ČESKÝ INSTITUT INTERNÍCH AUDITORŮ

The Institute of Internal Auditors

3|2014

INTERNÍ AUDITOR

ROČNÍK 18, ČÍSLO 3–2014 (73)
ČTVRTLETNÍK ČESKÉHO INSTITUTU INTERNÍCH AUDITORŮ

3/2014 POHLEDY NA BEZPEČNOST | 3/2014 POHLEDY NA BEZPEČNOST | 3/2014 POHLEDY NA BEZPEČNOST | 3/2014 POHLEDY NA BEZPEČNOST

OBSAH

Vážené čtenářky, vážení čtenáři,

pro většinu z nás již skončila hlavní část dovolené, kterou nejčastěji čerpáme v letních měsících. Doufám, že se Vám vydařila a přinesla Vám tolik potřebné osvěžení a nevšední zážitky. Určitě při svých cestách často využíváte nějakou formu pojištění, alespoň pro jistotu. Také to tak činím, abych nabyl jistoty a klidu, kdyby se přece jenom něco přihodilo. Vždyť na cestách v neznámém prostředí se můžeme setkávat s různým nebezpečím, bezpečnostními riziky.

Není nic smutnějšího, než když nám naše plány, výsledky práce, očekávané bonusy a jiná očekávání zhatí menší či větší bezpečnostní incident. Bezpečnostní rizika s námi žijí stejně jako ostatní rizika, a jak víme, mnohdy nás nečekané události zaskočí. A děje se tak jak v osobním, tak i pracovním životě. Zejména na bezpečnost v pracovním prostředí je zaměřeno toto číslo časopisu.

V anketě časopisu se ptáme na pohled Vás čtenářů na bezpečnostní rizika a jejich očekávaný vývoj v následujícím období. Oslovené autory jsme zase požádali, aby se podělili o svoje zkušenosti s bezpečností v praxi. Výsledkem by měla být i informace pro Vás čtenáře, jaký je stav ve vývoji bezpečnostních rizik v našem okolí, na co si dávat největší pozor, jak rizika eliminovat, jak zajistit prevenci. Jako červená nit se téměř všemi články k tomuto tématu vine lidský faktor.

Jako vždy přináší toto číslo standardní rubriky, včetně soutěže a fejetonu. Určitě zajímavá je informace z mezinárodní konference IIA v Londýně. Tam se na pár dní sešli interní auditoři z celého světa a seznámili se s tématy, která jsou aktuální v mezinárodním měřítku. Samozřejmě o nich i živě diskutovali.

Za redakční radu Vám přeji inspirativní a bezpečné čtení.

Jan Kovalčík

Vydává
Český institut interních auditorů, z. s.
Karlovo nám. 3
120 00 Praha 2
tel.: +420 224 920 332
+420 224 919 361
e-mail: ciia@interniaudit.cz
www.interniaudit.cz

Redakce INTERNÍ AUDITOR
Karlovo nám. 3
120 00 Praha 2
Registrace: MK-ČR-E-12322
ISSN 1213-8274

Redakční rada:
Vedoucí – Jan Kovalčík, Petr Cerman, Petr Hadrava, Daniel Häusler, Šárka Nováková, Andrea Káňová, Pavla Kostřibová, Petra Škvorová, Kateřina Zonygová

Ilustrace: Jitka Holečková
Foto: archiv ČIIA
Neprodejné, určeno pro Český institut interních auditorů
Náklad: 1 200 výtisků
Pre-press: Viktor Beránek
Tisk: Reproservis, s. r. o.
Distribuce: Mail Step a. s.

Zdeněk Macháček
ředitel úseku bezpečnost
Česká spořitelna, a.s.
zmachacek@csas.cz

DOBŘE ŘÍZENÁ BEZPEČNOST MINIMALIZUJE PŘÍPADNÉ ŠKODY

Bezpečnost je jedna z nejdůležitějších lidských potřeb. Bez primárního pocitu bezpečí nedokážeme v rámci společenství logicky a smysluplně fungovat. Moderní organizace je ve své podstatě také formou společenství a živým organizmem, který k efektivnímu fungování nutně potřebuje určité bezpečnostní mechanizmy. Žádná úspěšná organizace se tak dnes neobejde bez analýzy možných rizik, zavedení účelných opatření, jejich otestování v praxi a následného vyhodnocení.

„To, že je řeka klidná, neznamená, že v ní nejsou krokodýli."
malajské přísloví

Na začátku je důležité odpovědět si na základní otázky – co chceme chránit, proti komu a jak.

OCHRANA OSOB A MAJETKU

Z pohledu organizace je třeba brát v úvahu tři hlavní okruhy bezpečnostních opatření.

Prvním je **fyzická bezpečnost**, jejímž cílem je ochrana před neoprávněným vniknutím, krádeží nebo poškozováním majetku firmy. Velmi často bývá integrována s problematikou BOZP a PO. K zajištění fyzické bezpečnosti se využívá lidská ostraha nebo technologický dohled, tedy například kamerové a poplachové systémy. Oba mechanizmy mají svá pro i proti, proto se zpravidla kombinují tak, aby se jejich výhody a nevýhody vyvážily. I tento hybridní systém však má svá úskalí, a to především v interakci lidského faktoru a technologie.

Při řízení BOZP a PO se klade důraz především na prevenci rizik možného ohrožení zdraví a bezpečí zaměstnanců a majetkových škod. Soustavným monitorováním a vyhledáváním rizikových faktorů se podchycují nové hrozby, které vznikají především při použití nových technologií, s nimiž nejsou zaměstnanci dostatečně sžiti. Oproti minulým letům se také zvyšuje riziko úrazu při řízení služebního vozidla, a to především kvůli vyšší intenzitě osobní a nákladní dopravy.

V rámci prevence BOZP a PO v České spořitelně probíhají pravidelné kontroly pracovních podmínek, kontroly jednotlivých pracovišť, zdravotní prohlídky zaměstnanců a pravidelná školení. Správnost zvoleného směru a nastavení sytému péče o BOZP a PO potvrzují i výsledky kontrolní činnosti státního odborného dozoru, který provádí ročně více než 80 kontrol na pracovištích České spořitelny.

PRIORITA? BEZPEČNOST KLIENTŮ A JEJICH DAT

Druhým okruhem je **zajištění personální bezpečnosti**, při které jde především o ochranu před selháním lidského faktoru a s tím související ochranu dat klientů. Základní rámec ochrany dat je dán legislativou ČR. Stěžejní je přitom zákon o bankách, zákon o ochraně osobních údajů a nařízení ČNB. Vhodným doplňkem tohoto rámce jsou normy ISO 27000.

Česká spořitelna má vytvořen systém hlášení rizik při podezření na porušení bankovního tajemství či ztrátu dat. Zaměstnanci jsou oprávněni vstupovat do klientských systémů a dokumentace pouze v souvislosti s plněním konkrétních pracovních úkolů. Jednotlivé aplikace jsou logovány a v případě šetření je hodnocena konkrétní činnost zaměstnance v kontextu s činností vykonávanou pro klienta. Zaměstnanci jsou povinni nezneužívat klientskou dokumentaci k získání jakýchkoliv výhod. Toto bezpečnostní a reputační riziko ošetřuje pracovní řád, který zajišťuje vymahatelnost dodržování těchto pravidel. Nad rámec pasivního dohledu nad daty klientů má spořitelna i aktivní monitorovací systém, který vyhodnocuje pověřený zaměstnanec. Ten podle konkrétních matic zkoumá vygenerovaná data a upozorňuje nadřízené zaměstnanců, kteří se dopustili nepovoleného přístupu.

Důležitou součást preventivních opatření tvoří školení zaměstnanců a provádění kontrol osob, které se ucházejí o místo ve firmě, prověřování jejich minulosti na základě referencí a dostupných zdrojů (obchodní rejstřík, katastr nemovitostí apod.).

Také se fyzicky provádějí metodické prověrky a bezpečnostní inspekce na konkrétních pracovištích České spořitelny. Dalším kontrolním mechanizmem je transakční monitoring, díky němuž je sledován objem dat stažených z internetu a návštěv sociálních sítí. Následně se vyhodnocuje, zda tyto návštěvy jednotlivých zaměstnanců byly realizovány v souvislosti s výkonem práce pro banku.

V případě, že je zjištěno pochybení, překročení pravomocí, korupce nebo vynášení důvěrných informací, dochází k šetření zjištěných incidentů a následně jsou přijata systémová opatření, aby k podobnému selhání v budoucnu již nedošlo.

„Bezpečnost je jedna z nejdůležitějších lidských potřeb“

BEZPEČNOST V IS/IT

Třetím okruhem, který v posledních letech nabývá na významu s překotným rozvojem moderních technologií, je **zajištění informační bezpečnosti**. Většina bankovních služeb je dnes poskytována i elektronicky, prostřednictvím elektronických či alternativních distribučních kanálů. S prudkým rozvojem moderních cloudových a mobilních technologií a s neustálým důrazem na ochranu a bezpečnost dat vyvstává otázka, jak vše spolehlivě zabezpečit uvnitř prostředí banky. Často to znamená změnit celou strategii ochrany dat.

V České spořitelně je bezpečnost informačních systémů a informačních technologií součástí celkového řízení rizik a je jí věnována velká pozornost. Naší devizou a zároveň odměnou za toto úsilí je důvěra klientů v bezpečnost našich služeb. Víme, že to nejdůležitější, co musíme chránit, jsou data, a to ve všech jejich významech, výskytech a v použití v prostředí informačních systémů banky. Ke klasifikaci a ochraně dat byla zpracována rozsáhlá metodika a možná bezpečnostní rizika pro jednotlivé části informačního systému banky se průběžně analyzují. Jedná se o nikdy nekončící a stále se opakující proces.

Spořitelna používá v současné době cloudové řešení, vybrané bankovní aktivity outsourcuje u třetích stran a má stanoveny bezpečnostní zásady pro používání mobilních výpočetních prostředků (notebooků, tabletů a chytrých telefonů) v bankovním prostředí.

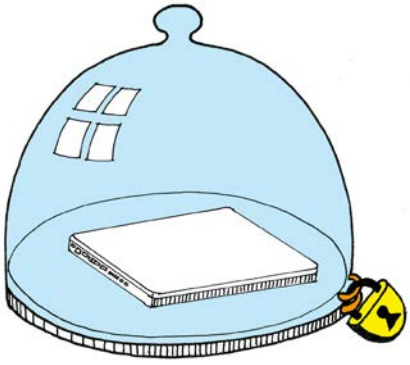
AKTUÁLNÍ HROZBY V BANKOVNÍM SEKTORU

Z pohledu bezpečnosti jsou banky a finanční instituce obecně pod drobnohledem laické i odborné veřejnosti více než jakákoliv jiná organizace. Nepatrným šlápnutím vedle může respektovaný bankovní dům přijít nejen o hmotné prostředky, ale především o důvěru klientů a o dobrou pověst, kterou si budoval dlouhá léta.

Kromě možnosti selhání v oblasti personální bezpečnosti, v níž může dojít k úniku a zneužití dat způsobenému úmyslně či v důsledku neúmyslného selhání lidského faktoru, se vytváří velký prostor pro vznik krizové situace právě v rámci informačních systémů a technologií. Nejaktuálnější hrozby v oblasti finančnictví představují:

- neplánované výpadky IT a komunikačních služeb, při kterých dochází ke ztrátě dostupnosti informačního systému z důvodu přerušení datového či napájecího elektrického vedení;
- kybernetické útoky DoS a DDoS, které mají za následek nedostupnost služby;
- kybernetické útoky v podobě malwaru, phishingu a podobně;
- únik dat a ohrožení integrity například chybou v databázové transakci;
- ztráta důvěrnosti způsobená například vlivem přístupu neoprávněné osoby k datům.

Ke konkrétním a nejčastějším hrozbám současnosti, se kterými se finanční instituce potýkají v souvislosti s rozvojem moderních technologií, patří kybernetické útoky jako phishing (rozesílání falešných zpráv pod identitou banky za účelem získání přístupových informací k účtu klienta), pharming (sofistikovaný útok spočívající v přesměrování uživatele z oficiálního webu banky na alternativní server, a to opět za účelem získání identifikačních dat k účtu klienta) a malware (počítačové viry, trojské koně, spyware a adware, jejichž cílem je ovládnout zařízení klienta banky a sbírat v něm informace).



Při zabezpečení systémů IS/IT je důležité zohlednit dva směry ochrany. Jde jednak o zabezpečení informace formou šifrování, přístupových hesel, logováním přístupů a činností nebo klasifikací dat, jednak o ochranu komunikačních cest, například před odposlechy.

uvědomuje rostoucí závislost klíčových aktivit a procesů na technologiích. Ty na jedné straně zvyšují komfort a nabízejí široké spektrum příležitostí pro rozvoj poskytovaných služeb i optimalizaci nákladů, na straně druhé je však třeba je vyvážit racionálním přístupem organizace k moderním technologiím a striktním dodržováním bezpečnostních zásad a standardů.

„Žádná úspěšná organizace se dnes neobejde bez analýzy možných rizik“

NA CO NEZAPOMÍNAT

Bezpečnost by měla být přirozenou součástí každodenního života organizace, ale nesmí omezovat a obtěžovat v běžném pracovním výkonu. Bezpečnostní pravidla a mechanizmy musejí být nastaveny jasně a srozumitelně a v zájmu účinnosti musejí být vymahatelné. Pokud má být ze strany zaměstnanců bezpečnostní systém organizace respektován, musí být jeho ochrana zjevná, aby si ji lidé uvědomovali a neměli tendence systém obcházet a ignorovat.

V případě potenciálních hrozeb u organizací typu banky nesmíme opomíjet ani ohrožení samotného uživatele moderních technologií a systémů navázaných na bankovní servis. Ne každý uživatel si uvědomuje, že za používání uživatelsky přátelských aplikací v moderních zařízeních platí daň, která spočívá ve ztrátě důvěrnosti některých informací nebo zvýšení hrozby ze strany lidí, kteří chtějí získat informace nebo finanční prostředky uživatele. Oběťmi takových útoků se dennodenně stávají miliony lidí po celém světě a pro nejbližší období musíme počítat s tím, že aktivita útočníků vůči našim klientům a jejich zařízením poroste. Naším úkolem proto je uživatele neustále informovat a vzdělávat v oblasti možných rizik a způsobů, jak se jim bránit.

PREVENCE JAKO NEJÚČINNĚJŠÍ NÁSTROJ

Závěrem nezbývá než konstatovat, že hlavní hrozby pro fungování organizací i trendy v oblasti bezpečnosti jednoznačně souvisejí s rozvojem informační společnosti. Veřejnost si

Ochrana bezpečnosti je náročná ve všech ohledech a v některých směrech se nám nikdy nepodaří se možným rizikům bránit skutečně efektivně. Vynalézavost kybernetických útočníků je prakticky bezmezná. V této oblasti tak vzniká potřeba kontinuálních preventivních analýz rizik na straně banky a maximální obezřetnosti při práci s internetem a mobilními zařízeními na straně uživatele.

Pro to, jak zajistit bezpečný a plynulý chod firmy bez nežádoucích výpadků, žádné univerzální pravidlo neexistuje.

Jedním z efektivních nástrojů, jak mapovat a chránit kriticky důležité procesy a činnosti, včetně dostatečných zdrojů a kapacit pro efektivní obnovu, je však řízení kontinuity činností (business continuity management – BCM). Zavedením tohoto systému a opakovanou údržbou – plánováním, testováním, aktualizací a rozvojem – lze výrazně snížit riziko zásadních dopadů hrozeb téměř v jakékoliv organizaci, a to bez ohledu na její velikost a zaměření.

V České spořitelně hraje BCM nezastupitelnou úlohu. Bohužel to tak není zdaleka všude. Podle průzkumu České zemědělské univerzity využívá řízení kontinuity činností pouze 18,9 % oslovených organizací, přičemž 50 % z nich jsou podniky se zahraniční účastí, kde je BCM zpravidla standardním požadavkem mateřské společnosti. Důvodem neochoty firem věnovat se řízení kontinuity činností jsou podle respondentů vysoké náklady a nedostatečná podpora managementu, ale především vnímání BCM jako nedůležité oblasti.

Je však dobré si uvědomit, že správné řízení bezpečnosti organizace vede k minimalizaci způsobené škody – pokud už se jí nelze vyhnout. ▲

Radek Kučera
Senior Head of Business Security Outer Liaisons
T-Mobile Czech Republic a.s.

ČLOVĚK – NEJVÍCE PODCEŇOVANÉ BEZPEČNOSTNÍ RIZIKO

Za dobu své praxe bezpečnostního experta jsem se v životě setkal s mnoha názory na bezpečnost a na to, jakým způsobem ji tu zesílit, tu naopak učinit méně viditelnou, jak ji financovat, jak ji naroubovat na podnikové prostředí, jak, jak, jak. Zkrátka stejně jako tomu bývá u mnoha jiných povolání, co člověk, to jiný názor. Řada lidí se pohybovala v určitém zajetí názorových stereotypů typu, co nejde silou, musí jít ještě větší silou, a tak často navrhovali více kamer, více plotů, více zámků, více antivirů, dohledů, kontrol a strážných. Bohužel, bezpečnost nepřináší na první pohled okamžité výnosy do společnosti, naopak poměrně dost prostředků spotřebuje, a tak se většina bezpečnostních ředitelů potýká se stále stejným problémem, a to jak vytvořit funkční bezpečnost v organizaci za stále méně peněz. Finanční krize započatá v Evropě v roce 2008 zaťala do tak bezútěšného stavu další ránu, neboť velmi často byly výdaje na bezpečnost omezeny, a to zvláště ty, které měly působit preventivně první na ráně, a tak tam, kde dříve byli dva strážní, dnes není ani jeden.

Pozornému čtenáři rozhodně neuniklo, že veškeré nástroje, které jsem vyjmenoval v prvním odstavci, jsou prostředky, které mají někomu zabránit či ztížit páchání protiprávní činnosti. A to lecjaké od vandalizmu přes krádeže a zpronevěry až např. po sofistikované hackerské útoky. Ale proti komu mají vlastně chránit? Odpověď je samozřejmě prostá. Proti samotným lidem. Ale proti kterým? „No samozřejmě proti těm venku," zní odpověď většiny laiků. „A chrání vás tyto dveře také před těmi, kteří už jsou uvnitř?" ptal jsem se já. Po chvíli mlčení a významném točením očima mi bylo často odpovězeno asi nějak takto „No, to kategoricky vylučuji, to se u nás nemůže stát," případně doprovázené větou, která je z hlediska bezpečnosti zcela devastující „my si tady věříme". Zkušenosti mě naučily nedívat se na bezpečnost skrze sílu instalovaných mříží, ale jen a pouze přes ty, kteří bez výhrady stojí za tím, když bezpečnostní standardy selhávají. Za samotnými lidmi. Neboť lidem je často věnováno trestuhodně málo pozornosti. Protože k čemu mi jsou zamčené dveře, když klíč má ta špatná osoba.

