iA interní auditor

ČTVRTLETNÍK ČESKÉHO INSTITUTU INTERNÍCH AUDITORŮ
ROČNÍK 23, ČÍSLO 2–2019 (92) 2|2019

Kybernetická bezpečnost nejen očima interního auditora

REZERVUJTE SI TERMÍN

VYSTUPUJÍCÍ

PETR HANZLÍK, OKD • **TOMÁŠ JINDRA,** UNICREDIT BANK • **MAREK JÍLEK,** DELOITTE
JAROSLAVA KOPOVÁ, MĚSTO ŠUMPERK • **JIŘÍ KHUN,** KPMG
DAVID NAVRÁTIL, ČESKÁ SPOŘITELNA • **DANA RATAJSKÁ,** MMR
JAN SEIDL, DELOITTE • **LADISLAVA SLANCOVÁ,** NKÚ
PETR ŠVUB, ČESKÁ SPOŘITELNA • **VLADIMÍR VALENTA,** ČEZ
MARTIN VLČEK, KÚ MORAVSKOSLEZSKÉHO KRAJE • **LENKA VONDRA,** KPMG

TÉMATA

AGILNÍ ŘÍZENÍ • COMPLIANCE PROGRAM • KYBERNETICKÁ BEZPEČNOST • MONITORING NÁPRAVNÝCH OPATŘENÍ
ROBOTIZACE, DIGITALIZACE, AUTOMATIZACE

COLORS OF AUDIT
COLORS OF AUDIT
COLORS OF AUDIT
žhavá témata 2019

ČIIA ČESKÝ INSTITUT INTERNÍCH AUDITORŮ | IIA The Institute of Internal Auditors

23.—24. 10. 2019 | OSTRAVA, HOTEL CLARION

WWW.INTERNIAUDIT.CZ

Vážené čtenářky, vážení čtenáři,

stále aktuální problematika kybernetické bezpečnosti, ke které se vrací toto číslo pod tématem „Kybernetická bezpečnost nejen očima interního auditora“, nás jen tak neopustí. Význam stále poroste. Časopis Interní auditor se tématu kybernetické bezpečnosti již delší dobu věnuje. Z předchozích čísel časopisu se této problematiky dotkly například články v číslech 3/2016, 4/2016, 2/2017 a 4/2017. Články se v podstatě zabývaly zákonem o kybernetické bezpečnosti a povinnostmi z něj vyplývajícími, bezpečnostními opatřeními podle tohoto zákona, audity kybernetické bezpečnosti.

Číslo, kterým nyní listujete, přináší v rámci tématu mimo jiné informace o praktické implementaci požadavků plynoucích ze zákona, přípravě na ni, reálných úskalích a efektech, se kterými se můžete v praxi setkávat. Této problematice se v poslední době věnovaly rovněž i některé akce, které Český institut interních auditorů pořádal. O nich vás v tomto vydání také informujeme.

V čísle najdete rovněž rozhovor v anglickém jazyce s Paulem J. Sobelem, který se dlouhodobě věnoval internímu auditu, risk managementu a v současné době je čelním představitelem COSO. Dále se můžete společně s autory zamyslet, zda jsou auditoři připraveni na očekávanou krizi a samozřejmě nechybí ani řada informací ze života ČIIA.

Pokud budete hledat starší čísla časopisu, tak nezapomeňte na jejich elektronickou formu. Od čísla 1/2008 najdete všechna na webových stránkách ČIIA.

Za redakční radu Vám přeji pěkné léto a dovolené dle vašich představ. ■

Jan Kovalčík
předseda redakční rady

Zveme Vás na odbornou akreditovanou konferenci

Název	Efektivní řízení územních samosprávných celků a jejich organizací
Pořadatel	Město Valašské Meziříčí a DYNATECH s.r.o.
Místo	Kino Svět Valašské Meziříčí, Nábřeží 268, 757 01 Valašské Meziříčí
Datum	Pá 20. 9. 2019
Čas	8:30 - 14:00
Akreditace	AK/VE-73/2019
Cena	1 200 Kč za osobu
Moderuje	Ing. Zdeněk Studeník, vedoucí finančního odboru Města Valašské Meziříčí
Anotace	Konference je zaměřena na legislativní novinky, vývojové trendy a sdílení dobré praxe v oblasti problematiky systému řízení veřejnoprávní korporace. Konference cílí na primátory, starosty, radní a zastupitele ÚSC, tajemníky, interní auditory a ekonomické pracovníky měst a obcí.
Přednáší	Mgr. **Radka Vladyková**, výkonná ředitelka Svazu měst a obcí ČR *Téma: "Dotace - příležitost, nebo past?"* JUDr. **David Bauer**, ředitel odboru 28 Ministerstva financí ČR *Téma: "Kde končí rozpočet a začíná účetnictví? - 1. část"* Ing. **Miroslav Matej**, Ph.D. ředitel odboru 12 Ministerstva financí ČR *Téma: "Kde končí rozpočet a začíná účetnictví? - 2. část"* Ing. **Michal Svoboda**, Ph.D., odbor Účetnictví a audit Ministerstva financí ČR *Téma: "Kolik stojí to, co dělám?"* Ing. **Jakub Bažant**, zástupce ředitele odboru 28 Ministerstva financí ČR *Téma: "Praktická ukázka získání informací z monitoru státní pokladny."* Ing. **Kamil Válek**, tajemník Města Uherský Brod *Téma: "Proč Město Uherský Brod získalo ocenění za inovaci v IA?"* Ing. **Martin Černý**, vedoucí ekonomického odboru Města Břeclav *Téma: "Zkušenosti z finančního řízení Města Břeclav"* Mgr. **Miloslav Kvapil**, Certifikovaný interní auditor ve veřejné správě *Téma: "Proč efektivně řídit veřejnoprávní korporaci?"* Mgr. **Emil Vařeka**, MBA - ředitel společnosti Icontio CR, s.r.o. *Téma: "Centrální správa požadavků veřejnoprávní korporace"*

