

# Ty nejlepší historicky z IT



Redakce BusinessIT a partneři



# Ty nejlepší historky z IT

**BusinessIT.cz**

---

Edice: BusinessIT ebooks

Autoři: Redakce BusinessIT.cz a partneři

Copyright © Bispiral, s.r.o., 2012

Titulní foto © OpenImageBank.com

Vydáno v roce 2012 v Bispiral, s.r.o.

Názvy použité v této knize mohou být ochrannými  
známkami příslušných vlastníků.

web: [www.BusinessIT.cz](http://www.BusinessIT.cz)

---

Možná je to laciné, možná podbízivé, možná až nevkusné, ale nemohli jsme odolat: Některé příběhy lidí z IT, které jsme slyšeli, nám přišly tak zajímavé (a, přiznáváme se, pobavily nás), že jsme se rozhodli jim věnovat samostatnou e-knihu. A pokud je snad nechcete číst prostě jen pro zábavu, nepochybně se v nich skrývá i nějaké to poučení.

Všechny příběhy, které zde zveřejňujeme, pocházejí od skutečných lidí, z masa a kostí, jak se říká, kteří se pohybují ve světě IT. Jakkoli jsou jejich příběhy pravdivé, některé detaily musely být pozměněny – a při čtení pochopíte, proč. Naším cílem není způsobit komukoli potíže – a nejméně ze všeho našim autorům nebo jejich zaměstnavatelům. Pokud máte vlastní zajímavé zážitky, o které jste ochotni se s námi a s našimi čtenáři podělit, těšíme se na ně. A pokud se vám nechce je pilovat do stylisticky dokonalé podoby, nevadí – po dohodě s vámi je rádi připravíme k vydání.

Redakce BusinessIT.cz

---

## **Průšvih za 34 milionů dolarů**

Naši společnost si firemní zákazníci často zvou, když u nich dojde k nějakému průšvihu spojenému s krádeží nebo s únikem dat; případ, o kterém tady bude řeč, je ale opravdu unikátní. Tentokrát jde totiž o průšvih d'ábelských rozměrů - o krádež finančních dat obsahujících mimo jiné informace o pěti tisících

velmi bohatých klientech; a škoda, která byla způsobena, dosáhla 34 milionů dolarů.

Ale nechci začínat od prostředka, a proto se teď raději vrátím k okamžiku, kdy se celý problém zrodil. A kdy ještě nikdo neměl tušení, jak velký vlastně bude. Ani jeho pachatel, ani další zaměstnanci firmy, jíž se dotkl. Mimochodem - dotčena byla společnost, která je opravdu velkým poskytovatelem finančních služeb. Působí po celém světě, zaměstnává více než 30 tisíc lidí a dále popisované trable se odehrály v její divizi zaměřené na správu investic.

## **Máte vyhazov**

Celý příběh začal v okamžiku, kdy se jeden manažer z oddělení privátního bankovníctví dozvěděl, že se jeho oddělení zavírá - a že všechny investiční operace budou zajišťovány z jiné země formou outsourcingu. Muž se rozhodl, že to nenechá jen tak - a o několik dní později si zkopíroval jména, kontaktní údaje a další data nejbohatších klientů společnosti na svůj USB disk. Mimochodem - tento seznam obsahoval záznamy řady skutečně důležitých lidí,

politiky počínaje a nejrůznějšími celebritami - včetně známých sportovců - zdaleka nekonče.

Zaměstnanec, který se rozhodl ukrást data své firmy, měl za sebou více než 15 let práce v oboru a více než 5 let působil na své současné pozici. Vždy odváděl velmi dobrou práci a svými nadřízenými byl kladně hodnocen. Neexistoval ani malý náznak, že by mohl spáchat krádež tohoto druhu. I proto měl zřejmě velmi široká práva přístupu do některých kritických informačních systémů.

## **Klienti si stěžují a začíná vyšetřování**

Krádež dat byla objevena asi 3 měsíce poté, co se odehrála. Jak se to stalo? Několik z oněch velmi bohatých zákazníků si stěžovalo, že je oslovila konkurenční firma. A ne ledajak: Vše podle nich nasvědčovalo tomu, že její makléři mají k dispozici důvěrné informace o jejich účtech, o posledních obchodech i o preferencích, které nikdo neměl znát. Tedy - nikdo kromě nich a firmy, která byla okradena o data.

Firemní oddělení IT bezpečnosti zahájilo ve

spolupráci s externími auditory pečlivé vyšetřování, při němž byl zjištěn download dat ze systémů. Ukázalo se rovněž, že jej provedl bývalý zaměstnanec, který nyní pracuje u té konkurenční firmy.

Škoda, kterou způsobil, zahrnovala poškození dobrého jména firmy, náklady na obhájce, náklady na konzultace a také ztráty způsobené odchodem klientů. Nebylo jich málo: Mimo jiné odešlo přibližně osm procent velmi významných firemních zákazníků. Celková škoda tak byla odhadnuta na 34 milionů amerických dolarů.

## **Je třeba přijmout opatření**

A právě v době, kdy se problém provalil a firma začala zvažovat, jak napříště podobným událostem zabránit, jsme vstoupili na scénu my. Prostudovali jsme všechny dostupné informace ohledně práce firmy s daty i o celém incidentu. Podle našeho názoru mu bylo možné zabránit a v tomto smyslu jsme informovali i klienta.

V důsledku celé události pak byla přijata řada

zásadních opatření. Ředitel firmy ve spolupráci s jejím představenstvem iniciovali vznik nových pravidel ochrany dat a vytvoření oddělení zodpovědného za jejich ochranu. Vznikla pozice šéfa ochrany dat na mezinárodní úrovni. Firma nyní provádí intenzivní audity monitoringu a shody s pravidly. Byly rovněž nasazeny systémy SIEM (Security Intelligence systems), které pomáhají v reálném čase identifikovat podezřelé transakce, a to především u privilegovaných uživatelů.

Jakkoli jsem v úvodu zmínil, že šlo o unikátní případ, nelze tvrdit, že se podobné problémy vyskytují zřídka. I když v nich ale třeba nejde o tak bohaté klienty a celebrity, případně škoda nedosahuje takových rozměrů, pro firmy jsou vážné. Smutné je, že bezpečnostní opatření jsou mnohdy zaváděna nikoli preventivně, ale až dodatečně.