„Přestože se jednalo o člověka, který měl nastoupit do výkonu trestu odnětí svobody, nastoupil místo něj do telekomunikační společnosti, kde to dotáhl až na post generálního ředitele"

PROVĚŘOVAT ZAMĚSTNANCE? NO PROSÍM VÁS...

Přestože některé standardy, které se týkají možného bezpečnostního prověření budoucího zaměstnance, jsou známy v anglo-saském světě již dlouho, v Evropě a speciálně v České republice si nacházejí cestu k zaměstnavatelům jen velmi pozvolna. Zčásti za to může neblahá zkušenost lidí s totalitním režimem, kdy

ANKETA ČIIA

OTÁZKY

POHLEDY NA BEZPEČNOST

1. Jaká závažnější bezpečnostní rizika se vyskytují v organizacích Vašeho typu?

2. Která bezpečnostní rizika jsou, dle Vašeho názoru, v současné době největší?

3. Co lze, dle Vašeho názoru, v oblasti vývoje bezpečnostních rizik očekávat v následujících třech letech?

Alena Marcínová

vedoucí odboru Interní audit a procesy
ČEPS, a.s.

1. Jako strategicky významná firma se snažíme bezpečnostní rizika předvídat a snižovat jejich pravděpodobnost. Velkým rizikem pro stabilitu soustavy je energie z obnovitelných zdrojů, především energie z větru.

2. Největším bezpečnostním rizikem je zřejmě nějaká forma teroristického útoku.

3. Bohužel zřejmě teroristické útoky a sabotáže.

František Orság

OSVČ
poradce – kontrolní a auditní systémy

1. Jako OSVČ mohu konstatovat, že se snažím rizika, která by se mě mohla týkat, minimalizovat tak, aby u mne neplatila následující věta: Aniž si to manažeři mnohdy uvědomují, je to riziko zneužití či úpravy informací, obsažených v ICT systémech.

2. Odpověď je obsažena v předcházející odpovědi.

3. Vzhledem ke klimatickým podmínkám očekávám zvýšení výskytu a dopadu rizika povětrnostních a klimatických vlivů s dopadem na zemědělství a logistiku ostatních odvětví.

Ing. Dana Vojíková, MSc, MBA

interní auditor senior
Magistrát města Plzně

1. Pokud budeme opomíjet rizika související se zneužitím informací v IS/IT veřejné správy a jejich písemných materiálech, tak jde převážně o rizika odcizení, zneužití, zpronevěry, poškození (vandalizmus, přírodní katastrofy) aktiv města. Dále rizika týkající se osob – zaměstnanců veřejné správy např. poškození zdraví úrazem, nákazou, nemocí z povolání nebo útokem jiné osoby (nespokojený klient). Dále jinou kapitolou jsou klíčová rizika povahy útoku na stěžejní infrastrukturu státu a veřejné správy.

2. Největší rizika jsou rizika zneužití, odcizení informací a rizika poškozování, zpronevěry, krádeže majetku veřejné správy. V úvahu by mohlo přicházet i vydírání veřejných osob.

3. Nadále bude pokračovat snaha o zneužívání a odcizení informací v informačních systémech veřejné správy.

Ludmila Jiráňová

vedoucí interního auditu a kontroly ČHMÚ

1. Bezpečnostní rizika v ČHMÚ vidím převážně v oblasti informačních technologií. Rizika bych ještě rozdělila na „interní" – zaměstnanci v dodržování nastavených předpisů a norem + „externí" – dodávky elektřiny, odborníci IT (cizí).

2. Za základ bezpečnostních rizik považuji „lidský faktor" v návaznosti na oblast IT – opomenutí, přehlédnutí, ale může zde být i určitý záměr.

3. Vývoj bezpečnostních rizik je v posledních letech tak rychlý, že nebudu předvídat ani věštit z koule, ale nechám se překvapit. Lidé by si měli uvědomit, že ČAS je neúprosný, PŘÍRODA je mocná a „nic se nemá přehánět".

byl člověk poměrně bedlivě sledován nejen ozbrojenou mocí, ale rovněž uličními výbory, a především kádrovými odděleními v jednotlivých podnicích. S úplně stejným pohledem jsem se potýkal i já, při snaze zavést některé tyto prověrky v naší společnosti. „A to se jako budeme těm lidem dívat do ložnic?" „Ne nebudeme, ale co o těch lidech vlastně víme?" „No, vždyť tu máme jejich životopisy, ne?" „Tam přeci najdeme všechno." Tak nějak probíhaly diskuze na toto téma ještě v roce 2008. Zkombinujeme-li zkušenost z totalitního režimu, navíc s častou nezkušeností některých personalistů, kteří jednoduše nevědí, jak by jim bezpečnostní screening zaměstnanců mohl pomoci, začínají nám důvody pro odmítání těchto nástrojů krystalizovat. Nejhorší je pak kombinace těchto faktorů s pocitem pošlapání vlastního ega, kdy někteří personalisté vnímají bezpečnostní screening jako projev nedůvěry k jejich vlastní práci. A když se k tomu přidají nutné investice, pro takovou prověrku, máme tady ukázkově zabetonovaný stav. K celkové nervozitě samozřejmě přispívá rovněž ne úplně vyjasněná právní opora pro takovou prověrku, kdy zaměstnanec požívá vysoké ochrany ze zákona, a žaloby zaměstnanců na zaměstnavatele nejsou v dnešní době ničím výjimečným. Pro úplnost pak jen dodám, že řada zaměstnavatelů se navíc v dnešní době plně spoléhá na služby personálních agentur, které však jakékoliv prověření neprovádějí zpravidla vůbec. A tak zde máme perspektivního uchazeče se skvělým životopisem, na kterého pěl předcházející zaměstnavatel samou chválu a jehož podpis na pracovní smlouvě bude pro naši společnost skutečným požehnáním. Opravdu? Nebo žijeme v iluzi?

TELEKOMUNIKAČNÍ ANIČKA A TI DRUZÍ

Pokud si do jakéhokoliv vyhledavače zadáte výraz „telekomunikační Anička", nabídne se vám příběh, o jakém jste si mysleli, že se nemůže stát. Václav Fůra se více jak deset let vydával za svého bratra Romana Fůru. Přestože se jednalo o člověka, který měl nastoupit do výkonu trestu odnětí svobody, nastoupil místo něj do telekomunikační společnosti, kde to dotáhl až na post generálního ředitele. Za celou dobu nikdo neměl o jeho skutečné identitě ani ponětí. Prostě stejně jako v případě Aničky Škrlové, která se pro změnu dosti úspěšně vydávala za chlapce. Naštěstí pan ředitel neměl podpisové právo na finanční transakce. „No jo, ale to bylo v roce 2000," namítnou někteří. A pracoval dobře a nic neukradl. Možná, že v tomto případě to bylo ještě levné. Následující případ však máme všichni ještě v živé paměti.

> „Obecně se uvádí, že zhruba 30 % životopisů obsahuje zkreslené informace, a 40 % pak přímo informace lživé"

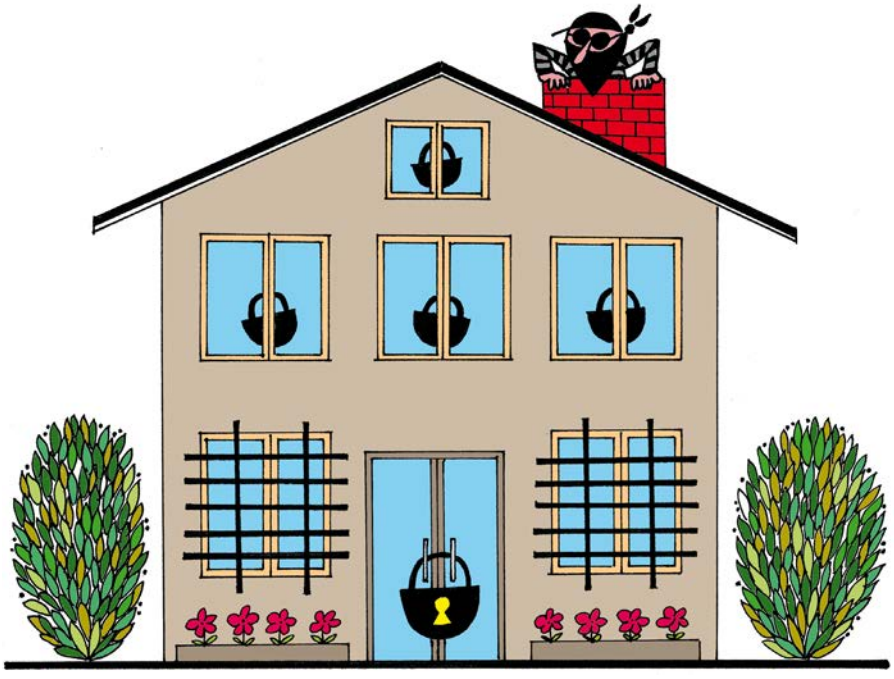
V létě roku 2008 přichází na konkurz na obsazení místa hlavního ekonoma do českobratrské církve evangelické Libor Liška. Liška tento konkurz vyhraje a do roku 2009 postupně převede na své účty přes 10 milionů korun. Když jej přijdou policisté zatknout, vychází najevo, že se jedná o mnohokrát soudně trestaného Vladimíra Prokopa. O něm se později soudní znalci vyjádří jako o asociální osobě s inteligencí v pásmu podprůměru. Ani to však Prokopovi nezabrání utéci z vězení a pro změnu vyhrát konkurz na ekonoma Národního zemědělského muzea, kde vystupuje jako vystudovaný inženýr ekonomie. Zde se mu opět až do jeho zatčení podařilo zpronevěřit dalších téměř 10 milionů korun. Je zřejmé, že i v tomto případě jakékoliv prověření selhalo, a to dokonce opakovaně. A co se s tím dá tedy dělat?

CO NÁM PŘINÁŠÍ BEZPEČNOSTNÍ SCREENING

Velmi pravděpodobně by podobným scénářům zabránil bezpečnostní screening, který by se měl provádět s každým uchazečem o zaměstnání, který nastupuje na místo, kde bude disponovat firemními finančními prostředky, přístupy k utajovaným skutečnostem nebo bude mít i nejvyšší

administrátorská práva k počítačovým systémům. Ve společnostech je tento proces znám často pod názvem background check či pre-employment screening. Cena za takové prověření je vcelku zanedbatelná oproti prostředkům, které společnost ochrání, a prostředkům, které bude muset společnost vynaložit při hledání jiného kandidáta. Cílem prověření je pouze ověřit, že všechny skutečnosti, které o sobě uvedl uchazeč ve svém životopise, se zakládají na pravdě a nejsou zkreslené. Tyto informace jsou zjišťovány z veřejných databází. Detailní popis toho, jakým způsobem takový screening provádět, by značně překračoval rámec mého příspěvku, nicméně je třeba připomenout, že k prověření kandidáta je třeba jeho výslovného souhlasu, plné moci a souhlasu se zpracováním osobních údajů. Rozsah prověrky se může značně lišit dle zadání společnosti, ale i ta nejběžnější by vždy pokrývala ověření identity, lustraci v databázi neplatných dokladů, ověření u předchozího zaměstnavatele a samozřejmě také to, zda uchazeč vystudoval školy v životopise uvedené a získal certifikáty, kterými se v životopise zaštituje.
Ve společnostech se zpravidla provedením této prověrky pověřuje externí subjekt, který by měl mít dostatek zdrojů a erudice k provedení takové prověrky. Zde bohužel narážíme velmi často na fakt, že pokud už zaměstnavatel souhlasí s prováděním těchto prověrek, často je pro něj klíčovým faktorem výběrového řízení pouze cena za takovouto prověrku. To často znamená, že prověrky se provádí velmi formálním způsobem, tak říkajíc od stolu, alibisticky a pouze prostřednictvím telefonu či e-mailu. Je pochopitelné, že taková prověrka potom často neodhalí skutečnosti, kvůli kterým se vlastně realizuje, což dále zvyšuje nedůvěru personalistů v účinnost a nutnost takového nástroje. Výsledek prověrky externí subjekt nijak nehodnotí, pouze tyto výsledky předá odpovědné osobě s personální pravomocí, na které bude, jakým způsobem s ní naloží.

Na téma, jakým způsobem o sobě potenciální zaměstnanci lžou, bylo provedeno několik studií, přičemž čísla jsou poměrně alarmující. Obecně se uvádí, že zhruba 30 % životopisů obsahuje zkreslené informace, a 40 % pak přímo informace lživé. Zájemci si tyto studie, včetně metodiky, jakým způsobem byly prováděny, mohou sami najít na internetu. Já sám jsem se dosud setkal s několika kandidáty, jejichž některé uvedené údaje nebylo možné ověřit, a dokonce rovněž s případem, kdy bylo předloženo padělané maturitní vysvědčení. Poněkud citlivým problémem se v dnešní době stávají informace o kredibilitě či bezdlužnosti, a to ať už vůči komerčním subjektům, či finančním úřadům. V podstatě téměř každý má dnes nějaké závazky, které zcela jistě nepředstavují problém pro přijetí do zaměstnání. Varující jsou spíše závazky, které se zcela vymkly z rukou, tedy například, když už je na potenciálního uchazeče vedeno několik exekučních řízení.



Pavel Broda

interní auditor
OKD, a.s.

1. Hlavní bezpečnostní rizika identifikujeme v několika oblastech. V oblasti fyzické bezpečnosti jde především o riziko krádeže. Další významné riziko představuje podvodné jednání (ať už z řad zaměstnanců, či externích subjektů). Oblast rizika podvodu zahrnuje prakticky veškeré činnosti podniku. Nejzávažnější riziko podvodu vnímám především v oblasti nákupu a výběrových řízení. V neposlední řadě se jedná o rizika spojená s informačními technologiemi a systémy.

2. Za nejvyšší bezpečnostní riziko v současné době považuji riziko podvodného jednání. Snaha externích subjektů spáchat podvod na organizaci může být v současnosti navýšena i kvůli změnám v Občanském zákoníku, na které nemusí být ještě všichni zaměstnanci společnosti plně připraveni.

3. V následujících několika letech neočekávám žádné bouřlivé změny v oblasti bezpečnostních rizik. Dá se očekávat posílení rizik v oblasti IT. Naopak nejasností kolem nového Občanského zákoníku by mělo postupně ubývat.

Simona Székelyová

vedoucí útvaru interního auditu
Státní tiskárna cenin, s.p.

1. S ohledem na charakter činnosti v organizaci jsou to především rizika týkající se narušení systémů a objektů.

2. V současné době vnímám jako aktuální rizika informační – narušení bezpečnosti dat, zneužití či poškození dat nebo informačního systému.

3. Vzhledem k rychlému vývoji informačních a komunikačních technologií očekávám identifikaci významných rizik v dané oblasti.

Je jasné, že zaměstnat takovou osobu jako pokladníka v bance může být ruskou ruletou se smrtícími následky pro firemní finance.

CO SE MOŽNÁ ODHALIT NEPODAŘÍ

Bohužel existují věci, které se často nepodaří odhalit, ani při sebedůkladnějším prověření. Osobně považuji za ty nejzávažnější, kterým čelíme v dnešní době, dvě, a to zneužívání omamných a psychotropních látek a patologické hráčství. Kolegové pracující na úseku bezpečnosti v jiných společnostech potvrzují, že podobným problémům čelí ve zvýšené míře i oni, nejedná se tedy pravděpodobně jen o nahodilou odchylku a sezonní problém. A tak zatímco v některých dělnických profesích je častým problémem alkohol a marihuana, v technologických či bankovních společnostech se čím dál častěji setkáváme se zneužíváním stimulačních tvrdých drog, především s pervitinem či kokainem. Kromě toho, že takový zaměstnanec zřejmě nepředvede nijak oslnivý výkon, je pravděpodobné, že v pozdějších etapách bude řešit také to, kde na svého koníčka vydělat. Ve své praxi jsem řešil případ mladé dámy, která považovala za svůj standard vykouřit o pracovních přestávkách cigaretu marihuany a pak se v klidu vrátit ke své práci. Zábavné na celém příběhu je fakt, že pracovala takříkajíc v první linii, na infolince poskytující prvotní informace klientům. Náslechy a bodové hodnocení nadřízených dokonce ukázaly, že po intoxikaci projevovala větší míru empatie a prodejních dovedností nežli před ní. Při pohovoru pak nebyla vůbec schopna pochopit, že se dopouští něčeho, co může být v rozporu se zákoníkem práce. Zdá se tedy, že společenská tolerance vytváří prostředí, kdy si řada zaměstnanců ani neuvědomuje, že se dopouští protiprávního jednání.

Sklony k patologickému hráčství žádná z prověrek velmi pravděpodobně neodhalí. Výjimku tvoří situace, kdy se potenciální uchazeč přizná k tomu, že byl léčen a vyléčen nebo, pokud toto skutečnost prozradí některý z bývalých spolupracovníků v rámci ověřování referencí v předchozím zaměstnání. Bohužel, na pracovním trhu však stále ještě často přežívá obava z toho, že pokud něco takového prozradím, vrhne to špatné světlo především na samotnou společnost. A tak i dnes dochází k tomu, že defraudant odchází z předchozích zaměstnání na dohodu a s příslibem dobrých referencí, výměnou za to, že neprozradí, že je firma zranitelná a zpronevěřené peníze „snad“ vrátí. V naší společnosti docházelo v minulosti k problémům především na značkových prodejnách, kde si někteří zaměstnanci „půjčovali“ hotové peníze z pokladny, přičemž v některých případech tyto peníze obratem mizely ve výherních hracích přístrojích. Jak to však bývá, automat nejenom, že peníze nevrátil, ale naopak dostával pravidelně peníze další, neboť cílem již nebylo nějaké peníze lehce vydělat, ale vrátit peníze chybějící v kase. Bohužel v letech 2008–2010 jsme zaregistrovali škody v celkové výši několika milionů korun a rovněž jsme inicializovali trestní stíhání u několika zaměstnanců. Po sérii masivních bezpečnostních opatření, které mimo jiné minimalizovaly objem hotovosti na prodejnách, došlo přesto v roce 2013 k bezpečnostnímu incidentu, kdy jeden z mladých zaměstnanců značkové prodejny odcizil více než 300 000 korun, přičemž skoro 200 000 korun prohrál za jediný večer a zbylé peníze se rozhodl utratit cestováním po Evropě. Poté hodlal spáchat sebevraždu. Naštěstí má tento příběh šťastný konec a mladý muž je stále na živu, byť je trestně stíhán a přišel o zaměstnání. Bohužel však platí, že pokud je zjištěn rozdíl v pokladnách a při bezpečnostním pohovoru s podezřelým se vyšetřovatel snaží zjistit motiv podvodného jednání, hráčství je dnes odpovědí ve více než polovině případů. Diskuzí s kolegy z jiných společností bylo bohužel zjištěno, že obdobná situace panuje i jinde.

