Průmysl

Ing. Petr Nobst

Vystudoval Elektrotechnickou fakultu ČVUT (obor Technická kybernetika), byl IT manažerem v Chotěbořských strojírnách a v roce 1996 začal působit na stejné pozici v textilním podniku PLEAS. Od roku 2007 je členem představenstva, od roku 2008 finančním ředitelem.

Když nikdy nikomu nekoupíte žádnou hračku, bude IT stagnovat

Není neobvyklé, že šéf podnikových financí převezme odpovědnost i za IT. Vy jste ale šel opačnou cestou. Technické vzdělání, vedení IT a potom jste byl jmenován finančním ředitelem.

Ano, nastupoval jsem do společnosti PLEAS v roce 1996 jako vedoucí IT. V té době jsme začínali implementovat SAP. O čtyři roky později jsme se pak pustili do podobného projektu v rámci celé korporace, pak přišly další projekty. Poté jsem odešel na dva roky do Německa dělat šéfa IT, a když jsem v té roli obstál, přišla otázka: Implementoval jste ekonomiku a controlling, vidíte do toho, už roky se o tom bavíte, nechcete tomu taky šéfovat? A já tu nabídku přijal. Vrátil jsem se zpět do České republiky jako šéf financí. Možná to tak na první pohled nevypadá, ale po pár implementacích informačního systému toho zpravidla víte o podnikové ekonomice víc než ekonom, který tu firmu nezná. Myslím, že je to lepší škola než obrácený postup. Musíte být ale na projektech ve správné roli. Nestačí být jen konzultant soustředěný na nějaké dílčí záležitosti. Pokud jste šéfem projektu a máte přehled o celé firmě od skladového hospodářství po ekonomiku a controling, za pár let se to naučíte.

Má to i nějaké nevýhody?

Samozřejmě. Zejména pro šéfa IT. Ve většině firem to totiž bývá tak, že chce-li šikovný šéf IT prosadit nějakou investici, dokáže spočítat přesně takovou návratnost, jakou chce vedení vidět. Prostě proto, že ví, jak ta čísla fungují. Ale když jste na pozici finančního ředitele a máte i zkušenost šéfa IT, okamžitě to prohlédnete. Dříve jste dělal to samé, a tudíž znáte metody, jak správně rozvrstvit náklady a jak vytvořit potřebná čísla, která budou stačit ke zdůvodnění investice. Když pak za vámi přijde šéf IT a začne rozkládat svá čísla, hned vidíte, o co jde. Můžete mu rovnou říct: Nechte toho a raději řekněte přímo, co chcete prosadit a kolik na to potřebujete peněz. IT se tím dostává do mnohem horší pozice.

K určitému tření mezi byznysem a IT ale dochází v téměř každé organizaci.

Nemyslím, že to tak nutně musí být. Znám tu situaci z obou stran a myslím, že znám i pohled jiných finančních ředitelů a vedoucích IT. Bývá to spíš o tom, že finanční ředitel může mít určitou obavu z toho, že dost nerozumí IT a že se před ním něco skrývá. Občas to má podobu takového vnitřního nevyjádřeného strachu. IT má zase pocit nepochopení. K těmto pocitům není důvod. Je to spíš historická záležitost. Pokud se toho dokážou obě strany zbavit a podívat se selským rozumem, vždy je možné najít kompromis.

A jak řešit situace, kdy byznys požaduje od IT něco, co je technicky nemožné nebo třeba procesně nesmyslné?

Z mého pohledu je to dáno především tím, že byznys má příliš velkou sílu. Snaží se protlačit svůj nápad a nenaslouchá druhé straně, která říká, že výsledný efekt nebude takový, jaký si představuje.

V posledních letech se hodně diskutuje o vývoji role IT v organizacích. Zda bude trend směřovat k tomu, že by technologie řídil byznys a IT hrálo jen podpůrnou roli, nebo zda bude

naopak IT tím vizionářským útvarem, co posouvá organizaci dopředu. Jaký je váš pohled?

