotechnické potreby a čistotu prostredia (prašnosť, elektromagnetické javy).

3. Technológie zabezpečujúce fyzickú bezpečnosť prevádzky. Fyzickému zabezpečeniu IT sa často prisudzuje menší význam, než by zodpovedal vysokému podielu bezpečnostných incidentov pri jeho podcenení. Do tejto kategórie incidentov patria poruchy hardvéru, chyba obsluhy, krádež dátových nosičov, nepovolený fyzický prístup, zneužitie zariadení, prírodná katastrofa, požiar a iné incidenty, ktoré znamenajú narušenie integrity IT zariadení v mieste inštalácie.
4. Dátová a softvérová bezpečnosť, ktorá súvisí s poskytovaním IT služieb. Bezpečnostným rizikom rozumieme fenomény ako spam, phishing, počítačové vírusy, softvérové chyby, chyby sieťových prvkov, vonkajší nepovolený prístup (po sieti) a zneužitie dát. Túto oblasť riešia softvéroví špecialisti, no len za predpokladu, že IT zariadenie pracuje v predpokladanom mieste (nie je od cudzené), vo vhodných prevádzkových podmienkach (monitorujeme kvalitu napájania a parametre prostredia).

Napriek všetkému, čo sme už uviedli, miera požiadaviek a prijateľných kompromisov bude mať len dve roviny: oficiálnu, ktorá sa viaže na splnenie príslušných noriem, nariadení a predpisov, a tú vašu, ktorú si stanovíte podľa svojich potrieb. Ako oblasť kritickej fyzickej infraštruktúry (Network Critical Physical Infrastructure, NCPI) uvedieme aspoň časť relevantnej predpisovej základne a najčastejšie bezpečnostné hrozby, ktoré sme schopní v súvislosti s návrhom NCPI dátových centier riešiť.

Predpisová základňa pre oblasť non-IT infraštruktúry dátových centier (celosvetovo):

- TIA/EIA 942 Telekomunikačná infraštruktúra a štandard pre dátové centrá (profesijný štandard)
- TUI DCIS Klasifikácia infraštruktúry dátových centier, Tier I až IV – Uptime Institute

Predpisová základňa pre oblasť fyzickej bezpečnosti (Európa):

- EN 54-1 Elektrická požiarová signalizácia
- EN 50131 Poplachové systémy EZS (elektronické zabezpečovacie systémy)

- **EN 50132/133** Poplachové systémy CCTV (uzatvorený televízny okruh)
- **EN 1143-1** Bezpečnostné úschovné objekty – fyzická odolnosť
- **EN 1047** Bezpečnostné úschovné objekty – požiarová odolnosť
- **ISO 14520** Plynové hasiace systémy

Potenciálne riziká pre prevádzku dátových centier

Výpadok napájania, výpadok klimatizácie, nedostatkové chladenie, prehriatie, oheň, voda použitá ako hasivo, korozívne plyny, vandalizmus, výbuchy/terorizmus, únava materiálu (zlom), prach, elektromagnetické rušenie, neoprávnený prístup (fyzický a pre dátové siete), krádež/vlamanie, záplava/povodeň

Systém monitoringu NCPI a kritický facility management

V neposlednom rade NCPI zahŕňa systémy mo-

onitoringu (technologický dohľad) uvedených non-IT technológií. Monitorujeme stavy, sledujeme trendy, predchádzame bezpečnostným incidentom. Ďalej sledujeme prostredie a procesy. Musíme si uvedomiť, že len dokonalá súhra monitoringu a prevádzkovo-organizačných opatrení umožňuje minimalizovať počet bezpečnostných incidentov.