Třetím problémem, který pravděpodobně žádná prověrka neodhalí, je tzv. slepá láska. A tak zatímco patologické hráčství je problémem spíše mužů, v tomto případě se setkáváme s převahou žen. Ve zkratce jde o to, že zaměstnanec se dopouští protiprávní činnosti, avšak nikoliv s cílem získat prospěch sám pro sebe, ale pro milovanou osobu. Tedy peníze či jiné výhody získávám

proto, že jsem hluboce, a především slepě zamilován a svému partnerovi bych přinesl, co mu na očích vidím. V bankovnictví je typickou situací schvalování úvěrů s vědomě nepravdivými údaji, v telekomunikacích se setkáváme se zneužíváním neveřejných nabídek či zneužíváním informací z telekomunikačního provozu. I v těchto případech je odhalení takového jednání spíše antickou tragédií, zvláště v situaci, kdy mezitím láska vyprchala a došlo k rozchodu. Přestože zaměstnanec je jednoznačným pachatelem, často v těchto situacích připomíná spíše oběť.

Otázka, která je nanejvýš naléhavá, zvláště v situacích, kdy většina protiprávního jednání je odhalena spíše na základě upozornění nežli vlastní činností interního auditora či interního vyšetřovatele, je, zda existují nějaké jasné znaky, které mohou upozornit na to, že se zaměstnanec dopouští protiprávního jednání. Samozřejmě, že jasné a průkazné znaky neexistují. Přesto však často pachatelé interní kriminality vykazují některé podobnosti, kterým bychom měli věnovat zvýšenou pozornost. Jaké to tedy jsou?

ZÁVĚR

Ať jsou to již závěry renomovaných poradenských společností, nebo zkušenosti bezpečnostních ředitelů v jednotlivých firmách, můžeme dnes s jistotou potvrdit, že za obří ztráty způsobené hospodářskou kriminalitou jsou z největší části odpovědni interní pachatelé, tedy zaměstnanci, často ve spojení s pachateli externími. Je proto až s podivem, jak málo pozornosti je ve společnostech věnováno nastupujícím zaměstnancům a jak moc jsou ignorovány některé rizikové prvky v chování zaměstnanců. Vezmeme-li v úvahu, že cena za takové prověření se pohybuje v rovině tisíců či maximálně desetitisíců korun na straně jedné, pak škody způsobené takovými zaměstnanci jsou bez výjimky vždy o několik řádů větší. Sebelepší monitorovací zařízení, mříže, ostraha či bezpečnostní politika nezabrání selhání člověka. Neboť ten je vždy nejslabším článkem bezpečnostního řetězu. Přeji vám při výběru zaměstnanců šťastnou ruku.

PROBLÉMOVÉ ZNAKY

VE SPOLEČNOSTI PRACUJE VÍCE NEŽ 5 LET A POŽÍVÁ VELKÉ DŮVĚRY

V 80 % případů, které jsem ve své praxi řešil, se jednalo o zaměstnance, kteří byli ve společnosti považováni za vysoce důvěryhodné a jejich pracovní poměr trval 5 a více let. Ovládali bravurně veškeré interní systémy a ovládali je tak, že často školili i své služebně mladší kolegy. Neváhali si brát práci navíc a byli svým okolím považováni za ty, kteří všechno vědí.

VE SPOLEČNOSTI PRACUJE DLOUHÁ LÉTA NA JEDNÉ POZICI/PRODEJNĚ APOD.

K tomu, aby zaměstnanec mohl skrytě páchat protiprávní jednání je kromě znalosti systémů nutné znát také ty správné lidi, zákazníky či dodavatele. Vzhledem k tomu, že páchání protiprávní činnosti se často děje tak, že spolu interní a externí pachatel úzce spolupracuje, je třeba, aby mezi sebou vytvořili určitou důvěru. Typicky problematickými pozicemi jsou tedy pozice nejrůznějších nákupčích, pokladních, vedoucích filiálek apod.

PRVNÍ PŘICHÁZÍ / POSLEDNÍ ODCHÁZÍ, PRACUJE I O DOVOLENÉ ČI SI DOVOLENOU TÉMĚŘ NEBERE

Úzce souvisí s předchozími znaky. Bohužel tento znak je často nadřízenými kvitován s povděkem a často je takový zaměstnanec dáván za příklad ostatním. V případě jednoho z největších podvodů v naší společnosti, kdy zaměstnanec uzavíral fiktivní účastnické smlouvy a odebíral dotované mobilní telefony, byl tento zaměstnanec proslulý tím, že běžně chodil pracovat i o víkendech. Těšil se takové přízni kolegů, že ti mu ochotně sdělovali svá přístupová hesla do systémů a nechávali jej vyřizovat některé vlastní obchodní případy. Případ mladého muže, o kterém jsem psal výše a který z pokladny společnosti odcizil 300 000 korun nesl právě znak toho, že na prodejnu se dostavil v mimopracovní dobu a byl zde zcela sám, takže v cestě k pokladnám mu nikdo nestál.

ŽIJE NÁKLADNÝM ŽIVOTNÍM STYLEM

Tento znak je velmi spekulativním, protože samotná skutečnost, že zaměstnanec má více peněz, než odpovídá jeho platu či mzdě, ještě nemusí vůbec nic znamenat. Varovné jsou spíše signály, kdy k takovému zbohatnutí dojde jakoby „náhle“. Již několikrát jsem měl možnost poslouchat historky o bohatém strýčkovi, vyhrání menšího obnosu v loterii nebo náhlém dědictví. Kolegům takového zaměstnance pak vůbec není podezřelé, že ten, který měl vždy hluboko do kapsy, je náhle pozorným hostitelem. Pokud sami mají z takového jednání profit, nikdy na takovéto jednání neupozorní.

ZTRÁTA MOTIVACE / POMSTA SPOLEČNOSTI

Zatímco v předchozích případech je cílem pachatele získat finanční profit či výhodu pro sebe nebo své blízké, v tomto případě je hlavním motivem snaha společnost poškodit. Získání profitu je následně racionalizováno slovy jako „stejně to dělá každý“, „když už byla ta příležitost“ apod. Zde je velmi důležité sledovat, zda se společnost, a to i nechtěně, nedopouští zjevných křivd, nejčastěji v oblasti nastavení mzdových podmínek, plánování směn a dalších.

Těchto pět znaků nemůže ani zdaleka pokrýt celou škálu znaků či indicií, které mohou svědčit o problémovém chování zaměstnance. Navíc sledovat tyto znaky není, a ani nemůže být úlohou auditora či vyšetřovatele, ale spíše úkolem manažerů na jednotlivých stupních řízení.

Tomáš Pluhařík
Manager
PricewaterhouseCoopers Audit s.r.o.

PROČ JE DŮLEŽITÉ MÍTI IT AUDITORA

Význam informační bezpečnosti v interním auditu ve světě nové legislativy

Současná geopolitická situace a kriminální hrozby nutí i konzervativní legislativce přijímat regulace a normy kladoucí na firmy i jednotlivce nové nároky a odpovědnosti. Informační bezpečnost tím začíná nabývat na reálném významu ve všech oblastech firemní a státní sféry. Ne že by tu nebyla již dávno, ale ruku na srdce, bývala často opomíjenou popelkou a otloukánkem rozpočtových škrtů. Důležité je, že se pomalu mění přístup, kdy je organizace zodpovědná pouze za svou IT infrastrukturu, na přístup, kdy je možné aplikovat zodpovědnost za škody způsobené zneužitím této infrastruktury (nebyla-li dostatečně zabezpečena). Aplikováno do běžného života, když váš neservisovaný plynový kotel zapálí kromě vašeho domu i ten sousedův, tak za to nesete odpovědnost – překvapivě v IT oblasti toto není zatím úplně běžné. Interní audit se tak čím dál častěji dostává do situace, kdy je konfrontován s politikami, které jsou natolik prorostlé s technologií, že jsou pro auditory neznalé IT obtížně zpracovatelné a pochopitelné.

NOVÁ LEGISLATIVA

Z pohledu Českého práva jsou úhelnými kameny problematiky (mimo zákonný rámec jednotlivých odvětví) zákon o kybernetické bezpečnosti (v platnosti bude od roku 2015) a poslední znění zákona o ochraně osobních údajů.

Zákon o kybernetické bezpečnosti (a jeho prováděcí vyhláška) zatím představuje menší hrozbu, protože současná kapacita NBU (respektive národního CERT týmu) a mírná forma sankcí nejsou pro klienty dostatečným motivátorem implementace zásadních změn. Většina tvůrců tohoto zákona, ale již dnes mluví o zpřísnění postihů v novele, která je připravována k projednání v roce 2015. Pro většinu odborné veřejnosti je tento zákon pouze prvním (a relativně měkkým) krokem ke komplexní normě pokrývající informační bezpečnost. Zákon se zatím dotýká pouze subjektů v tzv. kritické infrastruktuře státu a tzv. významných systémů. Jejich definice je bohužel stále poněkud vágní a bude upravována postupně prováděcí vyhláškou. Zatím je zřejmé, že se bude dotýkat hlavních utility provideru, telco firem, bank a některých státních institucí. Pro většinu subjektů je následující rok spíše rokem přípravným a pro ostatní inspirací, co je čeká do budoucna. S prohlubující se integrací IT infrastruktury ve všech oborech lidské činnosti je zřejmé, že pravidla navrhovaná zákonem budou ve střednědobém horizontu nějakým způsobem aplikována na všechny účastníky „informačního provozu“. Ideálním řešením je v rámci auditů již dnes zapojit IT auditory / IT security auditory, kteří dokáží poukázat na případné nedostatky a navrhnout vhodnou strategii/ roadmapu řešení. Stává se nám běžně, že vedlejším produktem takto koncipovaných auditů je i odhalení potenciálních fraudů a bezpečnostních rizik mimo IT.

Krátkodobě zásadnější je aplikace zákona o ochraně osobních údajů na informační systémy. Tento zákon totiž obsahuje mnohem tvrdší postihy a skryté velké riziko opomenutí povinností. Velké procento společností si je vědomo, jak s osobními údaji zacházet a jak je shromažďovat, avšak pouze na koncových (procesně viditelných systémech). V procesu/ infrastruktuře jsou pak často skrytá překladiště (mnohdy i mimo evidenci), která nebývají správně ošetřena, a představují tak zásadní riziko zneužití nebo ztráty citlivých osobních údajů. Dalším častým nešvarem je management přístupových práv a manipulace s daty, kdy na primárních úložištích jsou data spravována správně, ale na lokálních stanicích už jakákoliv ochrana chybí, a data jsou tak vystavena riziku odcizení nebo nežádoucí manipulace. Toto dokáže odhalit pouze důsledný IT auditor se schopností číst reálné IT procesy a vhodnými nástroji na sledování infrastruktury ve společnosti.

Do budoucna se domnívám, že vymáhání těchto zákonů povede k rozšíření poskytování informační bezpečnosti jako služby, protože pro menší subjekty může být naplnění litery zákonů finančně náročnou investicí. Obzvláště potřeba sestavení efektivních bezpečnostních týmů představuje pro menší subjekty personální zátěž (bez ohledu na problematickou dostupnost profesionálů v bezpečnostní oblasti).

PAPÍROVÍ TYGŘI

Neznalost IT/infosec problematiky (a nové legislativy) kombinovaná s tlakem zákazníka na nenarušování běžného provozu vede dnes někdy k IT auditům na papíře. Předkládané politiky jsou na papíře konfrontovány s vlastníky a účastníky těchto politik. Toto je sice pohodlné pro auditovaného, ale opomíjí jeden ze zásadních faktorů – lidskou schopnost improvizace (rád bych se vyhnul zobecňování, ale lenost zde hraje také svoji roli). Realita je vždy trochu odlišná od striktní papírové a je potřeba konfrontovat reálný provoz, nikoliv pouze jeho účastníky. Po důsledně provedeném IT auditu bývá sice někdy zákazník rozčarován, ale dobře navržená sada doporučení je mnohdy více než hodnotnou kompenzací. Pro naplnění nových požadavků legislativy a vnějšího světa už pouhé čtení a porovnávání nestačí.

Je prostě dobré firemní politiky číst, ale mluvit je potřeba s lidmi, kteří žijí každodenní praxí a audit provádět na této úrovni. Jakýkoliv jiný přístup vede k nepřesnému zobrazení reality a rizik. Toto zkreslení poté vytváří nebezpečnou iluzi klidu a bezpečí.

PROČ TEN NEGATIVNÍ TÓN?

Na závěr si dovolím objasnit mírně negativní tón, který může čtenář cítit z některých soudů výše. Základním problémem velké části subjektů v České republice je organicky budované IT, jehož strategií je nasytit požadavky zadavatele (businessu) a uchovat provoz v chodu. Většinou je však ignorováno jakékoliv strategické plánování a v posledních dekádách byla opomíjena i základní bezpečnostní pravidla. Změny, které přicházejí, však tyto nedostatky neodpouštějí, ať už se jedná o legislativu, nebo reálné bezpečnostní hrozby. Vnímejme toto jako velkou příležitost očistit IT prostředí od starých nešvarů a budovat poněkud koncepčnější a bezpečnější budoucnost.

General Data Protection Regulation (GDPR)
V nejbližších dvou letech bude zákonný rámec kolem ochrany dat ovlivňován novou direktivou EU. Cílem je pokrýt moderní trendy ve společnosti a nové technologie. Dále je také snaha problematiku zastřešit jednou právní normou. GDPR v podstatě nahradí legislativy jednotlivých států v oblasti ochrany osobních údajů a citlivých dat.

Igor Gricinko, MBA, CISA, C|EH
auditor IT
Komerční banka a.s.

FYZICKÁ A IT BEZPEČNOST: SPOLEČNĚ A NEROZDÍLNĚ?

Je to poněkud filozofická otázka. Fyzickou bezpečnost si lze poměrně snadno představit: vysoký plot, ostnatý drát, přísnou recepční nebo najatou agenturu. To vše proto, aby nám z firmy něco nezmizelo bez záznamu v účetnictví. „Půjčovat" si cizí věci je návyk starý jako lidstvo samo, proto kontroly v této oblasti nám jsou přirozené a každého manažera napadnou jako první.

S IT bezpečností je to o něco horší. Tu necháváme především na dobře placených odbornících. Investujeme do ní, aniž by byl viděn hmatatelný výstup. Firma kupuje hromadu techniky (firewally, proxy, systémy pro detekci průniků atd.) s cílem vybudovat bezpečnostní perimetr, ochránit vnitřní síť, uživatele a data před vetřelci.

Jak tyto dvě, na první pohled odlišné, oblasti spojit? Řekněme takto: různorodost kybernetických útoků dnešní doby již nutí bezpečnostní manažery uvažovat komplexně, tj. spojovat **fyzickou bezpečnost, IT bezpečnost** a ještě přidat **bezpečnost lidských zdrojů**.

V následujícím článku se pokusím ukázat, jak lze překonat IT bezpečnost i poměrně mohutně chráněné firmy a to pomocí „děr" na pomezí fyzické, IT a HR bezpečnosti.

V IT bezpečnosti je znám pojem „útoky na blízko". Jinak řečeno: útočník se fyzicky dostane ke své oběti. Proč jsou to nebezpečné situace a proč je úspěšnost takových útoků téměř 100%?

ZKUSME SI NAMODELOVAT 7 PŘÍKLADŮ:

1. **Přístup k aktivní relaci uživatele:** Necháte odemčenou obrazovku a odloučíte se na krátkou dobu např. na oběd, vyřídit telefon apod. Kolega vám vyfotí obrazovku pomocí Ctrl+PrintScrn, uloží výsledek do Malování, minimalizuje všechny okna a nastaví vám obrázek z Malování jako pozadí plochy. Po návratu nepoznáte rozdíl s tím, že vám žádné okno nepůjde zavřít, jelikož budete klikat na obrázek nikoli na aktivní okna. Celkem dobrý vtip, který je ale nutné chápat s odstupem. Při tomto útoku může kdokoli využít přihlášeného uživatele, jeho/její otevřené aplikace a provést cokoli ve vašem kontextu, např. převod finančních prostředků, ponížení evidence vozidel, ukončení stavebního spoření v cizí prospěch atd. Otázka zní: čí stopa zůstane auditorům a Policii v auditním logu? Přeci vaše.

2. **Nešifrovaný pevný disk:** Ponecháte svůj počítač v práci na delší dobu, např. přes noc. Vítané jsou soukromé notebooky. Kdokoli s přístupem k zařízení může udělat identickou bitovou kopii vašeho disku i s daty. Je to snadné: postačí USB disk s operačním systémem Linux, příkaz „dd" a nějaký vlastní disk na „odvoz" dat. Kdo nemá rád černé Linux obrazovky, může použít speciální programy, např. Acronis True Image. Útočník pak v klidu domova a s dostatkem času může „loupat perníček", tj. procházet vaše data, dešifrovat vaše hesla atd.

3. **Útoky na hesla:** Necháte počítač bez dozoru, ale zaheslovaný. Útočníkovi to nevadí, stačí jej vypnout a ukrást 3 soubory z vašeho pevného disku. Pokud používáte Windows, pak jsou to soubory SYSTEM, SAM, SOFTWARE, které jsou nejčastěji uložené v adresáři C:\WINSOWS\SYSTEM32\CONFIG\SAM. Útočník zapne počítač, nastartuje svůj Windows nebo Linux, připojí si váš disk a hotovo. Je to otázka 2 minut, ne více. Ukradené soubory obsahují veškerá hesla: jak lokálních uživatelů (nejčastěji Administrátora), tak i doménová (posledních 10 uživatelů, kteří se přihlásili na tomto počítači). Hesla jsou bohužel zakódována, což není překážkou. Na Internetu je množství manuálů a nástrojů jak je odkódovat. Při troše štěstí bude mít útočník hotovo od 2 minut do 24 hodin za cenu asi 30 USD.

4. **Instalace havěti:** Opět budeme uvažovat váš počítač v práci, který necháte chvilku odemčen a bez dozoru. Opět stačí 2 minuty a útočník Vám obohatí počítač o nějaký zábavný program. Dost často jsou to programy pro vzdálené ovládání neboli Remote Access Trojan (RAT). Máte přeci antivirus. To nevadí. Existují programy, které antivirus považuje za důvěryhodné (např. Virtual Network Computing), jehož účinky jsou devastující. Útočník na dálku může sledovat vaši obrazovku jako televizní program. Pokud nejsme i tak spokojení, trojské koně lze poměrně dobře maskovat změnou jejich bitového obsahu. Většina antivirových programů totiž pracuje na principu porovnávání signatur. Když změníte tělo viru, pak jej antivir nenajde. Je to jako když chřipkový virus mutuje a stará antivirotika na něj nezabírají.