Myslím, že to hodně závisí na typu organizace. Ve firmách poskytujících poradenství, služby atd. to skutečně může být tak, že uživatelé chodí s novými nápady, možnostmi a technologiemi. Ale v běžné výrobní firmě chce zaměstnanec přijít do zaměstnání, udělat svou práci a jít domů. Nemůžete čekat, že každý zaměstnanec bude kreativní, to možná tak někde ve vývojových útvarech. Když chcete takovou organizaci posunout dopředu, musí to být IT, kdo přichází s novými podněty. I jiní uživatelé mohou mít zajímavé nápady, ale IT by mělo být tím, kdo to „učeše“ a promyslí všechny aspekty.

Existuje nějaká společná IT výzva, které by dnes čelila většina českých průmyslových podniků?

Nemyslím, že tu bylo něco srovnatelného třeba se zaváděním ERP. V tom smyslu dnes mají IT firmy obtížnou pozici, protože objem zakázek se zmenšuje. Nicméně jsou tu změny, na které se musíme učit reagovat. Tou asi největší je obecné zrychlování. Nové technologie a systémy nastupují rychleji než dříve. To se týká implementace, nasazení, využití, standardizace… prostě všeho. Třeba chytré mobilní telefony. Když měl někdo před pěti lety telefon, do kterého chodily e-maily, tak byl „king“. Pak měli chytré telefony v IT. A dnes je normální, že i běžný uživatel má v mobilu několik systémů, které mu umožňují číst firemní e-maily, zadávat schůzky, tisknout a číst přílohy… Prostě dělat to, co se dříve dělalo jen v pracovní době. A najednou je běžné, že když zaměstnanec večer sedí doma a v telefonu mu zabzučí e-mail, samozřejmě se na něj podívá. Pro zaměstnavatele to znamená neskutečný benefit. Zaměstnanec má radost z krásného telefonu, ale firmě se to několikanásobně vrátí zpátky. Nemluvím teď o tabletech. Tablet je slepá ulička. Je fajn pro děti, na dovolenou k hrám nebo ke čtení novin, ale práce se přesouvá na mobil. Ten máte neustále u sebe.

A nějaká další výzva?

Přibývá dat. V každém zdánlivě obyčejném stroji je dnes počítač. To vyvolává nároky na přenosy dat, integraci, řízení…

Uvažujete o postupném nahrazování papírů elektronickými dokumenty s právním účinkem?

Podívejte se, papír vymysleli staří Číňané před asi pěti tisíci lety a je tu stále. Jak dlouho tu jsou cédéčka? A jak ještě dlouho budou? Dokážete načíst data ze starých kazet a disket? Až tu bude nějaké médium stejně dlouho jako papír, můžeme se o tom bavit. Co se týče oběhu dokumentů, tam je elektronizace výborná, ale pořád musíte udržovat i papírovou formu.

Když za vámi přijde vaše IT, že potřebuje peníze na novou investici, podle čeho se rozhodujete?

Především říkám, že kdo přijde s požadavkem na investici, musí za ni dýchat. Musí na něm být vidět, že je to pro něj opravdu důležité. Za druhé musí být schopen jasně vysvětlit, jaké budou přínosy. To nemusí znamenat složité vzorečky nebo výpočty, chytrý člověk si je beztak dokáže ohnout, jak potřebuje. Ale musí být jasné, že je to něco užitečného. Tím nemám na mysli investice typu obměny zařízení, kterému skončila životnost. Tam většinou není o čem diskutovat.

Mnoho finančních ředitelů má obavu, že schválí peníze na něco, co se později ukáže jako perfektně fungující hračka pro IT a firmě to fakticky nepomůže.

Je důležité najít rozumný kompromis. Nechceme utrácet za „hračky“, ale kdy-

„Úplně nejlepší je šeptanda. Třeba že kolegyně ze sousedního oddělení něco zanedbala a teď s tím má problémy. To funguje mnohem lépe než jakékoli vývěsky.“

bychom nikdy do žádné „hračky“ neinvestovali, tak se neposouváme dopředu. Třeba už jen ty mobily. Kdybychom byli u každé inovace přehnaně zdrženliví, tak ještě dnes máme Nokii 5110. Byl to dobrý telefon, uměl všechno, co bylo zapotřebí, a všichni s ním byli spokojeni. Ale protože někteří lidé dostali hračky, postupně jsme se učili, že telefon můžeme používat i k jiným věcem. Kdybychom nikdy nikomu nepořídili žádnou hračku, degenerovalo by IT v čistou obnovu.