*(Autorem této kapitoly je Dr. Larry Ponemon, který se specializuje na problematiku ochrany dat a informační etiku. V roce 2002 založil Ponemon Institute, výzkumné centrum zaměřené na pokročilé metody ochrany dat a soukromí. Mezi jeho další aktivity patřila nebo patří spolupráce s významnými soukromými i veřejnými*



*organizacemi na projektech spojených s hodnocením rizik a s ochranou dat. V listopadu 2011 zpracoval Dr. Larry Ponemon pro společnost Kingston Technology nezávislou studii „Stav bezpečnosti USB v Evropě“, která zkoumala úroveň USB bezpečnosti v deseti evropských státech. Tuto studii máme nyní k dispozici a to nejzajímavější z ní pro vás připravujeme.)*

## **Skutečný příběh: Vzal jsem servery a utíkal před povodní**

Nikdy bych si nemyslel, že budu psát tyto řádky – ale poté, co jsem nedávno na vlastní kůži zažil sílu matky přírody, dospěl jsem k závěru, že tohle stojí za zveřejnění. Než se dostanu k věci, musím na rovinu říci, že jsem právě zažil stresující, vyčerpávající a neuvěřitelně dlouhé čtyři dny. Většina firem v této době už má nějaké plány pro zotavení po katastrofě, ale dokud tu katastrofu opravdu nezažijete, nikdy nebudete vědět, jak to proběhne ve skutečnosti. Já už to vím.

## Extrémní počasí, verze 2011

Nejprve bych tu pro nezasvěcené rád krátce shrnul extrémní počasí, které nás na severovýchodě USA nedávno potkaly. Zažili jsme nejvlhčí léto, jaké tu kdo pamatuje. Nevyhnuly se nám ani extrémní deště, ani hurikány, ani tropické bouře, ani přivalové deště, které zemi zahltily i deseticentimetrovým sloupcem vody během dvaceti minut. Nedávno jsme tu dokonce měli i slabé zemětřesení. Takové podmínky v naší oblasti rozhodně nejsou běžné. Každá firma, ať už se nachází kdekoli, je vystavena určitému riziku. Můžete mít datové centrum v nejlepší možné lokalitě, ale stejně se nevyhnete všem hrozbám. Stačí třeba nehoda cisterny s benzínem nebo převrácený nákladník s chlorem poblíž vašeho areálu... Všichni také považujeme za jistou existenci elektrické sítě nebo vysokorychlostního připojení k internetu – páteřních sítí, které dosud nezažily velký výpadek – ale jak vám řekne nejeden síťový specialista, jednou k tomu velkému výpadku jistě dojde.

V neděli 27. srpna jsme s mou ženou seděli na

mezinárodním letišti Newark a čekali na let do Las Vegas, kde za pár dní začínala konference VMworld 2011. V posledních dnech se všude mluvilo jen o hurikánu Irena – a my jsme měli letět posledním spojem na západ před tím, než bude letiště kvůli počasí uzavřeno.

## **Hrozí nám něco?**

Osobně vždy sleduji počasí na východním pobřeží USA velmi pozorně. Jednak mě baví sledovat radarové snímky a počítačem generované grafy vývoje, jednak potřebuji vědět, co se děje v místech, kde máme pobočky. Je jich celkem 6 a ve většině z nich nemáme příliš serverů – je tam především síťová infrastruktura, která požadavky uživatelů směřuje do centrály. Tentokrát jsou na trase hurikánu – jednoho z nejsilnějších, který v posledních letech v této oblasti udeřil – čtyři ze šesti poboček – New York City, Virginia, New Jersey a New Hampshire. Když jsem přiletěl do Las Vegas, měl jsem sevřený žaludek a celý víkend jsem nebyl schopen myslet na nic jiného, než na silný vítr a déšť, kterým jsou naše

pobočky vystaveny. Do neděle večer naše centrála ve Scrantonu (Pensylvánie) schytala devět centimetrů vody a stále lilo – a mělo pršet až do pondělního rána. Takový déšť by nevadil, pokud by neexistovalo cosi, co se jmenuje Susquehanna - řeka, před kterou nás má chránit 12metrová hráz, která se nachází jen nějakých 30 metrů od naší centrály s hlavním datovým centrem. Tato zábrana byla vybudována armádou USA jako reakce na záplavy z roku 1972 způsobené hurikánem Agnes; tehdy šlo o nejhorší přírodní katastrofu v historii Pensylvánie.

V minulosti hráz vydržela už leccjakou zkoušku... A ani tentokrát nás nic zlého nepotkalo. Alespoň po dobu, kdy jsem byl v Las Vegas.

## **Katastrofa se blíží**

V týdnu, kdy jsem se vrátil z VMworldu, jsem byl unavený, ale chtěl jsem otestovat ESXi 5 a připravit nějaké plány na třetí čtvrtletí. Netušil jsem, že právě toto bude nejdrsnější týden mého života – i kariéry. Až do středy 7. září, to tak vlastně ani nevypadalo.

Předpověď počasí se opět zhoršovala s každým novým snímkem z radaru. Blížilo se k nám několik bouří, z nichž některé byly poměrně silné. Dalo se čekat, že na severu Pensylvánie i státu New York spadne velké množství srážek – přes 20 centimetrů, což může znamenat problém. V této oblasti je řada přehrad, říčních systémů, protipovodňových ventilů a další infrastruktury, bez níž by každé město od Syrakus po Filadelfii čekaly povodně. Část z těchto systémů ústí do řeky Susquehanna, jejíž hladinu zvedly už předchozí deště.

V naší organizaci máme definovány tři úrovně katastrofy:

Stupeň 1: Evakuace oblasti v okolí datového centra a dalších budov (při stoupající řece, chemickém zamoření apod.). Šance? 8 z 10. Toto je naše "typická katastrofa". Práce pokračují v náhradní lokalitě (disaster recovery site), provoz je směřován přes VPN a 100MB linku do centrály.

Stupeň 2: Dočasné přerušení spojení s centrálou (výpadek napájení, stoupající řeka, která si vynutí odpojení, nebezpečné chemikálie apod.). Šance? 3 z 10.

Stupeň 3: Kompletní ztráta konektivity do centrály,

kompletní ztráta systémů na neurčitou dobu (katastrofa v regionu nebo v celém státě, katastrofická ztráta budovy). Šance? 1 z 10. Tentokrát jsem se dostal do stupně 2,5. Nutno dodat, že naši náhradní lokalitu jsem navrhl a zařídil tak, abychom byli schopni řešit stupně 1 a 2. Proč ne 3? Prostě kvůli nedostatku času. Zajistil jsem konektivitu, což samo o sobě trvalo déle, než jsem čekal, navrhl záložní řešení pro virtuální stroje a přitom řešil upgrade i v našem hlavním datovém centru. To, že jsme byli schopni zvládnout i stupeň 2,5, považuji za slušný úspěch – obzvlášť když ještě před devíti měsíci žádný disaster recovery plán neexistoval.