5. **HW hračky:** Když už máte dobře chráněný vnitřek počítačové sítě, proč nezaútočit na počítač jako takový? Každý počítač má periférie, USB nebo starší konektor PS/2 pro klávesnici. K němu je připojena klávesnice, pomocí které musí každý z nás ráno zadat heslo. Ideální příležitost, nemyslíte? Povšimněte si obrázků níže, poznáte co je na nich divného?

USB keylogger.
Zdroj: *http://www.007spycamera.com*

PS/2 keylogger. Zdroj: *http://keyllama.com*

Taková zařízení jsou k mání do 2000 Kč, mají kapacitu až 2 GB a dokáží zaznamenat až 2 miliardy úhozů kláves. Nemáte je pod stolem i Vy?

6. **Útok na volně pohozený server:** Při provádění auditů jsem narazil i na případy, kdy řídící počítače (servery) byly umístěné ve veřejně přístupných prostorách. V takovém případě cíl je jasný. Dle popisků na serverech najít DC, neboli řadič domény. Lze jej na chvilku vypnout (služby by měl převzít sekundární nebo primární řadič) a provést:

- Vyzkoušet se přihlásit jako Administrátor heslem „Admin", „Administrátor" nebo prázdným. Pravděpodobnost je malá, nicméně není nulová.
- Off-line útok na hesla (viz bod 3) a zacílit na soubory NTDS.dit a SYSTEM. V těchto souborech je skryt poklad: hesla všech uživatelů domény. Dešifrování není zrovna jednoduché, nicméně je možné.
- Off-line útok na systémový účet, např. Off-line editací registru a záměnou spořiče obrazovky za příkazový interpretr cmd.exe. V případě úspěchu máte celou firmu.
- Linux systémy jsou rovněž zranitelné. Pokud se k serveru dostanete „na dostřel", pak útočník může off-line přidat uživatele do souboru /etc/passwd a přiřadit mu identifikátor „0". Výsledkem jsou administrátorská práva na doživotí, tj. dokud nebudete odhaleni při auditu lokálních uživatelů.

7. **„Veš v šatníku" neboli cizí zařízení v síti:** Když se podíváme pod stůl, tak alespoň já vidím nekonečná klubka kabelů, elektrické prodlužovačky apod. V takovém chaosu se snadno ztratí pár užitečných zařízení, např.

Pro realizaci všech výše uvedených scénářů je nutný fyzický přístup k zařízení či síťovým kabelům. **A to už není jen IT bezpečnost, ale bezpečnost fyzická.**

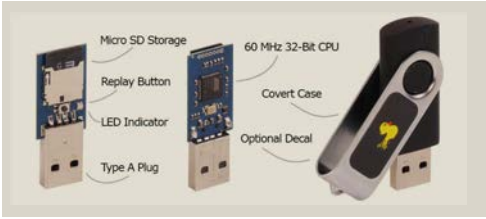
Obecně lze říci, že každý útok, má-li být účinný, začíná průzkumem terénu. Na základě výsledků takového průzkumu může útočník připravit „scénář na míru". Aktéři a pomocníci takového průzkumu jsou zaměstnanci jako takoví.

Jen oni zanechávají mnoho příležitostí a informací ke sběru, např.

- Vpuštění neznámých lidí na pracoviště pod jakoukoli záminkou (zapomenutá karta, schůzka s panem Novákem apod.)
- Pohození klasifikovaných dokumentů na pracovním stole
- Nevyzvednutí dokumentů z tiskárny
- Odpadkové koše (víte, že v roce 2000 si společnost Oracle najala agenturu, která třídila veškerý odpad od konkurenta společnosti Microsoft?)
- Telefonující kolega bez karty, kterému přidržíme dveře atd.

Každá z takových drobností může posloužit dalším kamínkem v mozaice; vytvořit obraz o síle (či slabosti) interních kontrol a posloužit k cílenému útoku.

Velkou kapitolou zůstává sociální inženýrství, aneb hacking bez počítačů. Techniky „jak oblbnout lidi" se dají efektivně použít i při průzkumu terénu. A nejen pro to. Uvedu opět příklad krásného USB zařízení.



USB počítač: *http://hakshop.myshopify.com/collections/usb-rubber-ducky/products/usb-rubber-ducky-deluxe#photo-3*
Cena: 39,99 USD

USB Rubber Ducky Deluxe stojí jen 40 USD, a je to plnohodnotný USB počítač, který lze naprogramovat pro cokoli. Může se například tvářit jako Human Interface Device (HID) a váš počítač si bude myslet, že jste připojili další klávesnici. Antivir rovněž nic neřekne. Kdo by kontroloval klávesnici na přítomnost virů? Místo toho tato „kachnička" něco provede, např. spustí krásnou prezentaci o zvířátkách nebo něco podobného chytlavého. Ideální je, pokud si co nejvíce zaměstnanců toto zařízení půjčí a obejdou s ním co nejvíce firemních a domácích počítačů.

A co poslední článek *„bezpečnost lidských zdrojů"*? Praxe ukazuje, že za nejvíce zákeřnými útoky stojí interní zaměstnanec. Když něco potřebujete od konkurence, proč se k nim nenechat najmout jako IT pracovník, uklízečka nebo asistentka? Znám jen hrstku firem, které provádějí tzv. background scanning/checking, tj. nezávislé a objektivní prověřování minulosti uchazeče o zaměstnání, samozřejmě s jeho souhlasem. Na českém trhu již existuje řada agentur, které takové auditní služby nabízí. Není to levné, ale dle mého se to u klíčových pozic vyplatí.

Napájecí „adaptér": https://www.pwnieexpress.com/product/pwn-plug-elite/
Cena: 695 USD

Podstatou těchto zařízení je působit tak, jako kdyby byly legitimní součásti vaší firemní sítě a obyčejný uživatel by si je nedovolil odpojit. Dobrým maskováním je napájecí adaptér, kterých pod stolem máme desítku. Ve skutečnosti je to mini-počítač, který je napájen přímo ze zásuvky. Je připojen na vaší vnitřní podnikovou síť a má v sobě 3G, Bluetooth a WiFi adaptér. Je to nejnebezpečnější a nejméně nápadný nepřítel, jelikož pomocí 3G mobilní sítě je neustále připojen na Internet a čeká na povely útočníka, které provede přímo ve vaší „bezpečné" síti. Ekonomickým pohledem se vaše investice do bezpečnostního perimetru v tomto okamžiku se staly nulovými. Veškeré firewally, proxy o samotná fyzická ochrana přestaly účinkovat, protože malý „napájecí adaptér" provedl by-pass, tj. vytvořil díru (nebo chcete-li tunel) od vás směrem do Číny, Ruska apod.

Pasivní odposlech sítě:
zdroj: http://hakshop.myshopify.com/products/throwing-star-lan-tap-pro#photo-3
Cena: 39,99 USD

Druhá černá krabička slouží pro pasivní odposlech síťové komunikace. Vypadá jako prodlužovací kabel, který spojuje více kabelů mezi sebou. Účel je podobný jako v bodě 5, zaznamenat vše, co se děje okolo.

Nemusíte potom mít strach, že Vám zaměstnanec před koncem zkušební doby „vynese“ celou firmu a nechá vám navíc na památku bílý napájecí adaptér v zásuvce pod stolem.

Abych nekřivdil jen zaměstnancům. Zkuste se podívat na chodby vaší firmy. Myslím, že roli „volavky“ by si mohl klidně zahrát i nějaký dodavatel, pracovník podpory IT, údržbář v pracovním oděvu atd. Speciálním případem jsou uklízečky. Myslím, že jsou ideálním kandidátem na spolupracovníka hackerů.

Uklízečky:

- Nejsou zrovna dobře placené
- Mají klíče od celé firmy
- Pracují v noci nebo brzy ráno, kdy mají „klid na práci“
- Jsou většinou zaměstnanci agentur, a tak se hůře evidují, sledují apod.

Představil jsem jen výňatek z palety rizik, kdy fyzická a IT bezpečnost jdou ruka v ruce. Jak tedy kontroly proti těmto rizikům auditovat?

Rozhodně bych se nebál vyhradit 10–15 MD z rozpočtu auditní mise na provedení penetračních testů fyzické bezpečnosti. Ideálně do týmu testeru zahrnout IT auditora, který by mohl posoudit dopady zjištěných nedostatků na IT bezpečnost. Takový druh auditu je dobré opakovat každý rok tak, aby se daly výsledky meziročně srovnat.

Dobré je připravit komplexní auditní testy, které by obsahovaly prvky sociálního inženýrství, útoků na IT, ověřování pozornosti a všímavosti zaměstnanců, uplatňování pravidel čistého stolu apod. Příkladem mohou posloužit tyto scénáře:

- Tester pod legendou návštěvy vstupuje do prostor. Dokumentuje okolí pomocí fotoaparátu/mobilního telefonu, pod různými záminkami se snaží dostat do chráněných prostor.
- Tester pod legendou schůzky s panem/paní XX prochází prostory a neustále hledá onu zasedací místnost. Při té příležitosti vstupuje i do chráněných prostor a sbírá pohozené papíry ze stolů, tiskáren apod.

Tester by mohl zanechávat na místě samolepky, USB zařízení apod. vše záleží na fantazii a reakci okolí.

„Každý útok, má-li být účinný, začíná průzkumem terénu“

Takové auditní metody mohou být pro někoho kontroverzní, nicméně si myslím, že jsou nesmírně účinné. Za minimum auditního času objektivně ověříte maximum kontrol. Navíc pozorujete reakce zaměstnanců přímo v terénu. Lze tedy dávat cílená a účinná doporučení na závěr. Navíc se kontroverze vryje do paměti všech a udržuje tím potřebné bezpečnostní povědomí.

„Různorodost kybernetických útoků dnešní doby již nutí bezpečnostní manažery uvažovat komplexně“

„Dobré je připravit komplexní auditní testy, které by obsahovaly prvky sociálního inženýrství, útoků na IT, ověřování pozornosti a všímavosti zaměstnanců, uplatňování pravidel čistého stolu“

Igor Gricinko, MBA, CISA, C|EH
Je absolventem Escuela Superior de Marketing y Administración a držitelem certifikaci „Certified Information Systems Auditor“ a „Certified Ethical Hacker“. Pracuje více jak 15 let v IT oborech, z toho 6 let jako auditor IT v Komerční bance. Je odpovědný za provádění IT auditů v 9 zemích a 30 společnostech Société Générale. Věnuje se zejména bezpečnosti informačních a komunikačních systémů, řízení IT rizik a problematice Basel AMA.

Ing. Lukáš Wagenknecht
1. náměstek Ministra financí ČR

NOVÝ ZÁKON O VNITŘNÍM ŘÍZENÍ A KONTROLE

Ministerstvo financí v současnosti finišuje poslední úpravy předběžného návrhu zákona o vnitřním řízení a kontrole. Paragrafované znění návrhu zákona bude poté poskytnuto k diskuzi veřejnosti. Ačkoliv se ještě diskutuje nad parametry jednotlivých ustanovení návrhu, principy nové právní úpravy se již jasně rýsují.

Návrh zákona vytváří ucelený rámec pro efektivní fungování veřejné správy. Obsahuje nástroje moderního řízení – například podrobnější pravidla pro řízení rizik nebo pravidla pro hodnocení projektů, které poskytnou managementu ujištění o přínosech projektů pro daňové poplatníky a o reálnosti vytyčených záměrů. Národní veřejné prostředky budou požívat stejné ochrany jako ty zahraniční.

Norma také zásadně mění kontrolní prostředí ve veřejné správě a přibližuje ho vyspělým demokraciím. V současnosti jsou zejména obce zatěžovány spoustou kontrol, které mnohdy ověřují tu samou věc. Návrh zákona ruší nadbytečné kontroly a zjednodušuje kontrolní systém. Zodpovědnost za řízení a kontrolu veřejných prostředků mají především entity, kterým jsou tyto prostředky přiděleny. V rámci vnitřního kontrolního prostředí nová právní úprava stanoví jasné rozdělení zodpovědností. Vedení již nebude moci svalit zodpovědnost za konkrétní operaci na řadového úředníka a „umýt si ruce“ nad řádným finančním řízením. Za to v souladu s novými pravidly plně zodpovídá schvalující osoba (nejvyšší úředník – představitel entity). Ta také společně se schvalujícím orgánem (orgán zodpovědný za hospodaření podle schváleného rozpočtu) zodpovídá za nastavení a fungování vnitřního kontrolního systému. Posiluje se nezávislost interního auditu, a to zejména zřízením výborů pro audit, nezávislých na správcích veřejných rozpočtů, u kterých budou zřízeny. Členy výborů pro audit budou osobnosti z akademické, neziskové nebo komerční sféry uznávané v některé z oblastí vnitřního kontrolního systému. Důraz bude kladen na jednotná pravidla a metodologii pro výkon ověřování, která umožní používání a sdílení výsledků ověřování. Interní audit bude ze zákona podléhat ověření kvality.

Finanční úřady mají vybírat daně. Návrh zákona ruší evropskou raritu, kdy se finanční úřady podílely i na kontrole veřejných výdajů. Asi nepřekvapí, že tato (daňová) kontrola mnohdy docházela k rozdílným závěrům než ostatní kontrolní orgány. Návrh zákona ruší tyto kontroly a umožňuje pracovníkům finančních úřadů věnovat se tomu, na co jsou experty – tedy na zajištění financí pro fungování veřejné správy. Tímto přeskupením dojde ke snížení nákladů na kontroly a zároveň umožní finančním úřadům se více zaměřit například na boj s daňovými úniky.

Návrh zákona v rámci posílení boje proti korupci nastavuje pravidla pro prevenci střetu zájmu v oblasti hospodaření s veřejnými prostředky. Stanoví také neslučitelnost některých funkcí v systému kontroly s funkcemi v politických stranách. Zamezuje tak nežádoucím politickým tlakům při kontrole veřejných prostředků.

Zákon stanoví požadavky na kvalifikaci úředníků, kteří hospodaří s veřejnými prostředky. O veřejných penězích tak budou rozhodovat úředníci, kteří prokázali, že mají k vykonávaným činnostem patřičné kompetence.

Ministerstvo financí vítá nadcházející veřejnou diskuzi, která může přispět ke zlepšení kvality navrhovaného předpisu, jehož přijetím dojde ke splnění závazků, které jsme v oblasti kontroly na sebe vzali ještě před vstupem do Evropské unie a které doteď nebyly řádně dodržovány. ▲

> „Návrh zákona ruší nadbytečné kontroly a zjednodušuje kontrolní systémy. Zamezuje tak nežádoucím politickým tlakům při kontrole veřejných prostředků“

Ing. Andrea Káňová, CIA, CGAP
kanova.andrea@gmail.com

ČEHO SI ANDREA POVŠIMLA

a neb CO SE DĚJE NA MEZINÁRODNÍ SCÉNĚ

▲ *Jako událost číslo jedna je snad na místě zmínit chystaný podpis nové rámcové smlouvy mezi Mezinárodním institutem interních auditorů a jednotlivými instituty ve světě. Tato nová rámcová smlouva má nahradit několik oddělených smluv, které se doposud pro úpravu vztahů mezi IIA a instituty používaly. Příprava nového textu smlouvy byla časově náročná a byly zohledňovány mnohé připomínky. Do tohoto procesu vstoupil aktivně také Český institut interních auditorů, který se především snažil prosadit to, aby dále zůstal tzv. administrujícím centrem pro skládání zkoušek Certifikovaný interní auditor a jiných, což se podařilo. Podpis nové smlouvy je plánovaný na prosinec tohoto roku.*

▲ *Zkouška CGAP – Certifikovaný auditor ve veřejné správě by se od ledna 2016 měla dočkat své revidované verze. V současné době probíhá její příprava, která navazuje na průzkum prováděný Mezinárodním institutem interních auditorů. Aktualizovaná verze této zkoušky by tak měla lépe odrážet reálné požadavky kladené na auditory v tomto sektoru.*

▲ *Měli jste někdy provést hodnocení vnitřního řídicího a kontrolního systému a nevěděli jste jak na to? Pak by pro vás mohlo být užitečné přečíst si novou publikaci na toto téma. Ke stažení je na této webové adrese: http://www.theiia.org/bookstore/product/evaluating-internal-contol-systems-download-pdf-1810.cfm*

▲ *Další užitečné informace, tentokrát na téma hodnocení kvality interního auditu, můžete načerpat z mezinárodního průzkumu provedeného Francouzským institutem interních auditorů. Zprávu z tohoto průzkumu si můžete stáhnout na následující webové adrese: http://www.theiia.org/bookstore/product/the-value-of-quality-assurance-and-improvement-programs-a-global-perspective-1821.cfm*

▲ *Pochybovali jste někdy o tom, že jste dobrým interním auditorem a jestli se do této profese skutečně hodíte? Richard Chambers ve svém blogu zmiňuje pět znaků, které byste měli mít, abyste v této profesi byli úspěšní:*
- *Umíte kriticky přemýšlet*
- *Jste přirozeně zvědaví a skeptičtí*
- *Snadno si vytváříte dobré mezilidské vztahy a dokážete je udržet*
- *Rádi prosazujete změnu a zlepšení*
- *Jste dobrými „spisovateli" – umíte dobře sdělovat informace v písemné formě*

Více na webové adrese: https://iaonline.theiia.org/5-sure-signs-you-are-well-suited-for-a-career-in-internal-auditing

CBOK 2015

Mezinárodní institut interních auditorů (The IIA) zahájil přípravy studie **Celosvětově sdíleného souboru znalostí interního auditu, tzv. CBOK 2015** (Common Body of Knowledge), který je ústředním bodem pokračujícího výzkumného úsilí, jež provádí Nadace pro výzkum Mezinárodního institutu interních auditorů (The IIA Research Foundation – IIARF).
CBOK poskytuje hodnotné informace o tom, jak se interní audit ve světě provádí a jak je nahlížen.

Tato studie je pro své rozsáhlé dotazování profesionálů z celého světa všeobecně uznávaná. Celkově se průzkumu z roku 2010 zúčastnilo více než třináct a půl tisíce interních auditorů ze sto sedmi zemí světa, čímž se stal největším průzkumem interních auditorů ve světě. *Ještě větší odezva je očekávána v roce 2015.*
IIARF Centrum na stránkách The IIA – **www.globaliia.org** poskytuje aktuální informace týkající se CBOKu 2015.

Průzkum bude spuštěn **v únoru 2015**. Pouhými 30–60 minutami svého času trvale přispějete své profesi. Průzkum si můžete v případě potřeby uložit a dokončit později. Vaše odpovědi budou spojeny s odpověďmi vašich kolegů z celého světa a na jejich základě bude vytvořeno několik praktických zpráv mapujících témata, která se objevují v rámci celé profese, včetně:
– trendů v ujištění řízení rizik,
– nejdůležitějších schopností interního auditora,
– dopadů rizik informačních technologií.
Průzkum bude připraven jak pro stávající, tak penzionované interní auditory z celého světa, včetně partnerů a zaměstnanců organizací poskytující služby interního auditu a akademických profesionálů, kteří vyučují nebo vedou výzkumy témat, jež jsou s profesí interního auditu spojeny.
Bude zcela anonymní, žádná z vašich odpovědí nebude spojena se žádným osobním údajem.
Dotazník bude dostupný ve více než dvaceti jazycích.
Český institut interních auditorů zajistil český překlad. Členové ČIIA obdrží pozvánku a dotazník, jakmile bude k dispozici.