Záver

Vzhládom na čoraz väčšiu koncentráciu výkonných IT zariadení v dátových centrách treba dokonale zvládnuť návrh a optimalizáciu NCPI, pretože len správny návrh topológie a správne dimenzovanie podpornej technologickej infraštruktúry môže zaistiť dlhodobu udržateľnú bezpečnosť IT systémov. Za pomoci monitorovacích systémov a vhodne nastavených eskalačných procesov sa dá eliminovať výskyt väčšiny bezpečnostných incidentov. Pri dodržaní vhodne zostavenej predpisovej základne sa neplánovane nestane, že by rozvádzače s tlačidlami STOP boli

umiestnené v bežne prístupnej chodbe, že dátová sála nie je vybavená bezpečnostnými dverami, že dátové centrum má nedostatočne citlivé detektory dymu alebo poddimenzovaný systém na hasenie požiaru. V prípade, že si riešenia non-IT časti necháte radšej vypracovať na objednávku, neváhajte s oslovením špecializovanej spoločnosti, ktorá sa výstavbou dátových centier sústavne zaoberá. Dokonca aj vtedy, keď ide len o rozširovanie alebo prestavbu existujúcej technologickej non-IT infraštruktúry, sa vyplatí prizvať si špecialistu, ktorý pozná rôzne varianty riešenia a aktuálne trendy.



■ TOMÁŠ KROUPA,
konzultant ALTRON, a. s.