## **Ujíždíme katastrofě**

Byl čtvrtek 8. září, 8:30 ráno. Toto datum si budu pamatovat navždy. Sledoval jsem počasí a vše nasvědčovalo tomu, že už tak vysoká hladina řeky bude i nadále stoupat. Vzhledem k její výšce jsem dospěl k závěru, že je na čase začít se připravovat na katastrofu – a řešit disaster recovery. Tušil jsem,

že odteď se nejméně 48 hodin nevyspím – a nebyl jsem daleko od pravdy.

Sáhnul jsem po našem plánu pro zotavení po katastrofě. Byl jsem si jistý, že bude fungovat pro stupně jedna a dva. Dojde-li k nejhoršímu, budu to muset nějak vyřešit.

Nejprve jsem naložil několik nejdůležitějších serverů do svého Jeepu. Byly to ty, které jsem neměl v záložní lokalitě – potřeboval jsem některé záložní obrazy systémů, záložní hardware a pár páskových jednotek. To, že jsem si tento hardware vzal s sebou, jsem později vyhodnotil jako jeden z nejšťastnějších kroků, které jsem učinil. Kluci, kteří mají na starosti desktopové počítače, naložili do dodávky pracovní stanice a připravili se na přejezd do záložní lokality, která je naštěstí jen 25 minut jízdy odsud – na kopci. Jakmile jsme tam přijeli, nastal čas řídit se pokyny plánu pro stupeň jedna, což bylo jednoduché. Nebudu vás nudit detaily – v záložní lokalitě je připravena síť, kterou stačí připojit k lince do hlavního datového centra. Pak tu může pracovat nějakých 30 až 40 lidí na běžném hardwaru a softwaru. A tak to také fungovalo až do páté odpoledne, kdy jsme se dozvěděli, že řeka kulminuje na 12 metrech a

energetická společnost vypne dodávku elektřiny v okolí řeky. Nastává řízená panika – a my přecházíme na stupeň dva.

Byl jsem na takovou možnost připraven, ale rozhodně jsem neměl touhu své plány realizovat v praxi. Stupeň dva znamená ztrátu konektivity do centrály, což je velmi blízko nejhoršímu scénáři. Plánoval jsem to, testoval jsem to, ale když se to skutečně stalo, bylo to něco úplně jiného.

Pro ochranu virtuálních strojů a virtuální infrastruktury používám Veeam Backup and Replication 5.0. V záložní lokalitě jsme měli tři servery Dell R710 s 48 GB RAM připojené ke třem úložným zařízením s 5 TB prostoru (založeným na open source Openfiler 2.99). A měli jsme 15 replikovaných virtuálních strojů připravených pro okamžité spuštění – včetně domain controllerů, některých serverů pro sdílení souborů, serverů Exchange, SQL a dalších. Slabým článkem byl chybějící systém pro replikaci od EqualLogic, kterému do implementace scházelo už jen několik měsíců, když jsem přišel o potřebné finance. Bez jeho nasazení bylo naše řešení nekompletní a provizorní. Nicméně i náš stávající systém byl schopen zajistit běh základních služeb.



## Největší slabina

Velmi brzy jsem zjistil, že hlavní slabinou našeho plánu pro zotavení po katastrofě je jeho často přehlížená složka – totiž komunikace. Nemám na mysli e-mail, SMS nebo telefony, ale komunikaci mezi státními i lokálními úřady a vedením firem v dotčených oblastech. Skutečnost, že ve skutečnosti nikdy nedošlo k přerušení dodávek elektřiny v naší centrále, nebo že jsme se nikdy spolehlivě nedozvěděli, jaká je aktuální výška řeky, nás vedla ke špatným rozhodnutím.

Ve čtvrtek v noci jsem s pomocí Veeam Replication v kombinaci s VMware Migrations kompletně převedl aktivity datového centra na záložní servery. K tomu zřejmě vůbec nemuselo dojít. Tehdy jsem to ale samozřejmě nevěděl. Naše e-maily, webové aplikace, IIS, intranet a aplikace pro core business (ty, které dosud nejsou v cloudu) normálně běžely v záložní lokalitě. Což považuji docela za úspěch, vzhledem k tomu, že nám spánkový deficit situaci rozhodně neusnadňoval.

## Dobré zprávy a pár doporučení

Dobrou zprávou je, že nebyla ztracena jediná transakce a firma normálně fungovala. To dokazuje, že disaster recovery byla úspěšná. V sobotu dopoledne jsem se pak dozvěděl, že voda v řece kulminovala na třinácti metrech, takže snad jen zázrak zachránil město před nejhorší záplavou v historii severovýchodní Pensylvánie.

Na závěr bych tu měl několik doporučení pro IT oddělení i pro všechny, kdo jsou zodpovědní za plány pro disaster recovery:

- Každá firma, velká nebo malá, pochopitelně potřebuje plán pro disaster recovery.
- Rozhodněte se, jaké jsou vaše obchodní cíle (priority) pro tento plán a – to je důležité – napište si je. V obtížné situaci se cíle bez pečlivého plánování mění.
- Plánujte vždy tu nejhorší možnost. Mějte definovány různé stupně, ale plánujte pro ten nejhorší.
- Ujistěte se, že máte víc než jednoho nebo dva

lidi, kteří mohou spravovat a nasazovat hardware nebo software. One-man show při katastrofě nefunguje.

- Využívejte cloud. Začněte zkoumat možnosti využití cloudu, obzvláště pokud se nacházíte v oblastech s vysokým rizikem katastrofy.
- Ověřte své zálohy, a co je nejdůležitější, kompletně otestujte svůj plán pro zotavení z katastrofy. Pokud něco nefunguje, opravte to ihned. Nečekejte s tím až na katastrofu.

*Autorem této kapitoly je Jonathan Franconi, odborník na virtualizaci a správce sítě jedné firmy v severovýchodní Pensylvánii (USA). Ve svém volném čase poskytuje konzultace ohledně virtualizace i dalším společnostem. Franconi publikuje na svém blogu VirtualizationImpact. Původní text byl pro publikování na BusinessIT.cz a v této knize se souhlasem autora přeložen, redakčně upraven a zkrácen.*

**Jak jsem chytil hackera – IT manažera**

Před nedávnem jsem byl jednou velkou finanční institucí požádán, abych v ní v souladu s požadavky regulátora provedl rutinní bezpečnostní audit IT. Tato organizace je povinna provádět vyhodnocení pravděpodobnosti zpronevěry vždy po několika letech. Většina prováděných transakcí se zde pohybuje v řádu mnoha milionů dolarů.

Šéf auditu IT (chraňme z právního hlediska nevinného a nazývejme ho panem X) projevoval starost především o oblast elektronických vkladů a převodů. Zprvu jsem předpokládal, že se obává, jaké slabiny bych mohl najít, protože to byl právě on, kdo nesl zodpovědnost za příslušný systém. A také to byl on, kdo zprovozoval všechna bezpečnostní opatření na jeho ochranu.