Bližší informace a možnost přihlášení naleznete na internetových stránkách www.dynatech.cz

OBSAH / CONTENTS

ROČNÍK 23, ČÍSLO 2–2019 (92)

2|2019

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: casopis@interniaudit.cz
www.interniaudit.cz

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

Vydavatel nenese odpovědnost za údaje a názory autorů jednotlivých článků.
Redakční rada:
Vedoucí – Jan Kovalčík, Petr Hadrava, Daniel Häusler, Ludmila Jiráňová, Andrea Lukasíková, Šárka Nováková, Petra Škvorová, Eva Štěpánková, Lucie Veselá, Milena Widomská, Kateřina Zonygová

Foto: archiv ČIIA, fotobanka 123RF
Obálka: 123RF (tohey)
Neprodejné, určeno pro Český institut interních auditorů
Náklad: 1500 výtisků
Pre-press: Viktor Beránek
Tisk: REPRO servis s. r. o.
Distribuce: Mail Step a. s.

iA interní auditor

Praktické zkušenosti implementace administrativně organizačních opatření v Pražské teplárenské

Ing. Jakub Hlavica, MBA – finanční ředitel
Působí na pozici CFO v Pražské teplárenské a.s. a kromě financí, controllingu a účetnictví je odpovědný za oblast nákupu, IT a v neposlední řadě za řízení rizik a kybernetické bezpečnosti.

V České republice byl přijat Zákon o kybernetické bezpečnosti (dále jen ZoKB). Společnost Pražská teplárenská, přestože dosud nebyla určena povinnou osobou dle ZoKB, se již na možné určení dlouhodobě připravuje a postupně implementuje jednotlivé požadavky ZoKB a jeho prováděcích vyhlášek.

Ing. Josef Mynář
Působí na pozici Business Development Manager v konzultační firmě NETIA® s.r.o., je dodavatelem SW a služeb s orientací na projektové řízení, řízení rizik, interních auditů, implementaci požadavků kybernetické bezpečnosti a řešení GDPR / Data Protection Officer.

Zákazník

Pražská teplárenská a.s. byla založena v roce 1992 a svými aktivitami navazuje na tradici Elektrických podniků královského hlavního města Prahy, které byly založeny dne 1. září 1897.

Pražská teplárenská je z hlediska počtu provozovaných zařízení jednou z největších teplárenských společností v České republice. Aktivity společnosti jsou soustředěny na oblast hlavního města Prahy a přilehlých oblastí. V Praze pokrývá téměř 25 % trhu s tepelnou energií a dodává teplo pro více než 220 000 domácností, řadu administrativních budov, průmyslových podniků, stovky školských a zdravotnických zařízení a dalších subjektů.

Hlavním předmětem činnosti společnosti je výroba a rozvod tepelné energie.

Důležitým krokem pro podporu ekologického řízení společnosti bylo získání mezinárodního certifikátu pro systém ekologického řízení společnosti dle ČSN ISO 14001 společně se systémem řízení bezpečnosti a ochrany zdraví při práci dle ČSN OHSAS 18001, které Pražská teplárenská nadále udržuje a rozvíjí.

Název společnosti:	Pražská teplárenská a.s.
Sídlo:	Partyzánská 1/7, 170 00 Praha 7
Právní forma:	akciová společnost založená na dobu neurčitou
Identifikační číslo:	452 73 600
Společnost je zapsána:	Městský soud v Praze, spisová značka B 1509
Základní kapitál:	4 139 958 000 Kč
Datum vzniku:	1. května 1992

Zadání projektu

Postupná implementace požadavků ZoKB v prostředí společnosti Pražská teplárenská a.s.

V tomto článku se budeme věnovat implementaci v oblasti administrativně organizačních opatření – řízení aktiv a řízení rizik, včetně obsazení zákonem definovaných rolí.

V rámci implementace řízení rizik dle ZoKB se řešení rozšířilo i o řízení strategických rizik, které zpracovává a reportuje management pro představenstvo společnosti.

V oblasti řízení rizik se využívalo zpracování formou rozsáhlých excelových tabulek, které bylo náročné na koordinaci, bylo třeba velkého počtu schůzek pro zpracování a finalizaci rizik, a to jak rizik strategických, tak i kybernetických.