Jak posuzujete investice do informační bezpečnosti? Podle čeho rozhodujete, kde má smysl investovat do ještě lepší bezpečnosti a kde už ne?

Jsme textilka, nejsme banka ani armáda. Nemáme žádné výrobní tajemství, jako je třeba recept na becherovku. Když projdete naši výroční zprávu, dozvíte se o nás skoro všechno. Vnější bezpečnost tedy řešíme externí službou. Je to firma, která se stará o desítky organizací, je standardizovaná a může investovat do technologií i do lidí výrazně víc, než bychom si mohli dovolit my. Kdyby šlo o armádu, bylo by na místě budovat vlastní interní bezpečnostní oddělení, ale naše situace je zcela odlišná. Nicméně i externí firmu musíte dobře vybrat. Nepřichází v úvahu měnit ji každé dva roky. Musíte ty lidi znát, vědět, co mají za sebou, věřit jim. Co se týče interní bezpečnosti, ta je zaměřená především na lidi.

Takže žádný monitoring dění v sítích a podobné pokročilé věci?

Skutečná rizika jsou jinde. Už minimálně 20 let např. platí, že nejslabším článkem obrany bývá sekretářka. Pokud má vaše sekretářka přítele, který se bude chtít dostat do vaší firemní sítě, nebude pro něj obtížné získat veškerá přístupová hesla. Tomu žádné technologické opatření nezabrání.

Říkáte, že nemáte žádná výrobní tajemství. Ale co třeba připravované smlouvy, speciální slevy, obchodní záměry apod.?

Když jste dostatečně dlouho na trhu, jako je ten náš, už všechny konkurenty znáte. Víte, jak prodávají, jak kalkulují, co kdo může od koho čekat. V něčem je to podobné jako trh s telekomunikačními službami. Tam je taková fluktuace obchodních zástupců, že stejný obchodník během několika let vystřídá O2, T-Mobile a Vodafone. Jaký smysl má chránit v takovém prostředí obchodní tajemství?

„Tablet je slepá ulička. Je fajn pro děti, na dovolenou k hrám nebo ke čtení novin, ale práce se přesouvá na mobil. Ten máte neustále u sebe.“

Nicméně mobily zaměstnanců chráníte. Jak to děláte?

V pracovních mobilech je nasazen MDM nástroj, který nám umožní telefon na dálku smazat, vrátit do továrního nastavení nebo jej vyhledat.

Jak se na to zaměstnanci dívají, že máte takové možnosti?

Myslím, že jim to nijak nevadí.

Ani to, že máte přístup třeba k jejich soukromé intimní komunikaci?

Hovory nemonitorujeme, takovou možnost ani nemáme. Především jde o to, aby si zaměstnanci uvědomili, že když má někdo firemní mobil, notebook, e-mailovou adresu, tak je to primárně určeno pro pracovní komunikaci. Když zaměstnavatel dovolí používat

tyto technologie i pro soukromou komunikaci, je to jeho benevolence. Jestli se někdo bojí o svůj soukromý obsah, nechť ho neukládá do firemního zařízení.

Zaměstnanci si tedy nemohou přinést své zařízení, musí pracovat s takovým, které jim přidělíte?

S vlastním zařízením zásadně nesouhlasíme. To si mohou dovolit firmy, které začínají na zelené louce. U nás se používá jednoznačně definované firemní zařízení.

Mohou si zaměstnanci vybrat oblíbený model?

Zaměstnanec si může vybrat, jestli firemní zařízení chce nebo nechce. Ostatní je dáno firemní politikou – typ počítače, monitoru, notebooku, automobilu, mobilního telefonu, a to včetně barvy.

Zaměstnanci to akceptují? Nestává se, že přijde manažer a nárokuje si, aby mohl používat svůj iPhone?

Víte, mou výhodou je, že nejsem jen finančním ředitelem, ale také členem představenstva. Takže manažer přijde za členem představenstva a ten mu vysvětlí situaci. Nestává se ale, že by kolem toho vznikaly konflikty. Spíš dochází k tomu, že když obměňujeme telefony, ne všichni to přijímají vřele. Ale naučí se s nimi zacházet a všechno je v pořádku. A pak za vámi chodí a říkají: Proč jsme to nedostali už dříve?