Výsledky budou zveřejňovány v pravidelných intervalech online na stránkách IIARF Centra výstupů CBOK. Zpráva, která bude vypracována jako výstup z obsahu studie, bude všem členům IIA k dispozici k bezplatnému stáhnutí.
Český institut interních auditorů bude zveřejňovat aktuální informace na svých webových stránkách.

Využijte i VY příležitosti stát se součástí největší a nejobsáhlejší studie profese interního auditu!

ŘÍZENÍ ÚTVARU INTERNÍHO AUDITU

TERMÍN
29.–31. října 2014

ČÍSLO
51. běh

OD–DO
09.00–16.00 hodin

MÍSTO KONÁNÍ
Český institut interních auditorů,
Karlovo nám. 3, Praha 2, 1. patro

KONTAKT
e-mail: sindelarova@interniaudit.cz
telefon: 224 920 332
www.interniaudit.cz

STORNO PODMÍNKY
www.interniaudit.cz/profesni-vzdelavani/seminare/

NOVINKA

CENA
člen ČIIA
3 800 Kč
(s DPH 4 598)

nečlen ČIIA
4 200 Kč
(s DPH 5 082)

URČENO PRO

Pro zkušené interní auditory, řídící a vedoucí pracovníky (malých i velkých) útvarů interního auditu, metodiky pro auditní činnost, auditory i experty připravující se na nezávislou validaci interního hodnocení a další, kteří se zajímají o problematiku interního auditu ve VS a mají k tématu co říct. Vítáni jsou také ti, kteří pociťují určitou vnitřní nespokojenost, vnímají potenciální rezervy a chtějí se v řízení činnosti interního auditu posunout, příp. slyšet praxi jiných útvarů.

Atestační kurz je zařazen v systému odborné certifikace na úrovni – Interní auditor ve veřejné správě – expert/konzultant.

CÍL SEMINÁŘE

Hlavním cílem kurzu je prosazení systematického přístupu k řízení interního auditu v subjektech veřejné správy, se zvláštním zaměřením na osoby přímo zapojené do řídícího procesu (vedoucí interního auditu či „samostatné“ auditory). Seznamuje účastníky s možnostmi a postupy pro řízení a zlepšování služby interního auditu s přihlédnutím k velikosti „útvarů interního auditu“ (odlišnosti malých a velkých organizačních jednotek), a to interaktivní formou pod vedením lektorů se zkušenostmi v jejich prosazování.

Pokusíme se odpovědět na otázky:

- Jak jsme/jste „daleko“ v profesní praxi a kudy dál?
- Můžeme/můžete a sneseme/snesete srovnání se srovnatelnými typy útvarů?
- Jsme/jste připraveni na validaci?
- Je kvalifikace, praxe a zkušenost interního auditora přenositelná?
- Můžeme/musíme si pomáhat?

Struktura kurzu je plánována interaktivní formou s řadou případových studií (ukázek lepších i horších konkrétních příkladů z auditní praxe – auditních zpráv, ročních zpráv, programů kvality, reportovacích nástrojů…). Předpokládá se optimálně aktivní přístup účastníků, ochota přispět k diskuzi vlastními zkušenostmi a názory.

PROGRAM

1. den
Požadavky na řízení interního auditu
Plánování interního auditu
Zpráva z interního auditu

2. den
Reporting a komunikace
Program kvality IA – teorie a případová studie

3. den
Případová studie – řízení malého útvaru IA
Případová studie – řízení velkého útvaru IA
Podpora výkonu praxe interního auditu ze strany MF a profesních sdružení
Test

LEKTOŘI

Mgr. Stanislav Klika, Ministerstvo financí; **Mgr. Jana Kranecová,** Ministerstvo financí; **Ing. Martin Trojan, CIA,** Centrum pro regionální rozvoj ČR; **Ing. Jiří Novák,** Čepro; **Ing. Blanka Štefanková,** Krajský úřad Moravskoslezského kraje, **Ing. Ivana Göttingerová,** Magistrát města Brna; **Ing. Daniel Häusler,** ČIIA

Ivana Krůželová
Expert v oblasti kohezní politiky působící v Londýně, Velká Británie

VELKÁ EVROPSKÁ RUKA TĚ ŠKRÁBE NA ZÁDECH

Kdo má rád dobré a temné detektivky (například ty severské), určitě by neměl vynechat obecné nařízení pro programové období 2014–2020. Nepochybně bude mít u nejednoho paragrafu stejný pocit, jako když čte Stiega Larssona, „no tohle už snad nemůže být pravda, a kdybych tohle nevěděl, implementovalo by se mi mnohem líp“.

Po dekádách, kdy se pod záminkami rozšíření EU o země nespolehlivé, nezauditovatelné a peníze všelijak neřiditelné Evropská komise rozhodla sypat jedno finanční a kontrolní opatření za druhým, přistoupila navíc k něčemu natolik troufalému, jako je vstup do samotné ekonomiky a řízení financí daného státu. Otázka je, kdo tyhle paragrafy čte. Může se také stát, že až přijde na účtování předvolebních slibů a sejde se kolize nesplněných přání o vybraných daních a všemocných fondech, kterými zalepíme deficit státního rozpočtu, bude probuzení o to zajímavější.

Aktuální Obecné Nařízení 1303/2013 nemá obsah, tematicky se paragrafy opakují, takže si velmi těžko označíte jednotlivé implementační sekce, v podstatě se to celé musíte naučit nazpaměť a hororové paragrafy očekávat na každé stránce.

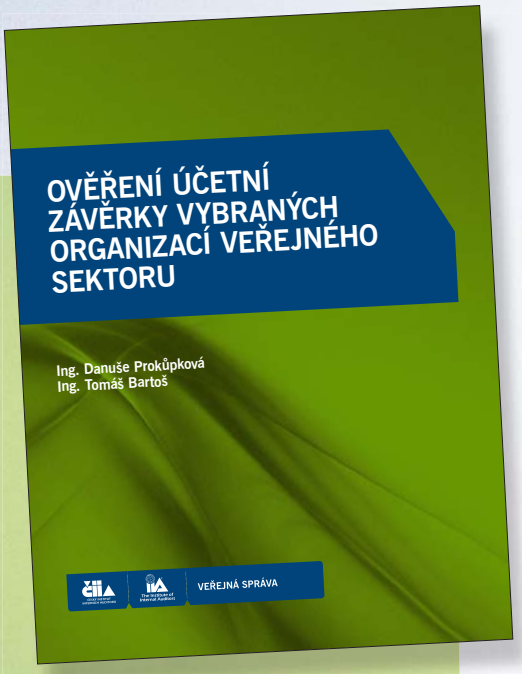
V jednom z předchozích článků jsme zmínili implementační nástroje, které ve své podstatě znamenají nastavení programu v programu, zvláště v případě, že EK doporučí některé zprostředkující subjekty, nebo naopak v rámci členského státu budou jednotlivé subjekty na statutu prostředkujících subjektů trvat. (Ve finále tak můžeme hovořit až o desítkách zprostředkujících subjektů v podobě měst, svazků obcí a podobně, u jedné priority.) K tomuto novému nastavení se například váže zajímavý článek 13, ve kterém EK avizuje přípravu návodu na to, jak přistupovat k příjemcům, jaké volit nástroje, jaké subjekty a tak dále. Znovu se tu, oproti předchozím obdobím, posouváme ve směru autority EK do oblasti implementace fondů, která by měla být v kompetenci členského státu. Ale to je pořád ještě patálie POUZE implementační.

Výrazně zajímavější v tomto ohledu jsou články, kde si EK stanovuje pravomoc pozastavit čerpání programů, vyvolat změny textů operačních programů či samotné Partnerské dohody. Například na základě článku 19 může EK pozastavit platby, pokud dojde k závěru, že předběžné podmínky nejsou dostatečně naplněny. A to, že se tyto podmínky týkají mnohem širších oblastí, než je čerpání fondů, už víme. Stejně tak tomu může být i u selhání implementace výkonnostní rezervy nebo naplnění povinných indikátorů.

Avšak úplně „nejbrutálnější“ je článek 23, který se vztahuje k efektivnímu řízení ekonomiky a státního rozpočtu, deficitu a tak dále. Prostřednictvím poskytnutí prostředků na ekonomický rozvoj, kterými fondy ESIF jsou, opravňuje se EK evokovat změny operačních programů, implikovat finanční korekce a pozastavit čerpání programů v rozmezí 50 až 100 % v případech, kdy shledá, že členský stát na tom s řízením ekonomiky („náprava makro-ekonomické rovnováhy“) a deficitem rozpočtu není tak dobře, jak se zdá, a hlavně nereaguje na podněty Evropské komise k nápravě. (Reagovat musí členský stát do dvou měsíců, s návrhy opatření, což je snový termín, pokud posílá nějaký požadavek členský stát EK.) Dobré na tom je (?), že při takovém pozastavování EK přihlédne k hospodářství daného členského státu (nějak). Další dobrá věc na tom je, že jsou v tom členské státy namočené všechny stejně, AŽ (a zase ten Cameron) na Velkou Británii, která je vyjmuta z aplikace bodů 6–12 hrůzného paragrafu 23, což souvisí s urputností nepodepsat fiskální dohodu.

> „Aktuální Obecné Nařízení 1303/2013 nemá obsah, tematicky se paragrafy opakují, takže si velmi těžko označíte jednotlivé implementační sekce, v podstatě se to celé musíte naučit nazpaměť a hororové paragrafy očekávat na každé stránce“

Všichni s tím nakonec nějak souhlasili, takže takový horor to zase být nemůže. Ale možná by bylo dobré okopírovat ta nejděsivější opatření pro pana premiéra, aby je měl k ruce. Pro jistotu. Kdyby náhodou.



OVĚŘENÍ ÚČETNÍ ZÁVĚRKY VYBRANÝCH ORGANIZACÍ VEŘEJNÉHO SEKTORU

Odborná publikace je zaměřená na popis celého procesu ověření účetnictví a účetní závěrky vybraných jednotek v rámci veřejných rozpočtů počínaje úvodním šetřením až po vydání zprávy ověřovatele a vyhodnocování následných událostí o případných rizicích, která ovlivňují budoucí finanční situaci účetní jednotky.

Příručka vznikla jako reakce na okamžitou potřebu a pro spolehlivější orientaci v daném předmětu činnosti. Cílem příručky je popsat postupy při ověřování, maximalizovat univerzálnost popisovaných principů a postupů, vytvořit základní metodiku pro provádění nejen ověření účetní závěrky těchto vybraných organizací v souvislosti s novými požadavky, zvýšit srozumitelnost dosud uplatňovaných postupů a maximalizovat univerzálnost popisovaných principů.

Příručka je vhodná jak pro interní auditory, tak i pro širší odbornou veřejnost.

Autoři:

Ing. Danuše Prokůpková – Vystudovala VŠE v Praze. Má bohatou praxi jako finanční analytik. Nyní se věnuje auditorské a poradenské činnosti (oprávnění Komory auditorů ČR, členka Výboru Komory auditorů ČR pro veřejné finance). Působí také jako lektor a má za sebou bohatou publikační činnost.

Ing. Tomáš Bartoš – Vystudoval VŠE v Praze. Podnikovou praxi realizoval ve finančních oblastech. Od roku 1994 se plně věnuje auditorské a poradenské činnosti (oprávnění Komory auditorů ČR; člen Výboru Komory auditorů ČR pro veřejné finance). Působí i jako lektor.

„Publikace je velmi hezkým příkladem studijního textu, který vyžaduje od čtenáře aktivní přístup. Dá se použít ke studiu vybraných záležitostí, dá se použít jako „úvod do studia“ určité problematiky, dá se ale použít i jako ucelený, komplexní, srozumitelný a logický návod, jak profesionálně, v souladu s mezinárodně uznávanou praxí i legislativou, ověřit účetní závěrku.“

Ing. Eva Janoušková,
předsedkyně Komise pro primární systém dohledu
ve Výboru Sekce veřejné správy při Českém institutu interních auditorů
a zástupkyně ředitele Krajského úřadu Kraje Vysočina

„Předložená příručka je zpracovaná v souladu s platným legislativním rámcem a reflektuje i budoucí potřeby.
Publikace je svým obsahem a zaměřením ojedinělá také tím, že vyplňuje mezeru, která dosud mezi odbornými publikacemi pro širší odbornou veřejnost, chyběla. Je to dobrý „odrazový můstek“ pro další kroky při zavádění integrovaného řízení a kontroly za účelem potřebné emancipace strategického i taktického řízení i v této sféře veřejných financí.“

Ing. Luděk Gulázsi
ředitel odboru Kontrola Ministerstva financí ČR

Ing. Petr Hadrava, ACCA, CIA, CISA
Interní auditor, MetLife pojišťovna a.s.

OHLÉDNUTÍ ZA MEZINÁRODNÍ KONFERENCÍ INSTITUTU INTERNÍCH AUDITORŮ V LONDÝNĚ

Mezinárodní konference Institutu interních auditorů se tento rok konala v Londýně, a to ve dnech 6.–9. července 2014. Její název byl: „TIME TO MAKE THE CONNECTION".

Konference se zúčastnilo přes 2300 delegátů z více než 100 zemí. Jednalo se o společenskou vzdělávací událost, kde se nám podařilo získat mnoho nových zajímavých kontaktů, vyměnili jsme si zkušenosti s kolegy auditory z celého světa a měli možnost účastnit se přednášek vedených odborníky z různých oborů.

Konference se konala v ExCeL London Exhibition and Conference Centre nedaleko centra Londýna. Tato lokalita byla velice dobře dostupná odkudkoli a spojení s letištěm bylo jednoduché i bez použití poměrně drahých taxi. V okolí konferenčního centra byl na výběr nespočet ubytovacích možností. Delegáti si mohli vybrat i ubytování na okraji Londýna a velice pohodlně se pomocí metra a povrchové vlakové dopravy DLR dostat za pár minut na místo konference.

Tato konference Institutu interních auditorů s pořadovým číslem 73 byla zahájena stylově, a to skupinou **Counterfeit Beatles**.

Poté přednesla delegátům pozdrav Jeho královská Výsost princ z Walesu, Charles. Rozhovořil se na téma *Sustainable business – and internal audit's role in promoting this.* Bylo to sice ze záznamu, ale zážitek to byl přesto silný. Princ Charles se dlouhodobě věnuje roli businessu ve společnosti a zkoumá dopady na prostředí a společnost. Věří tomu, že interní audit má potenciál hrát zásadní roli při identifikaci a řešení tzv. sustainability risks, které mohou mít zásadní dopad do dlouhodobého přežití společností.

Následovalo přivítání, které přednesl Paul Sobel, globální předseda Institutu interních auditorů, a **Nicola Rimmer**, ředitelka celé konference. Oba stručně představili program konference, který byl skutečně bohatý.

Kromě 6 tzv. General Sessions, kterých se mohli účastnit všichni delegáti, jsme si mohli vybrat z více než 60 tzv. Concurrent Sessions. To bylo vždy několik přednášek na různá témata v jeden okamžik a delegáti si vybírali, které se zúčastní.

První General Session nastavila laťku skutečně vysoko. Její název byl *Adapting to the Pace of Change.* Přednášejícím byl **Alastair Campbell**, po 10 let blízký spolupracovník, ředitel komunikace a mluvčí Tonyho Blaira, dřívějšího britského ministerského předsedy.

Další zajímavá přednáška měla název *Leading Multi-cultural Internal Audit Functions*, kde se **Naohiro Mouri**, generální ředitel, senior vicepresident a hlavní auditor MetLife v Japonsku, účastnil panelové diskuze na téma vedení různorodých auditních teamů, rizika, benefity a výzvy spojené s vedením multikulturních teamů. Diskuzi moderoval IIA president a CEO Richard Chambers a zúčastnili se Clare Brady, ředitelka interního auditu Mezinárodního měnového fondu, a Hans Winters, hlavní auditor v Siemens AG.

Mimořádný zážitek pro mě znamenala přednáška od **Michaela Woodforda** s názvem *The Power of the Whistle*. Michael je dřívější prezident a CEO Olympus Corporation, se sídlem v Japonsku. Byl propuštěn poté, co upozornil na účetní podvod ve výši 2 miliardy USD. Michael se podělil s delegáty o události, které vedly k odhalení tohoto podvodu, a je vzorem díky své osobní statečnosti. Je držitelem několika ocenění a vyznamenání. Celý případ shrnuje ve své knize Exposure: Inside the Olympus Scandal: How I Went from CEO to Whistleblower.

Noreena Hertz, která je popisována jako jedna z nejvýznamnějších současných myslitelů mladé generace, autorka a profesorka na University College v Londýně měla přednášku s názvem *How to Make Smart Decisions in a Complex World.* Během přednášky Noreena shrnula typické rozhodovací

strategie a úskalí, která jsou s nimi spojena. Z vědeckého pohledu popsala, proč a jak děláme rozhodnutí a jakým způsobem zlepšit rozhodovací proces. Noreena je vyhledávanou komentátorkou v televizi, rádiu a je poradkyní v oblasti strategických rozhodnutí nejvýznamnějším světovým CEOs v oblasti ekonomie, geopolitiky a obchodu.

Keith K. Heywood, Talent Development Executive, Keith Inspires, Zimbabwe, zaujal svojí přednáškou *New Business, New Value.* Keith popsal měnící se podmínky a hodnoty a dopady vývoje na činnost interního auditu, nastínil, kudy se musí interní audit vydat, aby byl stále platným partnerem pro management a popsal nové dovednosti auditora k maximalizaci přidané hodnoty pro společnost. Zmínil, že tzv. „business as usual" je minulostí a že nic takového již neexistuje.

Interní auditoři musí přizpůsobit svůj přístup tomuto rychlému vývoji, aby byli i v dnešní době stále platnými a relevantními.

Globální předseda Institutu interních auditorů **Paul Sobel** dělal rozhovor s **Mervynem Kingem** na téma *How Non-financial Reporting Is Changing the Role of Internal Audit.* King působí jako emeritní předseda Global Reporting Initiative a je znám jako předseda tzv. King Committee v Jižní Africe. Jako speciální host se připojil John Lelliott, finanční ředitel The Crown Estate. To byl stručně obsah General Sessions.