Pan X mi sdělil, že četl zprávy, podle nichž právě finanční transfery jsou často cílem hackerů. Svěřil se mi, že je až paranoidní při ochraně vlastnictví svého zaměstnavatele a že bere otázky informační bezpečnosti velmi vážně.

Když jsem vyjádřil přesvědčení, že některé části jeho síťové infrastruktury jsou neefektivní, nebo naopak přehnaně chráněné, zdálo se, že je na mě našťvaný. Potom se ale jeho emoce změnily v hrdost, že

vybudoval tak komplexní systém. Přitom stále opakoval, že pod jeho dohledem nedošlo v tomto oddělení nikdy k žádnému kriminálnímu činu.

## **Jak byly převody peněz zajištěny**

Manažeři zodpovědní za finanční převody dostávali denně nový autorizační kód, který jim umožňoval práci s elektronickými vklady a výběry. Denní obměna byla prováděna z bezpečnostních důvodů. Manažeři se přihlásili do svých aplikací, zahájili proces elektronického vkladu nebo výběru (obvykle ve formě převodu z účtu na účet) a při dokončení převodu získali autorizaci. Celý uvedený postup je první chybou systému: Finanční instituce by měla mít speciální náhodně generovaný kód pro každého manažera zvlášť, navíc měněný alespoň dvakrát za den.

Pan X, který byl zodpovědný za bezpečnost IT systémů, nainstaloval pro ochranu IT infrastruktury různé technologie – například pasti (honeypots), zařízení pro prevenci ztráty dat i forenzní zařízení (host based forensics devices). Objevila se ale

nečekaná slabina: Pan X byl schopen celkem snadno získat denní autorizační kód. Většinou to ani nevyžadovalo žádné technické znalosti. Stačilo jen pobýt s finančními manažery a nenápadně jim nahlédnout přes rameno. A když to nešlo takto, prostě mohl nahlédnout do logovacích souborů svých bezpečnostních nástrojů a heslo zjistit odtud. Je ironií, že tyto nástroje byly nainstalovány, aby právě proti tomuto druhu podvodů chránily.

## **Manažer hackerem**

Protože měl pan X přístup k systémům pro převod peněz, zřídil si zde uživatelské ID. Nikdo mu nijak neomezoval přístup, protože k jeho práci patřilo testovat software, takže potřeboval platné přihlašovací jméno. A protože měl autorizační kódy pro vklady a výběry, běžně zadával příkazy k převodům peněz na několik soukromých účtů po celém světě.

Pan X měl to pochybné štěstí, že najal právě mě, aby bylo učiněno zadost pravidlu vyžadujícímu audit systému. A byla to souhra okolností, že mě jeho

přístup přiměl zaměřit se na uvedené operace. Mohl bych tu kázat o potřebě nezávislého auditu, o nutnosti rozdělení kompetencí, o nezbytnosti přístupu založeného na rolích, nicméně základní pravdou je, že absolutní moc korumpuje. Zbytek tohoto příběhu si už dokážete představit...

*Autorem této kapitoly je Aamir Lakhani, konzultant, který se specializuje na pokročilou moderní kryptografii. Amir je poradcem v oblasti kybernetické bezpečnosti v řadě společností z Fortune 500 a také vládních organizací USA. Aamirovy názory jsou často zveřejňovány v různých publikacích a je obecně považován za jednoho z předních expertů na Cloud Computing, virtualizaci, next-generation networking, datová centra a technologie kybernetické bezpečnosti. Aamir Lakhani publikuje své texty také na blogu CloudCentrics.com. Tento text je publikován ve spolupráci s autorem. Mezititulky byly doplněny redakcí BusinessIT.cz.*

**Jak nainstalovat z Česka přes Indii server**

## ve Francii

Jestli si nejste zcela jisti, nakolik pro vás může být následující návod důležitý, pak vezte jedno:

Pracujete-li v nadnárodní korporaci, pak se to, co se stalo mně, může stát i vám. A asi z toho, stejně jako já, nebudete mít moc radost. I když se tu tedy nedozvíte nějaká ultravelká moudra, aspoň zjistíte, že v tom nejste sami.

### Začíná to objednávkou

Všechno začalo úplně nevinně. Nejmenovaný francouzský výrobce automobilů si u nás objednal komplexní řešení (protože komplexní řešení, to je to, na co jsme specialisté) zahrnující mimo jiné nový server s Windows. Měl bych dodat, že šlo o opravdu velký server od opravdu velkého světového výrobce serverů a že měl být podle smlouvy ke klientovi dodán v polovině února.

Má role je prostá: Jako vedoucí projektu sleduji plnění jednotlivých kroků a prostřednictvím našich outsourcingových partnerů zajišťuji, aby náš klient



dostal nikoli nějaké jednotlivé produkty, ale opravdu to, o čem už byla řeč, tedy komplexní řešení. Tolik teorie. V praxi ale server v polovině února naším partnerem dodán nebyl.

Zpoždění dodávky samozřejmě není nijak výjimečná situace a nikoho to nijak zvlášť nezervózní. I já mám pochopitelně časovou rezervu, a tak jen ve svém systému pro project management přetáhnu vybrané úkoly do nových termínů. V tomto případě na polovinu března.

## **Server je na místě**

A opravdu, 18. března stojí server na svém místě. O tři dny později ho francouzský kolega rozbalí, zapojí a... A zjistí, že chybí dvě karty s rozhraním fibre channel. Což je trochu problém, protože dokud není dodávka kompletní, nelze na serveru začít dál pracovat.

Spojím se s prodejcem výrobce, který tvrdí, že karty rozhodně byly součástí dodávky a je třeba je jen zasunout do slotů. Nová kontrola na místě ukazuje, že karty rozhodně součástí dodávky nebyly.

Spojím se s prodejcem výrobce, který připouští, že karty součástí dodávky být nemusely.

Prodejce se spojí se mnou a informuje mě, že karty součástí dodávky být ani neměly. Poměrně dlouze o tom vzrušeně diskutujeme a po zaslání několika e-mailů s již dříve předanými dokumenty dochází ke shodě. Karty součástí dodávky být měly.

V polovině dubna je problém vyřešen. Zdá se. Kontrolou na místě je však zjištěno, že se výrobce sice pochlapil, ale zaslal jen první z karet.

Spojím se s prodejcem výrobce. Opět poměrně dlouze diskutujeme, vzrušeněji než naposledy.

V polovině května je problém skutečně vyřešen. Obě karty jsou na místě, lze je zasunout do slotů a server konečně zapojit. Z mé části úkolu už zbývá jen drobnost – instalace operačního systému.

## **Instalujeme operační systém**

Můj čas je drahý. Jsem koneckonců vedoucím projektu. A tak instalaci operačního systému deleguji na někoho, jehož čas je levnější, totiž na kolegu v Indii. Teď už budu jen čekat, kdy mi oznámí

dokončení instalace a pak do svého systému pro project management zanesu informaci o dokončení projektu.