Jak se u vás řeší školení zaměstnanců o informační bezpečnosti? A jak je to s nároky na hesla?

Znám firmy, kde to mají tak, že heslo nesmí být osmkrát po sobě stejné ani mít stejný základ, musí mít 14 znaků, mají v něm být velká a malá písmena apod. Potom do takové firmy přijdete, otočíte klávesnici a najdete tam všech 8 hesel, jak po sobě následovala. Ale jsou firmy, které nemají takové nároky na hesla, občas udělají osvětu a řekl bych, že je to mnohem bezpečnější. Lidé se své heslo naučí, osvojí si i nějaké standardy chování a dodržují je. Když je občas maličko „postrašíme“ a doporučíme jim, jak se mají chovat, udělají to. Vědí, že každý je zodpovědný za to, co dělá a co posílá. Jestli někdo dá své heslo někomu cizímu, kdo napíše jeho jménem třeba členu představenstva, je to jeho odpovědnost. Není to technologická záležitost, spíš pracovněprávní, spojená s rozumnou osvětou, aby si lidé uvědomili, co se může stát.

> „Jsme textilka, nejsme banka ani armáda. Nemáme žádné výrobní tajemství, jako je třeba recept na becherovku. Když projdete naši výroční zprávu, dozvíte se o nás skoro všechno.“

Jak je možné lidi „strašit“?

Jde spíš o to, že na poradách upozorníme na nějaký problém a že by se mohlo něco stát. Ale úplně nejlepší je šeptanda. Třeba že kolegyně ze sousedního oddělení něco zanedbala a teď s tím má problémy. To funguje mnohem lépe než jakékoli vývěsky.

To ale znamená, že občas někoho musíte exemplárně potrestat.

Ano, to se občas opravdu stává. Když už to ale musíme udělat, snažíme se, aby z toho bylo dobré interní PR ve smyslu zvýšení povědomí o informační bezpečnosti.

Jaký je váš pohled na cloud?

Vlastně je to něco podobného jako outsourcing někdy v roce 2002. Tehdy všichni outsourcovali, mluvilo se o tom, že IT bude služba, spousta činností se dávala ven. Až teprve po čase všem došlo, že některé činnosti si musí nechat a především přijmout rozhodnutí o tom, u kterých znalostí je přípustné, že je firma ztratí. Umím si představit, že pro firmu, která vzniká na zelené louce a má jen pár zaměstnanců, to může být vhodné univerzální řešení. Dám všechno do cloudu a neřeším, jestli mi to bude za pět let ještě vyhovovat. Ale firma, za kterou je určitá tradice a roky vývoje, tam je to úplně jiné. Dovedu si představit některé věci v cloudu, ale není to univerzální řešení. My využíváme mobilní aplikace v interním cloudu. Dodavatel tu službu poskytuje jako externí cloud, ale my jsme ji nechtěli mít úplně mimo firmu, tak jsme jej požádali, aby ji nasadil u nás. Při rozhodování o cloudu musíte myslet i na uživatele a na to, co je pro ně přijatelné. Když máte malou firmu, kde pracují mladí lidé, může být pro vás dobrá volba Office 365. Ale ve velké organizaci, kde je řada zaměstnanců před důchodem, je nepřijatelné měnit každé dva roky verzi office. Zjistíte, že někteří raději odejdou předčasně do důchodu, než by se neustále učili nový software. Prostě musíte být trochu konzervativní.

Dá se to shrnout tak, že váš postoj je pragmatický, že záleží na praktických aspektech a že bezpečnost nevidíte jako fatální problém?

Přesně tak. Když se mě lidé ptají, zda bych souhlasil s umístěním našich dat v cloudu, odpovídám: Víte, kolik je na světě dat? Myslíte, že zrovna ta vaše jsou ta nejzajímavější? Myslíte, že všichni chtějí vidět vaše fotografie? Kdybyste byl slavná celebrita nebo politik, musel byste být opatrný. Ale u normálních řadových občanů to není nutné přehánět.

Ptal se Petr Hampl.