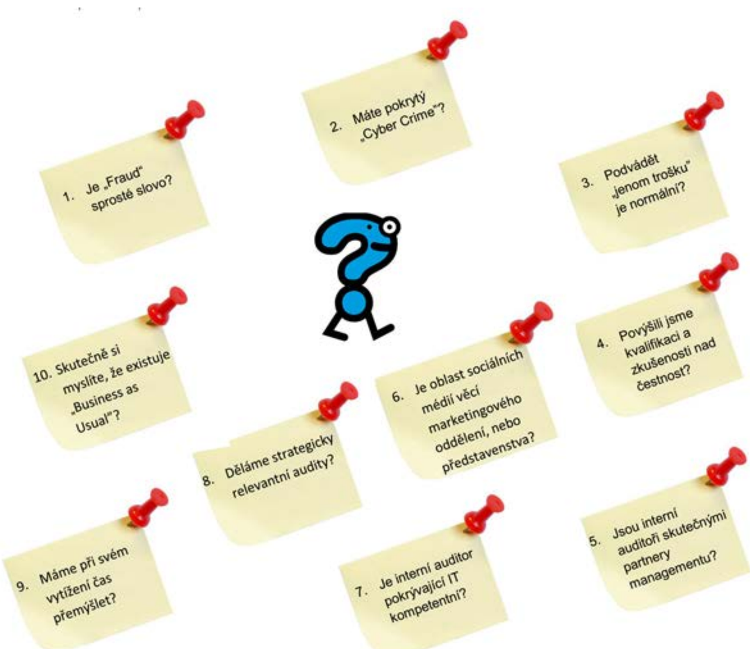
Níže uvádím přehled Concurrent Sessions.

Oblast	Téma	Přednášející
THE SIGNIFICANT IMPACT OF FINANCIAL SERVICES AUDITORS	Auditing in Financial Turmoil: Panel Discussion	Warren Stippich, CIA, CRMA Partner, National Internal Audit Leader Grant Thornton LLP, USA Despina Andreadou Group Audit Director Eurobank Ergasias SA, GREECE Ernesto Martinez Gomez, CIA, CRMA Corporate Deputy Chief Audit Executive Santander Group, SPAIN Ingrid Harbo Chief Audit Executive Swedbank Group, SWEDEN
	The Changing Face of Payments	George Thomas Senior Vice President, Chief Audit Executive First Data Corporation, USA
	Third Party Assurance In Financial Services	Lindsay Dart Managing Director Protiviti, UK
	Management Awareness of Culture and Related Controls: A Case Study	Scott Strachan Global Head of Internal Audit Aberdeen Asset Management PLC, UK
	A World of Regulations: Staying Ahead of the Compliance Curve	Jennifer Burke Partner Crowe Horwath LLP, USA Mark Howard Senior Vice President, Chief Audit Executive USAA, USA
	Do Financial Services Internal Audit Departments Need to Raise Their Game?	Paul Marshall Group Internal Audit Director Old Mutual, UK
	Data Analytics in Insurance	James Turner Group Wide Internal Audit Director Prudential, UK
FRAUD, BRIBERY & CORRUPTION: STOP THEM IN THEIR TRACKS	Auditing Fraud: How to Do It Right– A Practical Guide	Martin Robinson, CFIIA Independent Risk and Audit Consultant, UK
	Understand Risk and You Will Understand Fraud	Michael Fucilli, CIA, CGAP, CRMA Auditor General Metropolitan Transportation Authority, USA
	Proactive Anti-Corruption: The Necessity of Developing an Effective Program	Rob Kastenschmidt, CRMA Partner Mark McNamee Partner McGladrey LLP, USA
	Digital Forensics: The Five Big Questions	John Mitchell, Ph.D., CMIIA Managing Director LHS Business Control, UK
	Detecting Asset Misappropriation and Financial Reporting Fraud: Can Internal Auditors Help?	Rasha Kassem Lecturer in Accounting University of Northampton, UK
	A Primer on Fraud Investigations	H David Kotz, J.D. Director Berkeley Research Group, USA
	Risks of Fraud in Major Projects and Contracts	Mark Babington Director National Audit Office, UK
EMERGING GLOBAL ISSUES – WHAT DOES THE FUTURE HOLD?	Managing the Internal Audit Function for a Global Company and Elevating the Role of Internal Audit	Princy Jain, CIA, CCSA, CRMA Principal Partner PricewaterhouseCoopers, USA Inder Gulati Internal Audit Leader LinkedIn, USA
	Integrated Reporting: Value Proposition for Internal Audit's Stakeholders	Neil Stevenson Brand Director IIRC, UK Frank Curtiss Head of Corporate Governance RPMI Railpen Investments, UK Vincent Tophoff Senior Technical Manager IFAC, UK Helen Brand Chief Executive Officer ACCA, UK
	Adding Business Value Through the Governance & Auditing of Social Media	Tichaona Zororo, CIA, CRMA, CRMA Director EGIT I Enterprise Governance of IT, SOUTH AFRICA
	Auditing Integrated Reporting	Doug Anderson, CIA, CRMA Assistant Professor Saginaw Valley State University, USA
	The Future of the Three Lines of Defense Model	Rudi Hex, CIA, CFSA Audit Program Manager KBC Group, BELGIUM
	Auditing Sustainability: A Long-Term View	Anna Nefedova, CIA, CRMA Senior Manager Sustainability Deloitte&Touche LLP, USA
	How to Audit in a Virtual World	Marc Vael Chief Audit Executive, Smals vzw; President, ISACA Belgium vzw; International Vice President ISACA, BELGIUM
GOVERNANCE, RISK, & CONTROL: OBJECTIVE ASSURANCE, EFFECTIVE INSIGHT	Auditing Culture	Andrew Gallagher Group Audit Director BAE Systems, UK
	People Risk Management	Keith Blacker Consultant Values Count, UK
	Risk and Complexity in 21st Century Organizations	Richard Anderson Chair Institute of Risk Management, UK
	Sound Governance Needs a Strong Internal Audit Function	Bente Sverdrup State Authorized Auditor Gjensidige Forsikring ASA, NORWAY
	So You Think You Are Good– How Do You Get Better?	Greg Hollyman, CIA,CCSA, CFSA, CGAP, CRMA Chief Internal Auditor Australian Taxation Office, AUSTRALIA
	Integrated Auditing; Collaboration Between Second and Third Lines of Defense	Jonathan Calvert-Davies Partner PricewaterhouseCoopers, UK
	Are We Really Looking At Risks – Panel Discussion	Paul Sobel, CIA, CRMA Vice President, Chief Audit Executive, Georgia Pacific Corporation; 2013–14 Chairman of the Board of Directors, The IIA, USA Mark Fensome Director Group Audit Services Tui Travel PLC, UK Angela O'Hara Head of Northern and Central Europe Vodafone Group, UK Mike Roemer Group Head of Compliance Barclays, UK
INTERNAL AUDITOR OR INDISPENSABLE ASSET? THE CHOICE IS YOURS	Assuring the Audit Committee of Internal Audit's Quality	Anton B. van Wyk, CIA, CRMA Partner PricewaterhouseCoopers, SOUTH AFRICA
	Continuous Auditing: A Different Way of Providing Assurance	Karen Connell Audit Director Barclaycard, UK Lisa Nowell Global Director of Quality Assurance Barclays Bank, PLC, UK
	Auditing in a Hyper Growth Environment	David Shane Hogan Vice President, Global Audit Alliance Data, USA
	How Internal Audit Won Olympic Gold	Mary Munro Hardy Independent Director, UK
	Internal Audit's Contribution to the Regulatory Agenda	Iain Pickard Partner RSM Tenon, UK
	Innovations In Data Analytics for Internal Audit	Michael J. O'Leary Advisory Partner and Global Internal Audit Leader Ernst &Young, LLP, USA James Walton Advisory Analytics Senior Manager Ernst &Young, LLP, USA Amy A. Campbell Chief Audit Officer Caterpillar, Inc., USA Natacha Theytaz Chief Audit & Risk Advisory Executive F. Hoffmann-La Roche Ltd Group Audit & Risk Advisory, SWITZERLAND
	LEAN Internal Auditing – Achieving More With Less!	Sandro Boeri Managing Director Risk Audit Professional Development, UK

Fotografie str. 19–20 © 2014 by Institute of Internal Auditors, Inc.

TAKE YOUR TEAM TO THE TOP: MANAGE WITH IMPACT	Communication, Influence, and Partnerships	Rania Bejjani, CIA Vice President Group Internal Audit & Risk Management Colt Technology Services, UK
	Influencing and Political Know-how	James Paterson Director Risk &Assurance Insights Ltd., UK
	Leading and Managing the Internal Audit Function	Syed Imran Zia, CIA Chief Internal Auditor Gulf Drilling International, QATAR
	Importance of the Internal Audit Function Through the Stakeholders' Eyes	David Butler Head of Internal Audit Unum, UK
	Refocus and Transform Your Internal Audit Function	Carolyn Saint, CIA, CRMA Vice President 7-Eleven, Inc. 2013-14 Chair, North American Board of Directors, The IIA, USA
	The Audit Committee/Internal Audit Interface: A Vital Connection	Douglas van den Aardweg Director Fernwood Associates, UK
	Talent: The Differentiator of Great Audit Functions	Michael JK Taylor Head of Global Internal Audit Experian, UK
ELEVATING CORPORATE VALUES: IMAGINE THE POSSIBILITIES	Walking the Talk: Are You Willing to Pay the Price?	Deanna Sullivan, CIA, CRMA Principal Sullivan Solutions, USA
	Maintaining High Ethical Standards in an International Organization: The Experience of the European Commission	Stefan Sapundzhiev, CIA, CCSA, CFSA, CGAP, CRMA Head of Internal Audit of the Directorate - General for Internal Market and Services European Commission, BELGIUM
	Leadership Lessons from the Audit Trail	Richard Chambers, CIA, CGAP, CCSA, CRMA President and Chief Executive Officer The IIA, USA
	The Internal Auditor's Role in Corporate Social Responsibility	Barry Ackers, CIA Senior Lecturer University South Africa, SOUTH AFRICA
	Detecting Deception	Robert Cockerell Executive Director Korda Mentha Forensic, AUSTRALIA
	Implementing an Ethics Hotline: Lessons Learned	Andrijana Bergant Compliance Office Manager Zavarovalnica Triglav, d.d., SLOVENIA
	Different Governance Models: Do Any of Them Add Value?	Adrian Berendt Chartered Certified Accountant Berendt Consulting Ltd, UK Verra Marmilidou, CIA, CRMA Secretary General of the IIA Greek Chapter Hellenic Institute of Internal Auditors, Greece Peter Swabey Policy & Research Director ICSA, UK Frank Curtiss Head of Corporate Governance RPMI Railpen Investments, UK

THE DIVERSE FACETS OF PUBLIC SECTOR AND NOT-FOR-PROFIT	Success Strategies: Integrating Data Analytics in a Risk-Based Audit Plan	Bob Cuthbertson Chief Operating Officer CaseWare IDEA Inc., CANADA Peter Baker Principal Auditor Horsham District Council, UK
	Auditing in a Shared Services World	Robert Milford Head of Internal Audit Audit Cotswolds ~ Cotswold District Council, UK
	Governing Audit Committees	Sarah Blackburn, CRMA Chief Executive The Wayside Network Limited, UK Bruce Turner Audit Committee Chairman IIA Public Sector Committee, AUSTRALIA Bruce Sloan, CRMA Senior Principal Office of the Auditor General of Canada, CANADA Stephen Linden, CMIIA Director Protiviti Pty Ltd, AUSTRALIA Tea L. Enting-Beijering Chief Audit Executive Ministry of Infrastructure and Environment, THE NETHERLANDS
	Internal Auditing for Better Public Service Performance	James Jong Chief Internal Auditor Ministry of Education, NEW ZEALAND
	Unique Challenges for Public Sector and Not-For-Profit Organizations	Ara Kurazyan, CIA, CFSA, CCSA, CGAP, CRMA Senior Auditor Deloitte-Armenia, ARMENIA
	Emerging Trends In The Public Sector, Part 1	Drummond-Hill, CIA, CCSA, CGAP, CRMA Head of Internal Audit & Assurance (Retired), UK Bruce Turner Audit Committee Chairman IIA Public Sector Committee, AUSTRALIA Oliver Dieterle Chief Audit Executive Bundesagentur für Arbeit, GERMANY Tea L. Enting-Beijering Chief Audit Executive Ministry of Infrastructure and Environment, THE NETHERLANDS
	Emerging Trends In The Public Sector, Part 2	Drummond-Hill, CIA, CCSA, CGAP, CRMA Head of Internal Audit & Assurance (Retired), UK Bruce Turner Audit CommitteeChairman IIA Public Sector Committee, AUSTRALIA Oliver Dieterle Chief Audit Executive Bundesagentur für Arbeit, GERMANY Tea L. Enting-Beijering Chief Audit Executive Ministry of Infrastructure and Environment, THE NETHERLANDS
CIA EXAM REVIEW: PREPARE TO PASS	CIA Exam Prep Course: Part 2 — Internal Audit Practice	Raven Catlin, CIA, CFSA Trainer, Facilitator, Consultant Raven Global Training, USA Vicki McIntyre, CIA, CRMA, CFSA President First Plus Resolutions Inc., USA
	CIA Exam Prep Course: Part 2 — Internal Audit Practice CONTINUED	Raven Catlin, CIA, CFSA Trainer, Facilitator, Consultant Raven Global Training, USA Vicki McIntyre, CIA, CRMA, CFSA President First Plus Resolutions Inc., USA
	CIA Exam Prep Course: Part 2 — Internal Audit Practice CONTINUED	Raven Catlin, CIA, CFSA Trainer, Facilitator, Consultant Raven Global Training, USA Vicki McIntyre, CIA, CRMA, CFSA President First Plus Resolutions Inc., USA
	CIA Exam Prep Course: Part 3 — Internal Audit Knowledge Elements	Raven Catlin, CIA, CFSA Trainer, Facilitator, Consultant Raven Global Training, USA Vicki McIntyre, CIA, CRMA, CFSA President First Plus Resolutions Inc., USA
	CIA Exam Prep Course: Part 3 — Internal Audit Knowledge Elements CONTINUED	Raven Catlin, CIA, CFSA Trainer, Facilitator, Consultant Raven Global Training, USA Vicki McIntyre, CIA, CRMA, CFSA President First Plus Resolutions Inc., USA
	CIA Exam Prep Course: Part 3 — Internal Audit Knowledge Elements CONTINUED	Raven Catlin, CIA, CFSA Trainer, Facilitator, Consultant Raven Global Training, USA Vicki McIntyre, CIA, CRMA, CFSA President First Plus Resolutions Inc., USA
	CIA Exam Prep Course: Part 3 — Internal Audit Knowledge Elements CONTINUED	Raven Catlin, CIA, CFSA Trainer, Facilitator, Consultant Raven Global Training, USA Vicki McIntyre, CIA, CRMA, CFSA President First Plus Resolutions Inc., USA



Každý delegát si z konference odnesl mnoho poznatků a nápadů k zamyšlení. Já jsem vybral 10 oblastí, se kterými bych se s vámi rád podělil. Pokusme se nad uvedenými otázkami zamyslet a zkusit si upřímně odpovědět.

A jaké odpovědi byly během konference delegátům nabídnuty?

1. „FRAUD“ není sprosté slovo. Přesto se zdá, že v některých společnostech je zakázáno jej vyslovit. Přitom se jedná o riziko jako každé jiné. Je vysoce pravděpodobné, že se nějaká podvodná aktivita děje u vás ve společnosti právě teď. Interní auditor má jít v této oblasti příkladem a upozorňovat a otevřeně mluvit o tomto riziku.

„Máte při svém vytížení čas přemýšlet?“

2. Tzv. „Cyber Crime“ je údajně výnosnější než obchodování s drogami. Společnosti a auditoři by se měli ujistit, že se této problematice věnují dostatečně.

3. Podvádět „jenom trošku“ není normální. Materialita nemůže být v této oblasti zásadní. Jde o celkové nastavení kultury, morálky a organizačního zdraví společnosti. Nejdříve se pravděpodobně objeví pokusy o malé podvody (např. vyúčtování drobných výdajů), a pokud nejsou odhaleny a potrestány, budou se objevovat pokusy o podvody čím dál významnější. Tzv. „Tone at the Top“ je zásadní, ale stejně zásadní je „Tone in the Middle“. Tedy to, jakým způsobem jsou požadavky a očekávání vrcholového managementu přetlumočeny zaměstnancům. Klíčové je aktivní vyhledávání podvodů a zaměření se na riziko podvodů při každém auditu. Tento přístup podporuje i materiál IIA: „Internal Auditing and Fraud“.

4. Když přijímáme zaměstnance do své vlastní firmy, hledáme pravděpodobně především **čestnost**. Když přijímáme zaměstnance do „ne naší vlastní“ firmy, chceme **kvalifikaci a zkušenosti**. Je tento přístup správný? Zkusme se jen zamyslet nad možnými dopady této situace.

5. Interním auditorům je někdy vyčítáno, že pracují s malými vzorky a že jejich závěry nejsou reprezentativní. Řešením může být používání Continuous Auditing/Monitoring. Vyplatí se to pro identifikaci výjimek, anomálií a trendů. Na základě výsledů můžeme vytvořit kvalitnější plán auditu a můžeme testovat celou populaci. Výsledky lze rovněž ihned prezentovat managementu a nemusíme čekat, až bude daná oblast v plánu auditu. **Tím se vytvoří/podporuje partnerství s managementem.**

6. Máte pod kontrolou oblast sociálních médií? Máte v oblasti sociálních médií proaktivní přístup, nebo předstíráte, že se vás tato oblast netýká? Zamýšleli jste se někdy nad tím, kolik procent populace používá sociální média (Facebook, Twitter, LinkedIn…) a že nárůst použití je exponenciální? Jaký má/může mít dopad (např. na cenu akcií) zveřejnění informací na těchto sítích zaměstnanci/managementem? Má společnost někde definován přístup/strategii k sociálním médiím, role a odpovědnosti, má nástroje na sledování aktivit na sociálních médiích? **Pokud neřídíme sociální média, někdo to udělá za nás.** Zajímá někoho, zda je strategie v oblasti sociálních médií v souladu s obchodním modelem společnosti?

Strategie týkající se sociálních médií není už jen věcí marketingového oddělení, je to věcí představenstva.

7. Před 20 lety mohl pravděpodobně jeden IT auditor říci: „Umím zauditovat cokoli v oblasti IT“. **Není toto tvrzení v současné době již absurdní?** Společnosti by se měly zamyslet, zda mají dostatečné a kvalifikované zdroje pro kvalitní provedení IT auditů a případně uvažovat o out/cosourcingu.

„Podvádět ‚jenom trošku‘ není normální“

8. Děláme strategicky relevantní audity? Přemýšleli jste někdy, jak zásadní dopad má výběr oblastí pro audit na **vytvoření důvěry a partnerství s managementem?** Pokud se budeme zaměřovat na nepodstatné oblasti, nebude nás management brát vážně a žádné partnerství nebude existovat a naše přidaná hodnota pro společnost bude mizivá. Je nutné pokrývat klíčová rizika a diskutovat je napříč celou společností.