PREHLAD DODÁVATEĽOV: BEZPEČNOSŤ IT

Názov spoločnosti	Dodávateľ:		Poskytované:		Referencie v SR
	Výrobca	Poskytovateľ	Služby	Produkty	
3Com	Áno	Nie	Áno	Áno	Slovenský rozhlas
Accenture	Nie	Áno	Áno	Nie	Identity & Access Management projekt pre poprednú slovenskú banku
AEC, spol. s r. o.	Áno	Áno	Áno	Áno	OTP Banka Slovensko, Československá obchodná banka, SLOVNAFT, Poštová banka
AKCENT NOVA, s. r. o.	Áno	Áno	Áno	Áno	ALEX, Aplica group, COOP Jednota, Daňové riaditeľstvo, DREVOS, Grand Power, KOHAFLEX, Profitactic, SOAS, STAVIVA-Garaj
Alef Nula, s. r. o.	Nie	Áno	Áno	Áno	Neuvádzajú
ALTRON SK	Nie	Áno	Áno	Áno	Referencie poskytujú na vyžiadanie
ANASOFT	Nie	Áno	Áno	Áno	Slovak Telecom, SPP, SR, Poštová banka, UPC Broadband Slovakia, Poistovňa HDI - Gerling Slovensko
APC by Schneider Electric	Áno	Áno	Áno	Áno	SWAN, LightStorm Communications
AutoCont SK, a. s.	Nie	Áno	Áno	Áno	DEXIA banka Slovensko, KOOPERATIVA poisťovňa, AMSLICO AIG Life poisťovňa, BIBUS SK, ThyssenKrupp Ferostav, NUSCH, Plastika Nitra, Thermal park Bešeňová
CÍGLER SOFTWARE, a. s.	Nie	Áno	Áno	Áno	25 000 inštalácií v domácnostiach, malých a stredných firmách, veľkých spoločnostiach a inštitúciách verejnej správy
Cleverlance Slovakia, s. r. o.	Nie	Áno	Áno	Áno	Všeobecná úverová banka, VÚB Leasing, Tatra banka, S IT Solutions SK, T-Mobile Slovensko, Telefónica O2 Slovakia
CORINEX GROUP, a. s.	Nie	Áno	Áno	Áno	Riešenia v utilitych spoločnostiach, obrannom priemysle, finančných inštitúciách, verejnom sektore
DATALAN, a. s.	Nie	Áno	Áno	Áno	Zákazníci zo segmentov financie, telco, priemysel, verejná správa
Deloitte Advisory, s. r. o.	Nie	Áno	Áno	Nie	Deloitte poskytuje svoje služby zákazníkom v sektore bankovníctva, finančných služieb, telekomunikácií, energetiky, stavebníctva, priemyslu a verejného sektora
Disig, a. s.	Áno	Áno	Áno	Áno	Generali Slovensko poisťovňa, Kancelária Národnej rady SR, Prvá stavebná sporiteľňa, Spoločná zdravotná poisťovňa, TPA Horwath, Univerzita P.J. Safárika v Košiciach, Všeobecná zdravotná poisťovňa
ELTON, družstvo	Áno	Áno	Áno	Áno	Ministerstvo práce sociálnych vecí a rodiny, Bytové družstvo Petržalka, Bytový podnik Bratislava - Petržalka, PROGRES, Správcovská a realitná a iné
EMEL BRATISLAVA, s. r. o.	Nie	Áno	Nie	Áno	HORNEX, SLOVINTEGRA, PROF CREDIT Slovakia, Štátne lesy TANAPu, PPA CONTROLL, SLOVANET, ŠKODA AUTO Slovensko, ISTROBANKA, Privatbanka, Železnice Slovenskej republiky
ESET, spol. s r. o.	Áno	Áno	Nie	Áno	Slovenská sporiteľňa, T-Mobile, T-Com, Samsung Slovensko, Úrad vlády SR, Ministerstvo vnútra, Univerzita Komenského v Bratislave
IBM Slovensko, spol. s r. o.	Áno	Áno	Áno	Áno	Neuvádzajú
Info consult, s. r. o.	Nie	Áno	Áno	Áno	VSE IT Košice, MÚ Žiar nad Hronom, MÚ Prešov, MÚ Lučenec, NsP Vranov nad Topľou, OÚ sv. Alžbety Bratislava, NsP Bojnice, SE Bornezde Slovakia, ThyssenKrupp Ferostav
Kerio Technologies, s. r. o.	Áno	Nie	Nie	Áno	SkyEurope Airlines, Sodexho, Mestský úrad v Trenčíne, Železiarne Podbrezová, Konica Minolta Slovakia, Tmavský samosprávny kraj, Slovenský pozemkový fond, Štátny ústav pre kontrolu liečiv, COOP Jednota Nitra, Dóvera zdravotná poisťovňa
Microsoft Slovakia, s. r. o.	Áno	Áno	Áno	Áno	Lesy SR (partner: Softip), Slovenský vodohospodársky podnik (partner: Softip), Daňové riaditeľstvo SR
NESS Slovensko, a. s.	Nie	Áno	Áno	Áno	Tepláreň Košice, Slovenská elektrizačná a prenosová sústava, Jadrová a vyradovacia spoločnosť, Stredoslovenská energetika, Slovenské elektrárne, Poštová banka, First Data Slovakia, Paroplynový cyklus, Leasing SLSP, Česká sporiteľňa
Siemens, s. r. o., Siemens IT Solutions and Services	Nie	Áno	Áno	Áno	Slovenský plynárenský priemysel, Slovenské elektrárne, Ministerstvo obrany, Sociálna poisťovňa, Západoslovenská energetika, T-Com, PricewaterhouseCoopers Slovensko
S&T Varias, s. r. o.	Nie	Áno	Áno	Áno	Neuvádzajú
SOFT-TRONIK SK, s. r. o.	Nie	Áno	Áno	Áno	Neuvádzajú
SOITRON, a. s.	Nie	Áno	Áno	Áno	Agentúra pre riadenie dlhu a likvidity, CSOB Leasing, MV SR, MS SR, Úrad vlády Slovenskej republiky, Národný ústav srdcových a cievnych chorôb
Symantec GmbH (ČR & SR)	Áno	Áno	Áno	Áno	Neuvádzajú
TEMPEST, a. s.	Nie	Áno	Áno	Áno	UNIPHARMA Prievidza, Slovenský plynárenský priemysel, SLOVNAFT, Slovenská národná knižnica, Jurki - Hayton, Tatra banka, Volkswagen Finančné služby Slovensko, T-Mobile Slovensko, Národná diaľničná spoločnosť, Dexia banka, CETELEM Slovensko, Letové prevádzkové služby SR
TrustPort, a. s.	Áno	Nie	Pripravuje sa	Áno	Britrade Slovakia, IBEAM, Profibed Slovakia, Základná škola J. Hollého, Topoľčany, Základná škola Kainičiakov, Bratislava
X-NET, spol. s r. o.	Nie	Áno	Áno	Áno	Neuvádzajú