O dva dny později mi volá kolega z Indie. V šest hodin ráno. Časový posun si ve velké korporaci vybírá svou daň. Bohužel na mně. A proč kolega, jehož čas je levnější než můj, volá? Server mu nejde nainstalovat, protože A) má strašně pomalé připojení a nedaří se mu vzdáleně nabootovat ze vzdáleného instalačního média a B) když se mu to po několika hodinách podaří, nevidí disky - díky tomu, že ve standardní instalaci není ovladač k internímu RAID poli a on to neumí vyřešit. No, nevím kdo to vymyslel dělat podporu z Indie a „nenatáhnout“ dostatečně „silné“ dráty. Že by to bylo proto, že ta podpora v Indii klidně může strávit s instalací dny místo hodin?

Bohužel super procesy v nadnárodních společnostech jsou připraveny úplně na všechno, ale samozřejmě na takovou prkotinu ne (a hlavně ne v reálném čase). A tak se na procesy musím... .. je obejít. Zadáám do Google ta správná klíčová slova a během několika minut mám řešení. Připravím upravené instalační médium a vzdáleně připojím – díky heslům, která jsem se jakoby omylem dověděl (jako project

manager je přesně přeposílám mezi jednotlivými pracovníky a stejně jsou většinou defaultní :-)). Když je nainstalováno, předám k doděláním indickému kolegovi a začínám přemýšlet, jak ve svém projektovém plánu zamaskovat několik dnů strávených instalací Windows. Těch pár indických dní se ztratí, ale co ty moje „drahé“ hodiny?!

Voilà!

*(Toto je skutečný příběh skutečného projektového manažera skutečné nadnárodní korporace. Několik drobných detailů příběhu bylo mírně pozměněno, protože nadnárodní korporace nemají rády, když se vynášejí do světa jejich know-how.)*

## **Antispam, největší nepřítel internetu**

Právě jsem nastoupil do nového zaměstnání a jednou z povinností, které jaksi spadají do popisu mé pracovní náplně, je správa e-mailového serveru. Což, po pravdě (jak všichni víme), není až taková zátěž, pokud všechno šlape, jak má, a nemusíte denně řešit desítky nově přichozích a odcházejících zaměstnanců (anebo na to máte chytré scripty, které

se samy spouštějí odněkud z HR). Ale pochopitelně, kdyby všechno šlapalo tak, jak má, tak bych sem nepsal tenhle text.

Firma, ve které jsem se ocitl, je malá. Nějakých padesát zaměstnanců, plus mínus. Během pár hodin jsem pochopil, že na nějaké velké oficiální hierarchie se tu nehraje, stejně jako se tu moc nehraje na nějaké papírování. Tedy alespoň ne na to, které je zbytné (rozumějte: za které nehrozí šikana ze strany úřadů). A zbytná je zjevně i dokumentace zdejších IT systémů (mohu-li to tak vzletně nazvat), což je obzvláště prima, neb se svým předchůdcem jsem se nikdy nesetkal. A jak jsem pochopil z různých narážek, mělo to zřejmě své důvody. Konkrétně zřejmě panovala obava, abych se nenakazil jeho „móresy“. Ať už si pod tím představíte cokoli.

## **Konec světa**

Třetí den ve firmě se zbořil svět. Přestal fungovat e-mail. Ne, že by přestal fungovat úplně, ale přestaly chodit některé důležité e-maily. Což jsem se dozvěděl tak, že mi zavolal můj nejvyšší šéf a

ustaraným hlasem mi sdělil, že mu nechodí maily. Načež připustil, že jen některé z nich. Jak se ukázalo, nepřišly mu jen dva. Vyrozuměl jsem, že šlo o nějaké zásadní rodinné záležitosti. To mě trochu uklidnilo, neb zjevně nešlo o ztráty na zisku v milionech dolarů, nicméně přece jen jde o nového šéfa, takže zase rozhodně nejde o incident na levelu Zero.

Nastal tedy čas se blíže seznámit s naším e-mailovým serverem. Přiznávám, že s Qmailem na Linuxu jsem do téhle chvíle neměl tu čest, ale trocha brouzdání po internetu mi přinesla rychlé osvětlení. A trocha zkoumání nastavení pak i zjištění příčiny problému: Mailový server řeší (samozřejmě) i otázku ochrany proti spamu, v našem případě mimo jiné i pomocí databáze Sorbs.net. A zjištěný spam si odkládá stranou (ne, naštěstí nemaže), takže se k němu adresát nedostane. Ne, neptejte se mě proč. Prostě když padne rozhodnutí, že zasilka je spam, tak ji buď čekáte – a požádáte administrátora (tedy mě), nebo o ní nevíte – což je nepochybně ta častější varianta – a pak máte smůlu.

**Někdo se zbláznil**

Vrcholem průšvihů je pak to, že Sorbs.net zjevně mydlí do své databáze IP adresy hlava nehlava, takže v našem konkrétním případě nepřišel e-mail z Gmailu, konkrétně od šéfovy manželky z firmy, kde používají Google Apps (na vlastní doméně). Vážně to někdo myslí vážně s antispamem, který bez skrupulí odstřihne odesílatele Gmailu? Krátkodobé řešení je rychlé: Ztracený mail předávám šéfovi a se Sorbs.net končím. Možná do budoucna budeme tuto nebo jinou databázi k filtrování spamu používat, ale rozhodně bude mít jen poradní hlas. Pokud totiž zařadí mezi problémové adresy servery Gmailu, tak se v době cloudových firemních mailů není o čem bavit, to je prostě fail jako hrom. A zaměstnanci samozřejmě musejí napříště dostávat své spamy do spamové schránky. Protože jinak jsou na tom hůře než uživatelé freemailů.

**Utekli jsme od Linuxu k Windows a ke cloudu**

Nechci se vyjadřovat ke sporům mezi stoupenci Linuxu a Microsoftu. Mohu ale popsat, jaké rozhodnutí jsme udělali a proč jsme ho udělali. Podstatné přitom pro nás bylo jen to, abychom se mohli věnovat pacientům a nemuseli ztrácet příliš času tím, že bychom se starali o technologie. A jak jsme si poradili tam, kde potřebujeme vytvářet věci přesně na míru, protože naše podnikání je hodně specifické, a zároveň nechceme být závislí na žádném „IT kreativci“.

Naše společnost Sanatorium TOPAS provozuje nestátní zdravotnická gerontopsychiatrická zařízení zaměřená zejména na pacienty, kteří trpí Alzheimerovou chorobou a dalšími typy demencí i různými fyzickými postiženími, a to včetně onkologických onemocnění. Naše zařízení ve Škvorci, Ostředku a u Sečské přehrady mají celkem více než 400 lůžek a jsou jedinečná tím, že se dokáží postarat o lidi, kteří trpí fyzickou nemocí a zároveň s takovými změnami v mozku, které jsou důsledkem stárnutí a omezují kognitivní funkce (někdy to bývá označováno jako stařecká demence).