9. Máme při svém vytížení čas přemýšlet? Vyplatí se na chvíli zastavit se a zamyslet se nad tím, zda to, co děláme/plánujeme dělat, dává smysl a přináší skutečně hodnotu pro společnost. Je nutno auditovat chytře – neplatí čím více, tím lépe. Je nutné zaměřit se pouze na důležité oblasti. Dělání čehokoli jen z důvodu, že se to dělalo v minulosti, neobstojí.

10. Jsme flexibilní a schopni se rychle přizpůsobit měnícím se podmínkám? Už neexistuje nic jako „business as usual“. Interní auditor nesmí zaspat. Zejména rychlost technologických změn klade na interní auditory zvýšené nároky a musí svoji činnost stále přizpůsobovat, aby zůstali pro společnost relevantní.

Tak to byly oblasti, které vedly k zamyšlení mě. Pokud budete mít jakékoli dotazy, můžete mě kontaktovat na petr.hadrava@metlife.cz.

A co říci závěrem? Snad jen, že pomyslnou štafetu v pořádání konference IIA převzal kanadský Vancouver, kde se 74. konference Institutu interních auditorů s názvem **Mountains of Change… Oceans of Opportunities** uskuteční ve dnech 5.–8. července 2015. Pro bližší informace sledujte webové stránky Institutu interních auditorů.

Tento program je veden v angličtině a nabízen ve spolupráci s CIIA (Czech Institute of Internal Auditors) jako plnohodnotná verze CIA kvalifikace.

ČESKÝ INSTITUT INTERNÍCH AUDITORŮ

Certifikovaný interní auditor CIA®

Co je CIA®

Proč studovat CIA®

Výhody studia s Akademií

Detaily programu

Více informací a registrace

Certifikovaný interní auditor (CIA®) je **jedinou globálně uznávanou certifikací pro interní auditory** a zároveň představuje standard, na jehož základě jednotlivci prokazují své schopnosti a profesionalitu v oblasti interního auditu.

Jste auditor s dlouhodobou praxí nebo se připravujete na kariéru budoucího manažera a chcete **zvýšit svůj kariérní potenciál** a **dosáhnout profesních úspěchů v oblasti interního auditu**? Potom je CIA® pro vás ideální volba.

- ✓ **Profesionálové z oddělení auditu** PwC, kteří mají rozsáhlé znalosti obsahu této kvalifikace
- ✓ Ucelené PwC **studijní materiály**, připravené podle **nového sylabu** a plně **schválené IIA** (The Institute of Internal Auditors)
- ✓ **Výuka v angličtině** - získáte ucelený slovník obsahující **terminologii interního auditu**, užitečný v mezinárodním podnikatelském prostředí
- ✓ **Zvýhodněná cena** pro členy ČIIA (sleva 2 000 Kč z každé části)

Část I	Část II	Část III
10. - 12. prosince 2014	**16. - 18. března 2015**	**červen 2015**
Úloha interního auditu při řízení a správě společnosti, řízení rizik a kontrole	*Realizace interního auditu*	*Analýza podnikání a informační technologie*

V případě zájmu vám rádi poskytneme další informace. Kontaktovat nás můžete na email **the.academy@cz.pwc.com** nebo na tel. **+420 251 152 446**.
Registrovat se můžete na našich webových stránkách, kde také naleznete více informací.
www.pwc.cz/academy

pwc

PwC's Academy

inzerce

IDEA je v ČR a SR již 20 let!

Dvacetileté výročí neslavíme každý den, a proto neváhejte a využijte mimořádné příležitosti zakoupit software IDEA s **20% slevou!**

IDEA
20 let s Vámi
20 % sleva

ZA KAŽDÝ ROK
1 % DOLŮ!

J + Consult spol. s r.o.
Čapkova 2/195, 140 00 Praha 4
Tel.: +420 244 118 411, www.jconsult.cz

IDEA 20 let s Vámi

jconsult

COSO 2013 – klubové odpoledne

ČESKÝ INSTITUT INTERNÍCH AUDITORŮ

Corporate Governance Institute
Risk, Ethics and Compliance

pwc

Český institut interních auditorů (ČIIA) ve spolupráci s Corporate Governance Institute (CGI) a za podpory PricewaterhouseCoopers (PwC) uspořádali dne 19. června 2014 v příjemných prostorách Rytířského paláce České spořitelny v centru Prahy Klubové odpoledne s nosným a aktuálním tématem COSO 2013. Akce byla zahájena ze strany prezidentů Tomáše Pivoňky (ČIIA) a Vladimíra Brože (CGI). Oba zdůraznili potřebu pozitivně vnímat aktualizovaný rámec COSO jak z pohledu interního auditu, tak z pohledu corporate governance. Na toto zahájení pak navázali vystupující Bohuslav Poduška (Česká spořitelna), Dalibor Schikuta (Škoda Auto) a Chris Michael Tait (PwC). Ve svých prezentacích představili praktické aspekty uplatňování rámce COSO v rámci vnitřních řídicích a kontrolních systémů s přihlédnutím k jeho aktualizované podobě.

Bohuslav Poduška představil mimo jiné historický vývoj rámce COSO, včetně zásadních prvků aktualizované podoby COSO 2013. Velmi přínosné bylo praktické představení vyhodnocení řídicích a kontrolních systémů prostřednictvím interního auditu.

Dalibor Schikuta pojal svoji prezentaci z praktického pohledu interního auditora, konkrétně jak prověřit COSO komponenty ve vztahu k hodnocení systému risk managementu a internímu kontrolnímu systému.

Chris Michael Tait ve své prezentaci celkově shrnul integrovaný přístup k podnikovým rizikům a kontrolám. Velmi detailně představil přínosy aktualizovaného rámce COSO v rámci pohledu a požadavku na vnitřní kontrolní systémy. Zdůraznil, že nové COSO nejenže nezvyšuje požadavky na kontrolu, ale ponechává prostor pro uplatnění vlastního úsudku ve vnímání požadavků na vnitřní kontrolu.

▲

Daniel Häusler

PŘEDSTAVUJEME CORPORATE GOVERNANCE INSTITUTE (CGI)

Autor: Vladimír Brož

CGI je spolek sdružující tajemníky společnosti a další profesionály působící v oblasti compliance, podnikatelské etiky, správy podnikatelských seskupení a majetkových účastí, řízení rizik a dalších příbuzných správních oblastech a funkcích (řízení rizik, společenská odpovědnost, prevence podvodů a dalších forem nežádoucího jednaní atd.). Cílem CGI je prosazovat principy corporate governance do praxe a ukazovat, že řádná administrace správy společnosti , etika podnikání, compliance a další správní funkce nejsou zbytnou činností či trpěnou povinností, nýbrž předpokladem pro dlouhodobou udržitelnost podnikání a ziskovosti obchodních korporací a obecně pro kontinuitu činnosti a existenci právnických osob. CGI je právním nástupcem Českého institutu tajemníků obchodních společností, který byl založen v roce 2002. Z hlediska svého zaměření a cílů je CGI přirozeným a zároveň jedním z nejbližších partnerů ČIIA. Bližší informace a kontakty: www.governance.cz

CPE
KONTINUÁLNÍ PROFESNÍ VZDĚLÁVÁNÍ

INFORMACE PRO VŠECHNY CERTIFIKOVANÉ OSOBY

Doba hlášení	Všichni certifikovaní musí podávat hlášení **každý rok**.
Datum hlášení	Datum hlášení **ke dni 15. prosince**
Počet hodin vyžadovaných pro CIA	• 40 hodin za rok (pokud jste praktikující) • 20 hodin za rok (pokud nejste praktikující) • 0 hodin (pokud jste v důchodu)
Počet hodin vyžadovaných pro CCSA, CFSA, CGAP, CRMA	• 20 hodin za rok (pokud jste praktikující) • 10 hodin za rok (pokud nejste praktikující) • 0 hodin za rok (pokud jste v důchodu)
Požadavky CPE pro specializované certifikace	25 procent získaných hodin CPE musí být v oblasti specializovaných odborných znalostí.
Osvědčení vyžadované v okamžiku podávání hlášení CPE	Postupujete v souladu s Mezinárodním rámcem IIA pro profesní praxi (IPPF). Budete se řídit Etickým kodexem IIA. Nepoškodíte dobré jméno IIA. Stvrdíte neexistenci záznamů v trestním rejstříku vzniklých od předchozího hlášeného období.
Poplatek za roční hlášení CPE	Členové 0 Nečlenové 100 USD (přepočteno dle aktuálního kurzovního lístku + DPH)

Všechny certifikované osoby jsou odpovědné za udržování svých znalostí a dovedností a doplňování svých znalostí a dovedností z hlediska zdokonalování a současného vývoje v oblasti standardů interního auditu, jeho postupů a metod nebo v jejich oblastech specializace (audity státní správy, finanční služby, sebehodnocení řízení a kontroly, nebo ujištění v oblasti řízení rizik). Držitelé certifikátů musí potvrdit za svou osobu absolvování vyžadovaného počtu hodin průběžného vzdělávání a odpovědností každé certifikované osoby je, zajistit, aby hlášené hodiny CPE byly v souladu s pokyny stanovenými Radou IIA pro profesní certifikaci.

V případě zachování statutu „aktivní“ je nutné nejpozději **do 31. prosince** každého roku podat hlášení CPE. Pokud je hlášení podáno do Českého institutu interních auditorů, termín je **do 15. prosince** každého roku. Certifikovaní musí předložit příslušný formulář do Českého institutu interních auditorů, který následně informace o certifikovaných odesílá do mezinárodního institutu The IIA.

Nepředložení formuláře hlášení CPE do stanoveného termínu má za následek automatickou změnu stavu certifikace z „aktivní – certifikován“ na „neaktivní“ a pro obnovení platnosti je pak nutné podat hlášení CPE v počtu hodin odpovídající aktuálnímu stavu a uhradit poplatek za obnovení platnosti.

ROČNÍ POPLATEK ZA UDRŽENÍ CPE

Členové ČIIA mají hlášení CPE zahrnuto v rámci poplatku za celoroční členství.

Hlášení CPE je zpoplatněno pouze pro nečleny ČIIA a to ve výši 100 USD (přepočteno dle aktuálního kurzovního lístku + DPH). ČIIA do konce roku vystaví faktury všem certifikovaným – nečlenům.

V případě, že faktura za hlášení CPE nebude uhrazena, držitel certifikátu bude zařazen do stavu „neaktivní“.

Všechny podrobné informace k CPE je možno nalézt v Organizační směrnici č. 4:2011, která určuje požadavky týkající se průběžného profesního vzdělávání pro všechny druhy certifikačních programů nebo na stránkách ČIIA www.interniaudit.cz

Z důvodu lepší transparentnosti a snazšího ověření, zda certifikovaná osoba je zařazena ve stavu „aktivní“ nebo ve stavu „neaktivní“, jsou zveřejněna jména všech certifikovaných osob na webových stránkách ČIIA. V případě nesouhlasu tohoto kroku prosím kontaktujte kancelář.

▲

Magda Barnatová

CERTIFICATE OF HONORS

V minulém čísle Interního auditora jsme informovali o mimořádném úspěchu pana Aurela Badaniče, senior interního auditora ve společnosti T-Mobile, který složil všechny části zkoušky CIA na první pokus, s vysokým bodovým ohodnocením, a stal se tak prvním držitelem „speciálního certifikátu" v České republice. Jaké jsou jeho dojmy a zkušenosti z certifikačních zkoušek, přinášíme právě nyní:

Jak dlouho se věnujete internímu auditu a jak jste se k této profesi dostal?

K internímu auditu jsem se dostal více-méně náhodou. Po studiích managementu jsem osm let pracoval jako konzultant a projektový manažer. Také v T-Mobile jsem začínal jako projektový manažer pro zlepšování procesů – v rámci malého specializovaného týmu interních konzultantů jsme optimalizovali různé oblasti businessu. Moje pozadí je tedy silně businessové, i když pro zlepšování procesů je nevyhnutné dobře zanalyzovat výchozí stav a jeho příčiny, takže jsem několik desítek takových businessových auditů realizoval i předtím. O profesi interního auditora jsem však neuvažoval, až při reorganizaci v roce 2011 jsem dostal nabídku využít jako „oficiální" interní auditor propojení svého businessového pohledu se strukturovanou metodikou interního auditu. Chvíli jsem váhal, obával jsem se přílišného svázání formálními pravidly, ale ukázalo se to jako výborná synergie.

Co pro Vás bylo impulzem pro to, abyste o titul CIA usiloval? Je tato certifikace vyžadována Vaším zaměstnavatelem?

T-Mobile certifikaci CIA pro auditory nevyžaduje, ale doporučuje ji a podporuje. Impulzem pro mě bylo právě to, že jsem měl praxi, ale chyběly mi teoretické a metodické znalosti, a tak, když mi zaměstnavatel certifikaci v rámci osobního rozvoje nabídl, neváhal jsem. Měl jsem zájem nejenom nastudovat pravidla, ale do hloubky pochopit vnitřní logiku auditování a specifickou roli interního auditu ve společnosti.

Vaše výsledky při skládání zkoušky CIA byly absolutně mimořádné. Jak dlouho vám trvala příprava na jednotlivé zkoušky? Absolvoval jste nějaké přípravné kurzy, nebo jste se připravoval sám, popř. z jakých materiálů jste vycházel?

Nevěděl jsem, odkud začít, neznal jsem nikoho, kdo by certifikaci CIA dělal od doby, kdy se přešlo na počítačové testování, tak jsem se na základě doporučení přihlásil na přípravný kurz organizovaný PwC Academy. Před každou částí zkoušky jsme měli 3–4 dny intenzivní „nálévárny" spojené s procházením vzorových testovacích otázek. Toho učiva je opravdu hodně, ale já jsem se spíše snažil porozumět logice kladení otázek a hledat klíčová slova, na základě kterých je možné odhalit správnou odpověď. Na kurzech jsem si totiž všiml, že delší praxe může být paradoxně překážkou při hledání správných odpovědí na teoretické otázky – člověk už vidí předestřené situace z pohledu toho, co při auditování zažil, a praxe je vždy komplexnější a méně jednoznačná než teorie. Den před samotnou zkouškou jsem ještě věnoval zopakování hlavních témat a vzorovým testovacím otázkám.

Co bylo klíčem k úspěšnému složení zkoušek?

Odvaha to zkusit. Z přípravných kurzů jsem pokaždé odešel s několika svazky učebních materiálů, což v čase, kdy už máte mnoho let po škole a dávno jste zapomněli, jak se drtí na zkoušky, působilo dost děsivě. Navíc, statistika úspěšnosti na zkouškách CIA je možná ještě horší než na těch vysokoškolských. Viděl jsem, že účastníci přípravných kurzů z toho byli dost vystrašeni a odkládali samotnou zkoušku na nějaký klidnější čas, kdy budou mít více prostoru pro samostudium. Já jsem věděl, že s prací a rodinou už žádný klidnější čas mít nebudu, a tak jsem se snažil přihlásit na zkoušku vždy bezprostředně po kurzu, nejlépe v následujícím týdnu, abych alespoň nezapomněl to, co do mě na kurzu „natlačili". To byl můj klíč k tomu, že jsem to vůbec udělal.

Co vám pomohlo, že jste dosáhl tak vysokého počtu bodů?

Sám nevím. Po jednotlivých zkouškách, ale ani na závěr, při udělení certifikátu CIA, vám nikdo neřekne, kolik bodů jste dostal – bylo to pro mě nepochopitelné, ale v USA si to střeží jako největší tajemství. Takže když mě rok poté kontaktovali ohledně udělení čestného certifikátu za mimořádně vysoký počet dosažených bodů, byl jsem z toho hodně překvapený.

Co pro Vás bylo na zkouškách nejobtížnější, např. jaká část byla nejnáročnější?

Určitě účetnictví ve třetí části, to bývá nejtěžší téměř pro všechny. Sice jsem měl několik zkoušek z účetnictví na vysoké škole, potkávám se s ním i v auditorské praxi, ale zejména mezinárodní účetní standardy, a ještě k tomu anglické názvosloví – dělal jsem totiž přípravu i zkoušku v angličtině – byl oříšek. Naštěstí, a tím snad povzbudím i další, na samotné zkoušce až tolik účetních příkladů nebylo, takže se to dalo dohnat na jiných tématech.

Časový limit na jednotlivé části byl dostačující?

Myslím, že ano. Já při zkouškách dost přemýšlím, tedy stíhal jsem to jen tak tak, ale vždy jsem zvládl dojít až k poslední otázce, akorát jsem to někdy už nezvládal po sobě znovu kontrolovat.

Co byste poradil kandidátům, kteří se na zkoušky připravují, aby dosáhli co nejlepších výsledků?

Mít odvahu a používat selský rozum – to platí jak při zkouškách, tak i v životě.

Děkuji za rozhovor.

Magda Barnatová

NOVÍ CERTIFIKOVANÍ *(nejen)* INTERNÍ AUDITOŘI

V současné době evidujeme celkem 304 certifikovaných:

276	CIA
10	CGAP
2	CCSA
3	CFSA
13	CRMA

V měsících květen–červen–červenec 2014 nám řady certifikovaných rozšířili tito:

Pavel Krčál, CIA, CRMA; Vendula Lajblová, CIA
Luboš Trojan, CIA; Bedřich Hejl, CIA, CRMA
Robert Pecha, CIA, CRMA; Bohuslav Poduška, CIA, CRMA; David Risser, CRMA; Andrea Schlossarek, CIA, CRMA; Jan Špaček, CIA, CRMA

GRATULUJEME!

Upozornění: Kompletní certifikační program je nutné dokončit do 4 let od podání registrace.

Certifikace interních auditorů ve veřejné správě

Přehled o počtu žádostí a vydaných certifikátů

Počet žádostí od 1.1.2014	34
Počet vydaných certifikátů	29
Celkový počet žádostí od r. 2011	256
Celkem vydaných certifikátů od r. 2011	243

Upozornění pro certifikované

	VIAS	VIAK
Hlášení CPE do konce roku 2014 pro vydané certifikáty v roce	2011	2012

Počet certifikovaných auditorů ve VS dle oblastí do 31.8.2014

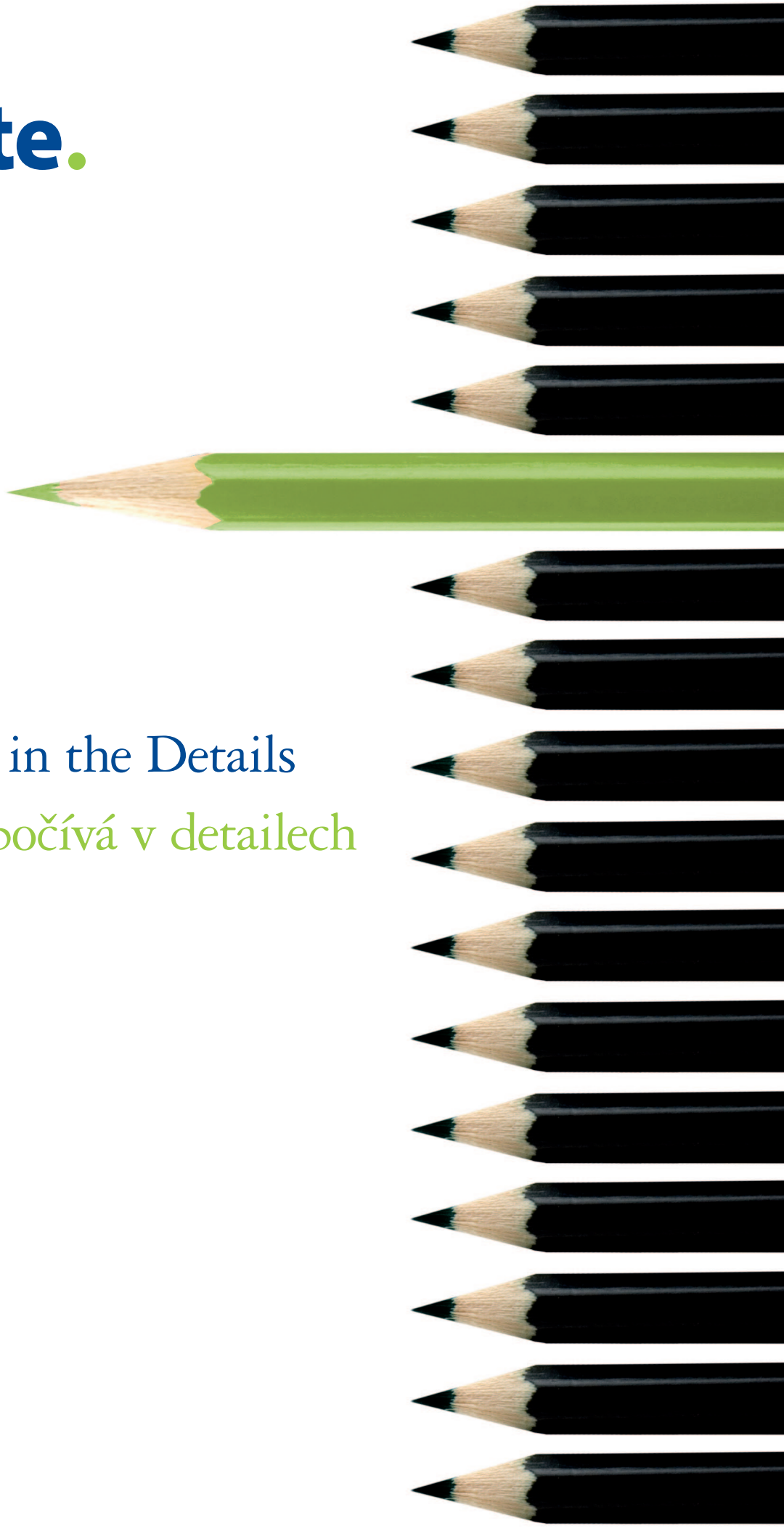
Oblasti	Počet VIAA	Počet VIAJ	Počet VIAS	Počet VIAK	Počet IA dle oblastí
Ministerstva	9	7	35	14	**65**
Krajské úřady	1	2	3	6	**12**
Úřady měst a obcí	8	11	20	5	**44**
Policie a Hasiči	3	4	5	2	**14**
Vysoké školy	0	0	4	2	**6**
Ostatní	14	16	18	10	**58**
Celkem IA ve VS	**35**	**40**	**85**	**39**	**199**

Z toho č. vydaného certifikátu 10 (VIAK, oblast Vysoké školy) je neaktivní pro nesplnění hlášení CPE.

NOVÍ ČLENOVÉ ČIIA

- Ing. Irena Andělová, Euro-Trend, s.r.o.
- Ing. Martina Brázdová, Ministerstvo vnitra ČR
- Ing. Marie Burešová, CSc., Generální finanční ředitelství
- Ing. Lubomír Cakl, ČD Cargo, a.s.
- Ing. Mgr. Marek Čáp, FCCA, KPMG Česká republika, s.r.o.
- Ing. Zdeňka Dlesková, Generální finanční ředitelství
- Ing. Eva Dobrá, ING Management Services, s.r.o.
- Ing. Mgr. Radka Domanská, Ředitelství silnic a dálnic ČR
- Ing. Jana Hanzalíková, Česká správa sociálního zabezpečení
- Ing. Hana Hojgrová, Hasičský záchranný sbor Jihočeského kraje
- Ing. Libor Jelínek, Státní pozemkový úřad
- Ing. Barbora Jonaštíková, OHL ŽS, a.s.
- Mgr. Mária Jurečko, MBA, NEWPS.CZ s.r.o.
- Ing. Sarah Kabanji, Individuální členka
- Ing. Zuzana Kašparovská, Pražská plynárenská, a.s.
- Ing. Lucie Kiesewetterová, Komerční banka, a.s.
- Ing. Marie Kolářová, Město Šternberk
- Mgr. Peter Kopačka, Individuální člen
- Ing. Ludmila Kostelníková, Město Uherský Brod
- Kateřina Koudelková, Státní tiskárna cenin, s.p.
- JUDr. Ing. Petr Krömer, Generální finanční ředitelství
- Mgr. Pavel Kunc, Ministerstvo pro místní rozvoj ČR
- Ing. Vendula Lajblová, Komerční banka, a.s.
- Mgr. Eva Leblová, Dopravní podnik hl.m. Prahy, a.s.
- Ing. Jana Lepičová, Ředitelství silnic a dálnic ČR
- Ing. Petr Lukavec, CISA, PricewaterhouseCoopers Audit, s.r.o.
- Ing. Martina Muchová, Individuální členka
- Ing. Mgr. Michaela Müllerová, Global Payments Europe, s.r.o.
- Ing. Karel Nosek, CISA, ING Management Services, s.r.o.
- Mgr. Andrej Osadský, HORNBACH BAUMARKT CS spol. s.r.o.
- Ing. Martina Pipková, Individuální členka
- Ing. Barbora Pastuchová, Komerční banka, a.s.
- Ing. Michaela Penková, CIA, ING Management Services, s.r.o.
- Ing. Nikol Pitoňáková, Pražská energetika, a.s.
- Ing. Hana Průšová, RCI FINANCE CZ, s.r.o.
- Jan Roubíček, DiS., ČD Cargo, a.s.
- Ing. Miloš Rybka, ČD Cargo, a.s.
- Ing. Helena Soukupová, Generální finanční ředitelství
- Ing. Klára Sýkorová, Generální finanční ředitelství
- Ing. Pavlo Sud'a, Individuální člen
- Ing. Hana Šilhavá, Česká obchodní inspekce
- Ing. Eva Štěpánková, Ministerstvo pro místní rozvoj ČR
- Ing. Tereza Vítková, Česká správa sociálního zabezpečení
- M.Sc. Kateřina Zajacová, Individuální členka
- Ing. Pavel Zehnálek, Ph.D., MBA, Individuální člen
- Ing. Beata Žílová, Ministerstvo pro místní rozvoj ČR

Deloitte.



Success is in the Details

Úspěch spočívá v detailech

Vážení čtenáři,

od roku 2013 nalézáte v časopise Interní auditor stránku s oddychovo-naučnou rubrikou. V každém čísle je pravidelně zveřejněno několik otázek z oblasti interního auditu, které jsou součástí testu na certifikaci CIA, a také křížovka nebo obdobná zábavná hra s tajenkou. Správné odpovědi na otázky, včetně tajenky, jsou slosovatelné o hodnotnou cenu, přičemž odpovědi na otázky a tajenka příslušného čísla jsou zveřejněny vždy v dalším čísle časopisu Interní auditor.

Odpovědi na otázky a tajenku je možné vyplnit pouze na webu – www.interniaudit.cz, a to do 31. října 2014. Výherce bude následně vylosován na nejbližším jednání Redakční rady. Vylosovaný výherce z čísla 3/2014 obdrží jednodenní seminář na ČIIA zdarma dle vlastního výběru.

Přeji hodně štěstí.
Daniel Häusler

SUDOKU

	3	7	1	8		5	6	
5				3		7		8
8	6	9		5	4	1		2
6	7	5	3		9	4	8	1
		3	4	7	5	9	2	6
2		4	8	6			5	7
7	1			4			9	3
9		6		1		8		4
3		8	6		7	2		

Správná tajenka z minulého čísla:
LEGISLATIVA

Výherce z minulého čísla *(mimořádně dva výherci):*
Jaroslava Bradová, Statutární město Jihlava
a David Polášek, Česká spořitelna, a.s.
GRATULUJEME

OTÁZKY INTERNÍHO AUDITORA

1. Jaké jsou základní teze interního auditu?

a. Interní audit je objektivně ujišťovací a poradenská činnost.

b. Interní audit pomáhá organizaci dosahovat jejích cílů tím, že přináší systematický metodický přístup k hodnocení systému řízení rizik.

c. Interní audit je nezávislá, objektivně ujišťovací a poradenská činnost zaměřená na přidávání hodnoty a zdokonalování procesů v organizaci. Interní audit pomáhá organizaci dosahovat jejích cílů tím, že přináší systematický metodický přístup k hodnocení a zlepšování účinnosti systému řízení rizik, řídicích a kontrolních procesů a řízení a správy organizace.

d. Interní audit přináší systematický metodický přístup k hodnocení a zlepšování účinnosti systému řízení rizik, řídicích a kontrolních procesů a řízení a správy organizace.

2. Základní zásady, důležité pro profesi a praxi interního auditu, dle Etického kodexu jsou:

a. Integrita, Objektivita, Odpovědnost, Slušnost

b. Objektivita, Integrita, Čestnost, Slušnost

c. Důvěrnost, Objektivita, Integrita, Kompetentnost

d. Kompetentnost, Důvěrnost, Profesionální jednání, Respekt

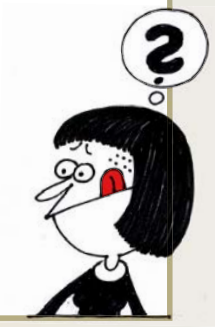
3. Které z uvedených nejlépe popisuje ujišťovací služby poskytované interním auditem organizaci?

a. Ujišťovací služby představují objektivní posouzení informací s cílem poskytnutí nezávislého názoru.

b. Ujišťovací služby představují objektivní posouzení informací, jehož cílem je poskytnutí nezávislého názoru nebo závěrů ohledně určitého procesu, systému nebo jiného předmětu posouzení. Charakter a rozsah ujišťovací zakázky určuje auditor. Ujišťovací služby obvykle zahrnují tři strany – Interního auditora, Vlastníka procesu či auditované oblasti a Uživatele hodnocení.

c. Ujišťovací služby obvykle zahrnují dvě strany – Interního auditora (provádějící hodnocení) a Vlastníka procesu či auditované oblasti (jedince či skupinu, kteří jsou v přímém vztahu k dané organizační jednotce, jednotlivým činnostem, funkci, systému nebo jiné předmětné záležitosti).

d. Ujišťovací služby obvykle zahrnují tři strany – I. Interního auditora (provádějící hodnocení), II. Vlastníka procesu či auditované oblasti (jedince či skupinu, kteří jsou v přímém vztahu k dané organizační jednotce, jednotlivým činnostem, funkci, systému nebo jiné předmětné záležitosti) a III. Uživatele hodnocení (jednotlivce nebo skupinu využívající hodnocení a závěry interního auditu).



Správné odpovědi z minulého čísla...

1. Náležitá role interního auditu je:

a. Slouží jako nezávislá, objektivně ujišťovací a konzultační činnost přidávající hodnotu společnosti

b. Slouží jako vyšetřovací orgán představenstva

c. Pomáhá externímu auditorovi při snižování poplatků za externí audity

d. Provádět studie, které podpoří dosažení vyšší efektivity činností společnosti

Vysvětlení: Odpověď «A» Definice interního auditu zní: „Interní audit je nezávislá, objektivně ujišťovací a poradenská činnost zaměřená na přidávání hodnoty a zdokonalování procesu v organizaci. Interní audit pomáhá organizaci dosahovat jejích cílů tím, že přináší systematický metodický přístup k hodnocení a zlepšování účinnosti systému řízení rizik, řídicích a kontrolních procesů a řízení a správy organizace.“

2. Nejdůležitějším důvodem pro zajištění adekvátních a dostatečných zdrojů interního auditu je:

a. Splnit povinnost zajištění efektivního plánu následnictví

b. Zajistit důvěryhodnost interního auditu před auditním výborem a vedením společnosti

c. Prokázat dostatečnost zdrojů pro splnění auditního plánu

d. Zajistit, že interní audit je chráněn před outsourcingem

Vysvětlení: Odpověď «C» Dle standardu 2030: „Vedoucí interního auditu musí zajistit, aby zdroje interního auditu pro splnění schváleného plánu byly vhodné, dostatečné a účinně rozmístěné.“

3. Která z následujících aktivit nepatří k povinnostem interního auditu?

a. Ochrana majetku

b. Hodnotit efektivitu činností a aktivit oddělení v dosahování stanovených cílů

c. Hodnocení kontrol zajišťujících soulad se zákony a regulacemi

d. Zjišťování plnění nastavených cílů

Vysvětlení: Odpověď «A» Ochrana majetku je operativní aktivita a z tohoto důvodu nepatří k povinnostem interního auditu.

Karel Javůrek
absolvent fakulty sociálních věd
Univerzity Karlovy v Praze, obor mediální studia

Nástrahy na cestách

Když jsem dostal zadání napsat něco na téma bezpečnosti, řekl jsem si, že by to mohl být dobrý námět na dovolenou. Jenže nové číslo vyjde až po létě. Takže to tentokrát budou takové příslovečné rady „s křížkem po funuse“.

Někteří jednotlivci si však dovolenou vybírají až po sezoně, pro ně tedy může být téma ještě aktuální. Nástrah na cestách číhá na člověka celá řada. Pominu takové banální nehody, kdy si člověk chtivý bronzové pleti, připeče kůži do červena hned první den tak, že zbytek dovolené stráví ve stínu napatlaný panthenolem. S riziky v době letních radovánek je potřeba počítat na každém kroku.

Pokud máte malé děti, víte, že takové dítě je přímo magnet na úrazy. Celý den je v podstatě jeden zadržovaný pád. Můj syn si zrovna nedávno rozsekl bradu, takže jsme místo výletu jeli rovnou do nemocnice na šití. Stačí chvilka nepozornosti, když zrovna píšete manželce textovou zprávu, jak vám ta společná dovolená s dětmi krásně klape.

Dalším potenciálním zdrojem nebezpečí jsou motorová vozidla. Dáte si třeba před dovolenou vyměnit v servisu brzdové kotouče a vesele vyrazíte na cestu. A ejhle! Než dojedete ke kýženému cíli, porouchá se vám… hádejte co? Pochopitelně, brzdové kotouče. V místním servisu vám pak sdělí, že předchozí oprava byla provedena neodborně. Tato informace vás trochu zaskočí, protože jste v intencích bezpečné cesty vyhledali autorizovaný servis. Po návratu z dovolené vás ještě místo omluvy nutí dokazovat důvod opravy. Obvykle si přece člověk na dovolené z plezíru zajde do servisu a nechá vyměnit funkční součástku, že?

A co teprve jídlo! To je na dovolené také riskantní podnik. Nemyslím tím pouze různé exotické plže, mlže a hlavonožce. Pokud trávíte dovolenou v zahraničí, řešíte i jak se v restauraci domluvíte. Nebo si objednáte něco, co jste vlastně nechtěli. Ve španělsky mluvících zemích si objednáte třeba „tortillu con pollo“, ale místo křupavé kukuřičné placky s kousky masa a zeleniny vám přinesou obyčejnou vaječnou omeletu. Kuře abyste v ní hledali lupou. I na nedalekém Slovensku můžete s jazykovou odlišností narazit. Místo zajímavě znějící „kapustové polévky“ dostanete normální zelňačku. A co teprve když si objednáte „vyprážanú pečeň“. Místo pečínky najdete na talíři fádní smažená játra.

Na cestách je ale potřeba dávat si pozor nejen na děti, auta a jídlo, ale hlavně na sebe sama. Vidíme se prostě jinýma očima. Vaši známí a kamarádi jistě ocení tu úžasnou fotku ze skalního útesu za cedulí „Nevstupovat! Nebezpečí pádu!“, kterou okamžitě pošlete na sociální sítě. Prostě si užíváte. Od toho také dovolená je.

Sklon k dobrodružství by ale neměl překročit naše instinkty. Liška chycená do pasti si prý v pudu sebezáchovy uhryže nohu. Lidem by jen stačilo, aby se do pasti vlastí neopatrnosti nechytili sami a nehryzaly je pak výčitky svědomí.

ENGLISH ANNOTATION

Zdeněk Macháček

Well-Managed Security Minimises Potential Damages

In his article, the author points out the importance of security management in organisations, posing and answering the questions of what we want to protect, against whom and how. We learn about the basic groups of security measures, the current threats in the banking sector, and prevention as the most effective way to protect ourselves.

Radek Kučera

The Human Factor – the Most Underestimated Security Risk

The author deals with various security risks that organisations face, especially in the human resources field.

Tomáš Pluhařík

Why is it important to have an IT auditor?

The author discusses IT security in the context of the current national legislation, and the risks and obligations it brings.

Igor Gricinko

Physical and IT Security: Joint and Several?

How is physical security related to e-shops on the internet when you happen to have a spare 40 to 700 USD and you feel like playing? How can a small box devalue investments in IT security amounting to hundreds of thousands? The author of the article seeks to draw a parallel between physical, IT and HR security using real-life examples from his experience as an auditor.

Lukáš Wagenknecht

New Act on Internal Management and Control

The author presents the key ideas of the proposed new act on internal management and control.

Ivana Krůželová

The Big European Hand is Scratching Your Back

The author comments on the policy of the European Commission towards EU states in which structural funds are used.

Petr Hadrava

A Review of the International Conference of the Institute of Internal Auditors in London

The author briefly summarises the content of the International Conference that took place in London, 6–9 July, 2014. He also points out the key takeaways that could be used by the readers in their day to day work.

Daniel Häusler

COSO 2013 – Club Afternoon

Brief information about the meeting of the representatives of internal auditors and secretaries of trading companies on the topic of the COSO framework.

Magda Barnatová

Certificate of Honors

Interview with the CIA title holder who obtained special Certificate of Honors for excellent exam results.

Žádné podnikání pro nás není malé

ČESKÁ SPOŘITELNA
Jsme Vám blíž.

Naši poradci pro podnikatele znají potřeby malých a středních firem. Stavte se u nás v pobočce a přesvědčte se, že máme komplexní nabídku i pro Vaše podnikání.