Naše druhá společnost, Almed Servis, provozuje přípravnu jídla. Dodává chlazená jídla do domů s



pečovatelskou službou, základních škol, mateřských škol a podniků. Vznikla vlastně jako vedlejší produkt našich zdravotnických aktivit. Nejdřív sloužila jen pro potřeby sanatoria ve Škvorci, ale když se postupně objevovali další zájemci o dodávky jídel, vyrostla z ní samostatná firma. Obě firmy mají společné IT a využívají i podporu dalších centrálních útvarů, například účtárny.

## **I my musíme IT trochu rozumět**

Když hovoříme o IT, měl bych ještě dodat, že i když počítače nejsou můj obor, určitou orientaci přece jen mám. Sleduji základní trendy v oboru a občas se podívám do odborných časopisů. Máme tedy poměrně jasnou představu, jak by nám mohly informační systémy pomoci a dokážeme dát IT expertům zadání.

Také bych měl dodat, že naše IT je relativně složité. Potřebujeme pokrýt běžné podnikové činnosti, jako jsou účetnictví, personalistika a podobně. Vedle nich potřebujeme speciální zdravotnické agendy: karty pacientů, žádanky, výsledky vyšetření a podobně.

Pak tu jsou systémy pro řízení provozu jídelny: objednávky jídel, plánování, nákup potravin a podobně. Náročnost se zvyšovala se zakládáním dalších poboček. Dnes potřebujeme, aby se stejnými systémy mohli pracovat uživatelé ve třech různých lokalitách.

## **IT pomalu rostlo a komplikovalo se**

IT rostlo spolu s firmou bez nějakého speciálního plánování rozvoje. Na začátku jsme měli pár počítačů, potom přišel čas pořídit první server... postupně tak vznikla kompletní infrastruktura: serverovna, sítě, informační systémy, uživatelské počítače, tiskárny a všechno ostatní, co potřebuje zdravotnické zařízení, které pečuje o řádově 400 pacientů. Nikdy jsme neměli žádného svého IT zaměstnance, vše jsme řešili smlouvou o podpoře s menší místní firmou.

Rozvoj vypadal obvykle tak, že jsme zjistili, že potřebuje další IT funkci, oslovili jsme zmíněnou firmu a ta zjistila, že v rámci stávajícího uspořádání není možné požadovanou funkci zajistit. Po složitých

debatách se podařilo naši potřebu naplnit, ovšem za cenu toho, že výsledné uspořádání bylo ještě složitější než dosud, takže příště vše bylo ještě komplikovanější.

Náš dodavatel navíc preferoval Linux a byl toho názoru, že na každý specifický problém má být specifické řešení. Vytvořil tedy v rámci našeho IT řadu nasazení a nastavené, která nejspíš byla velmi zajímavá z technologického hlediska, ale pro nás znamenala především nepřehlednost. Navíc se stávalo, že se i na straně dodavatele měnili lidé a dokumentace se nevytvářela. O to komplikovanější pak byla každá další změna.

Problémy se tak postupně kupily. Naše trpělivost skončila ve chvíli, kdy jsme potřebovali vyvinout vlastní aplikaci pro objednávání jídel a zjistili, že není možné ji zasadit do stávající infrastruktury. Musela by fungovat zvlášť, na jiném serveru a dodatečně bychom pak museli řešit všechny záležitosti integrace.

**Nacházíme nové řešení**

O problému jsem se bavil i se svým známým Petrem Pilinem, majitelem iPodniku. A po jedné takové diskusi Petr přinesl něco, co jsme už dávno potřebovali. Jednoduchý přehledný papír, kde byly uvedeny různé varianty dalšího rozvoje IT. Co by která varianta znamenala z hlediska nákladů, co by znamenala z hlediska podpory uživatelů, jaké by byly další výhody a nevýhody. To byl přesně ten přístup, který nám scházel. Od té chvíle jsme byli schopni i jako netechnici řídit rozvoj vlastního IT!

První velké rozhodnutí, které jsme takto udělali, bylo směrem ke standardním produktům Microsoftu a ke cloudu. Ne proto, že je to módní, ale že jsme v rozvaze viděli, že je to praktické.

Nový dodavatel přebral naši stávající serverovnu a začal postupně migrovat jeden systém za druhým. Tak, aby si toho uživatelé pokud možno nevšimli. Proběhlo to naprosto hladce. Uživatelé se jen začali jinak logovat. iPodnik zařídil i migraci dat do nového účetního systému (v cloudu běží Pohoda). Naštěstí pomohli i lidé našeho dosavadního dodavatele, oné linuxové firmy, co vše řešila předtím. Navzdory našemu odchodu byli osobně hodně vstřícní a v rámci svých možností udělali, co bylo v jejich silách.

Konečně začaly fungovat všechny ty obyčejné věci, které člověk od dnešního IT očekává. Třeba možnost připojit se do systému přes internet. Zlepšila se také podpora. Dřív, když něco nefungovalo, znamenalo to, že expert musel přijet k nám do serverovny.

Samozřejmě to nějakou dobu trvalo. Občas se na místě ukázalo, že potřebuje dalšího experta, takže jsme museli čekat další dlouhé hodiny. V cloudu je to přece jen snadnější. A rozinka na závěr. Zatímco dříve jsme museli všem zaměstnancům kupovat Microsoft Office, dnes pracujeme s openoffice.org a jenom když někdo potřebuje na pár hodin plné funkce Excelu nebo PowerPointu, využije Microsoft Office z cloudu. Víte, kolik peněz nám jen tato samotná změna ušetřila při stovce zaměstnanců?  
*(MUDr. Alexander Kučera)*

## **Jak jsme k nám hledali nové ajťáky**

Tuhle otázku si čas od času nepochybně pokládá každý zaměstnavatel: „Jak najít a přilákat ty správné zaměstnance?“ Tím myslím ty, kteří něco umí, jsou ochotní něco dělat (pro firmu, samozřejmě) a navíc

jsou zrovna volní, nebo ochotní udělat změnu. My jsme letos hledali nové zaměstnance pro naše IT centrum v Brně a rozhodli jsme se to pojmout hodně netradičně.

Najali jsme týmy hostesek, vyškolili je a nasadili do předem určených míst, kde jsme předpokládali vysokou koncentraci IT odborníků. (Víc o volbě lokalit říkat nebudu, je to naše cenné know-how :).) A hostesky oslovovaly předpokládané IT odborníky: „Jste student oboru IT?“ „Jste zaměstnanec pracující v IT segmentu?“ „Mohu vám položit jednu otázku z oboru?“ Pokud byla odpověď na odbornou testovací IT otázku správná, uchazeč obdržel hlavolam. Pokládání otázek z IT se osvědčilo, protože hlavolamy jsme chtěli rozdat pouze ajťákům, ne náhodným kolemjdoucím. Mnoho lidí řeklo, že tomu rozumí, ale jejich odpovědi nasvědčovaly opaku. Docela nás pobavil chlapík, prý z oboru, který na otázku, co je to router, odpověděl, že asi nějaký dravej pták.

**Zájemci chodili i sami**

Hostesky vyvolaly mezi ajťáky velký zájem. Inu – přehnaně mužský obor :). Možná ale, že lákaly i ony hlavolamy. Zpráva o tom, že je rozdáváme, se roznesla rychlostí blesku. Zájemci (o hostesky nebo o hlavolamy) chodili často sami – s otázkou „Copak to tady máte?“

Nakonec naše vyškolené týmy oslovily celkem tisícovku potenciálních uchazečů o práci v IT centru. Jejich reakce na hlavolam byly veskrze pozitivní. „Aňáký bonbony by k tomu nebyly?“ odrovnal nás jeden dotaz. Pokud jde o úspěšnost skládání, byla značně různá. Někdo po hodině přišel zpět a hlásil, že to bylo moc lehké, že má hlavolam již rozluštěný, jiný se po hodině vrátil naopak s komentářem, že je to moc těžké.

Když se uchazeči podařilo hlavolam rozluštit, našel uvnitř adresu internetové stránky a vstupní heslo. Teprve tam se dozvěděl název naší společnosti, naši nabídku i požadavky.

## **Podařilo se**

Vím, že většina příběhů, které na BusinessIT

vycházejí, má příchut' nějaké kalamity, ale já, omlouvám se, žádnou nenabídnu. První fáze naší kampaně se podařila, zaznamenali jsme velké množství návštěvníků webové adresy, která byla uvedena v hlavolamu, a dostali spoustu profesních životopisů. V tomto okamžiku ještě nevíme, zda z nich vybereme vhodné zaměstnance na všech 40 pozic v IT centru, ale já osobně věřím, že ti, které takto vybereme, na svoje první pracovní setkání s naší firmou nikdy nezapomenou.

*Autor kapitoly pracuje pro IT centrum skupiny Home Credit, která toto neobvyklé oslovení nových IT zaměstnanců realizovala.*

## **Ženy v IT: Výzvy i pozitivní diskriminace**

Za mezinárodní den žen v IT by se dala s trochou nadsázky označit jedna z akcí, které se letos na jaře konaly v Praze. Girls in ICT Day si kladl za cíl ukázat dívkám, že i ony mohou v IT uspět. A jak jinak to ukázat lépe, než na konkrétních případech. Dva takové vám v rámci našeho speciálu příběhů z IT nabízíme i my.



Podle posledních údajů Českého statistického úřadu tvořily v roce 2010 ženy jen 12,6 % všech studentů vysokých škol v oboru informatika. V praxi je pak jejich podíl ještě nižší: Mezi IT odborníky je proti 89 % mužů jen 11 % žen.

Organizátoři celosvětové akce Girls in ICT Day upozorňují, že mezi studentkami, jejich rodiči i učiteli panuje nedostatek povědomí o tom, co může kariéra v IT nabídnout. A tak chtějí dát dívkám možnost vyzkoušet různé technologie a osobně se setkat s ženami, které v oboru něčeho dosáhly.

## **Místo hudby si vybrala počítačové sítě**

Černou ovčí rodiny se prý v jistém slova smyslu stala Veronika Štorková, nyní systémová inženýrka ve společnosti Cisco Systems, když se na rozdíl od zbytku rodiny rozhodla, že se profesionálně bude věnovat nikoli umění, ale informačním technologiím. Po gymnáziu tak místo na maminkou vysněnou konzervatoř nastoupila na pražskou Vyšší odbornou školu informačních služeb. Později se přihlásila na Vysokou školu

ekonomickou, kde se v 5. ročníku zapojila do Cisco Networking Academy. Po zdárném ukončení studia úspěšně absolvovala telefonní interview a hodnocení v assessment centru, a tím se jí otevřela cesta do ročního kariérního programu Cisco Sales Associate Program v Nizozemí. Po tomto pobytu pak byl už jen malý krok k tomu, aby začala v roce 2007 pracovat pro pražskou pobočku Cisco jako systémová inženýrka.

V roce 2009 pak v Bruselu po několikaměsíční intenzivní přípravě získala technickou certifikaci Cisco Certified Internetwork Expert (CCIE) a stala se tak vůbec první Češkou v historii, která tento titul obdržela. Před ní se to podařilo 69 českým mužům. Jednu z velkých výzev pro ni rovněž znamenala příležitost ucházet se o pozici ve společnosti Cisco ve Velké Británii. Žít v zahraničí byl Veroničin velký sen, a ten se jí tímto splnil. Dodejme, že mezi její hlavní zákazníky nyní patří rozhlasová a televizní společnost BBC.

**Žena mezi muži**

Jaké výhody jsou podle Veroniky spojeny s prací v oboru, kde převládají muži? Protože je žen v IT stále poměrně málo, je prý možné dobře vyniknout. A ženská přítomnost podle ní mírně odlehčuje velkou soutěživost mezi muži, zmírňuje napětí a zároveň otevírá cestu k většímu dialogu.

Práce mezi většinou mužů má ale i své nevýhody. Žena podle ní musí mnohem tvrději pracovat a neustále dokazovat, že je stejně dobrá, jako její mužští kolegové. „Další nevýhoda je, že ne všichni muži se chovají korektně a slušně a nezohledňují přítomnost ženy na pracovišti. Často jsem v české kanceláři „rostla“ z různých vulgárních vtipů některých kolegů. V Anglii si na tohle dávají mnohem větší pozor a dosud jsem se s tím nesešla,“ popisuje odlišnost českého a anglického prostředí.

## **IT v roli dobrého sluhy**

Martina Lovčiková, obchodní ředitelka CCS Česká společnost pro platební karty, se v oblasti ICT podle vlastních slov cítí být spíše pokročilým uživatelem, případně zadavatelem s velkou představitostí, než

vlastním hybatelem IT zázraků.

„IT pro mne proto vždy bylo klíčovým partnerem pro systémy řízení obchodu, marketingu, produktového vývoje i péče o klienty. Měla jsem možnost spolupracovat na řadě velmi zajímavých projektů, mimo jiné na náročnou integraci Eurotelu a Českého Telecomu nebo spuštění prvního firemního internetového bankovníctví, na kterém jsme spolupracovali s vývojovými týmy v různých časových pásmech od Indie po Los Angeles,“ vypočítává Martina Lovčíková a dodává: „Ve všech firmách, kde jsem pracovala, jsme také zaváděli nebo vylepšovali databázové systémy řízení vztahů s klienty (CRM), vybavovali technologiemi a procesy prodejní a servisní call centra, řešili on-line prodejní kanály, firemní weby a podobně.“

Vzápětí upozorňuje, že ICT může – ale nemusí – zjednodušit komunikaci a řízení obchodu a marketingu, ale jen když IT funguje v rámci dobrého firemního týmu. Komunikace s lidmi, ochota a schopnost se dohodnout, naslouchat potřebám klientů a následně jim umět vytvořit a dodat užitečná řešení, to je podle ní práce pro lidi, ne pro hardware nebo software. „V tomto ohledu jsme jako ženy od

přírody údajně lépe vybaveny než muži. Dobrá zpráva pro dívky je, že v typicky mužských oborech a týmech, se díky tomuto přesvědčení mohou připravit občas i na určitou pozitivní diskriminaci, což znamená, že za předpokladu stejně znalostně a zkušenostně vybavených kandidátů velké firmy často preferují ženy s cílem vytvořit vyvážené a dobře fungující týmy,“ říká Martina Lovčíková.

Martina Lovčíková upozorňuje ještě na jednu výhodu IT, kterou (nejen) ženy ocení – ICT řešení totiž umožňují větší volnost, pokud jde o práci z domova, či z dalších míst. Pro ženy je tak jednodušší skloubení rodiny a kariéry.

## **Nová pracovní místa v IT**

Podle Výzkumného ústavu práce a sociálních věcí v Česku do roku 2015 přibude v IT sektoru 22 688 nových pracovních míst. A potenciál získání dobrého zaměstnání nabídne IT i mimo ČR. IDC tvrdí, že v roce 2015 bude 90 % pracovních pozic vyžadovat alespoň základní IT dovednosti. Odborná příprava takového množství lidí vzdělaných v informačních

technologiích je nepochybně pro české školství velkou výzvou. Vzhledem k nedostatku absolventů IT oborů, kteří by poptávku zaměstnavatelů uspokojili, je podle organizátorů akce Girls in ICT Day jednou z možností také motivace většího počtu žen, aby se v tomto odvětví realizovaly. Dodejme, že v Česku letos tato akce proběhla na půdě společnosti Cisco Systems.

## **Logistiku bez IT si už dnes nedokážeme představit**

Podstatou podnikání logistických firem je dostat zboží z bodu A do bodu B. Pro jeho rychlé dodání a povědomí o aktuálním stavu všech zakázek je v dnešní době potřeba komplexní informační systém založený na integraci mnoha aplikací. Pochopitelně tomu ale tak nebylo vždy.

Není to tak dávno, co jsme stav zásilek zadávali do systémů ručně. Omyly a problémy s tím spojené si asi dokážete představit. Naštěstí v uplynulé dekádě prošly dramatickým vývojem systémy Track&Trace, takže dnes jsou uvedené činnosti již plně

automatizovány. Asi nejdůležitější částí procesu Track&Trace je zaznamenání doručení zboží do místa určení (IOD – Information on Delivery) a potvrzení o dodání zboží (POD – Proof of Delivery). Před implementací digitálních per bylo nutno po stvrzení příjemcem konkrétní originál dodacího listu fyzicky doručit do naší pobočky v České republice. Pokud se tedy dopravce nevracel po vyložení zpět do naší společnosti ten samý den, získali jsme tento dokument i s několikadenním zpožděním.

## **Můj milý zákazníku**

Možná vás překvapí, že i v dnešní době existují zákazníci, kteří preferují objednávání přepravy zasláním faxu. Samozřejmě se snažíme, aby docházelo v co nejvyšší míře k objednávání a potvrzování prostřednictvím elektronické výměny dat (EDI), nebo alespoň o využití objednávacího nástroje DSV E-services – a aby bylo, navzdory občasnému odporu legislativy, zajištěno elektronicky nejen objednávání, ale také akceptace a fakturování přeprav.

Díky IT ovšem nedochází jen ke zvyšování produktivity práce, ale i k přibližování se k formám dokonalé konkurence. Zatímco ještě před deseti lety byla většina přepravních služeb nasmlouvána a objednána vždy v rámci omezeného okruhu poptávajících a nabízejících, elektronická tržiště odbourala kapacitní omezení poptávajících. Nyní může i o drobnou zásilku soutěžit velký okruh nabízejících. Souvisejícím aspektem je i úprava nabídkových cen, která musí být stejně pružná jako trh přepravních služeb.

V lidském rozměru docházelo v logistice bez IT i ke komickým situacím, kdy se obchodní zástupce hned nedokázal rozpomenout, že s konkrétním člověkem již před nedávnem jednal, nebo nabízel znovu nechtěné produkty, což naší společnosti pochopitelně příliš neprospívalo. Přesto, že se tato pochybení stávala zřídka, implementace pokročilého CRM systému je vymýtila úplně.

## **Co používáme dnes**

Naše společnost dnes v rámci svého procesního



řízení využívá několika desítek informačních systémů a technologií. Některé jsou externí, tj. ty, které nejsou spravovány naší společností a k nimž pouze přistupujeme, další pak interní – mateřské, jež jsou spravovány naší mateřskou společností v Dánsku, a proprietární, jež jsou vyvíjeny a udržovány naším IT oddělením nebo externími dodavateli služeb.

Mezi externí informační systémy řadíme především zákaznické databáze (Albertina) a elektronická tržiště přepravních služeb – RaalTrans a Timocom Truck&Cargo. Na těchto tržištích se setkávají nabízející a poptávající. Dochází zde k uzavírání obchodních vztahů především v rámci tzv. vytěžování nákladních vozidel. Za externí informační systémy považujeme i řadu systémů veřejné správy, především aplikace celní správy České republiky (on-line nahlížení do systému TARIC, Stav tranzitní nebo vývozní operace, InstatDesk, apod.). V hojné míře využíváme i dnes značně rozšířenou CRM aplikaci Salesforce.

Základním interním informačním systémem je aplikace CargoLink, kterou sdílí většina našich partnerů po celém světě. V tomto informačním systému se uskutečňuje sdílení informací o všech

zásilkách mezi všemi pobočkami, které se o zásilku během její přepravy starají. Tento informační systém používáme i pro fakturaci směrem k zákazníkům. Nejdůležitějším lokálně vyvíjeným systémem je pak unikátní systém pro zpracování poptávek našich zákazníků s názvem DSVCommerce.

Prostě život s IT, jakkoli možná někdy problematický, je daleko jednodušší, než byl dříve. A nepochybně nejen v oblasti logistiky.

*Daniel Rydzi, Business Change Manager, DSV Road a.s.*