Komplikovaná pak byla zejména dokumentace nápravných opatření vyplývajících ze zpracovaných analýz rizik.

Společnost se rozhodla najít odpovídající SW nástroj, který by tyto oblasti podpořil a zajistil potřebnou SW podporu.

Jak implementovat požadavky zákona a vyhlášky o kybernetické bezpečnosti v utilitní společnosti?

Pokud tedy společnost patří pod ZoKB, má dobu jednoho roku na implementaci požadavků zákona. Z našich zkušeností je tato doba poměrně krátká pro splnění většiny podmínek ZoKB. Doporučujeme proto k implementaci použít projektový přístup a zákonem dotčené oblasti jako např. fyzická bezpečnost, IT bezpečnost atd. řešit jako několik paralelně běžících projektů.

Pro náš projekt se nám osvědčil následující postup:

- Definovat personální obsazení rolí ZoKB – manažer kybernetické bezpečnosti, správce aktiv, architekt kybernetické bezpečnosti, auditor kybernetické bezpečnosti, a to včetně přípravy interních směrnic a předpisů.
- Provést audit organizace dle ZoKB – provedení auditu, ze kterého vyjde, jaké administrativně organizační a technická opatření je nutné implementovat. Na základě auditu je možné stanovit personální a finanční požadavky na pokrytí ZoKB.
- Projekt – Administrativně organizační opatření, který zahrnuje přípravu a zpracování bezpečnostních politik dle ZoKB.

„Společnost se rozhodla najít odpovídající SW nástroj, který by tyto oblasti podpořil a zajistil potřebnou SW podporu.“

Projekt administrativně organizační opatření zahrnuje: řízení aktiv (provedení inventury aktiv a zpracování seznamu aktiv); řízení rizik (provedení analýzy rizik a nastavení systému řízení rizik); školení uživatelů (v souladu s plánem rozvoje bezpečnostního povědomí zajistí poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení).

Jednotlivé kroky implementace v Pražské teplárenské a.s.

1. krok – Obsazení rolí

„V rámci společnosti jsme se rozhodli nejdříve obsadit roli Manažera kybernetické bezpečnosti, a to výběrem vhodného kandidáta," říká p. J. Hlavica CFO PTAS. Tato role je pro úspěch celého projektu klíčová.

Ostatní role dle ZoKB (garanti aktiv, architekt kybernetické bezpečnosti) byly obsazeny z interních zdrojů. Samozřejmě po získání potřebných znalostí v oblasti kybernetické bezpečnosti, zejména se jednalo o proškolení v oblasti ZoKB, ISO 27000 a dalších odborných oblastech.

V případě auditora kybernetické bezpečnosti se také využilo interních možností a role se obsadila v podobě kolegyně z interního auditu. Díky tomu je zajištěná potřebná nezávislost ve vazbě na vlastní IT odbor a další odborné útvary společnosti.

2. krok – Audit organizace

Provedení úvodního auditu, jehož předmětem je zjištění shody s požadavky ZoKB, představuje první logický krok pro následnou implementaci jednotlivých technickoorganizačních opatření. V případě naší společnosti jsme prvotní audit realizovali ve spolupráci se společností Axenta. Díky výsledkům z auditu jsme kromě zjištění stávajících nedostatků získali i přehled o možném finančním dopadu a jednotlivé budoucí náklady jsme pak mohli časově rozvrhnout do několika dílčích investic.

3. krok – Projekt – Administrativně organizační opatření

Společnost Pražská teplárenská a.s. se pokusila najít na trhu SW řešení, které by pokrývalo námi zadané požadavky a procesy.

Požadavky na SW řešení byly:

- Jednoduchost.
- Garance správného postupu.
- Hlídání termínů.
- Automatická auditní stopa.
- Dostupnost v podobě vzdáleného přístupu.

Požadavky funkčnosti na SW byly:

- Popis a vizualizace procesů.
- Automatizace procesů.
- Správa dokumentace katalogu rizik.
- Uživatelské přehledy.
- E-mailové notifikace.
- Správa uživatelů, rolí a organizační struktury.

Podařilo se nám najít řešení od společnosti NETIA®, která měla takový produkt vytvořen na platformě TAS (výrobce Neit consulting) – TAS – KYBEZ. Po prezentacích se společnost rozhodla toto řešení implementovat.

Projet byl zahájen 1. října 2018 a celá implementace se uskutečnila do 3 měsíců.

V rámci projektu byl kladen velký důraz z vedení společnosti na zdárný průběh projektu –

byly vyčleněny požadované kapacity pro implementaci a celý projekt měl jednoznačnou podporu managementu společnosti.

Implementace SW řešení neprobíhala na zelené louce – společnost měla velmi dobře zpracovány interní metodiky a směrnice. Podle metodik došlo k parametrizaci a nastavení SW řešení. Je nutné říci, že neprobíhal žádný SW vývoj, protože platforma Team assistant – TAS je velmi univerzální a všechny požadavky se realizovaly pouze donastavením nad standardním produktem TAS – KYBEZ, pro specifika Pražské teplárenské. Proces řízení strategických rizik se nastavoval celý.

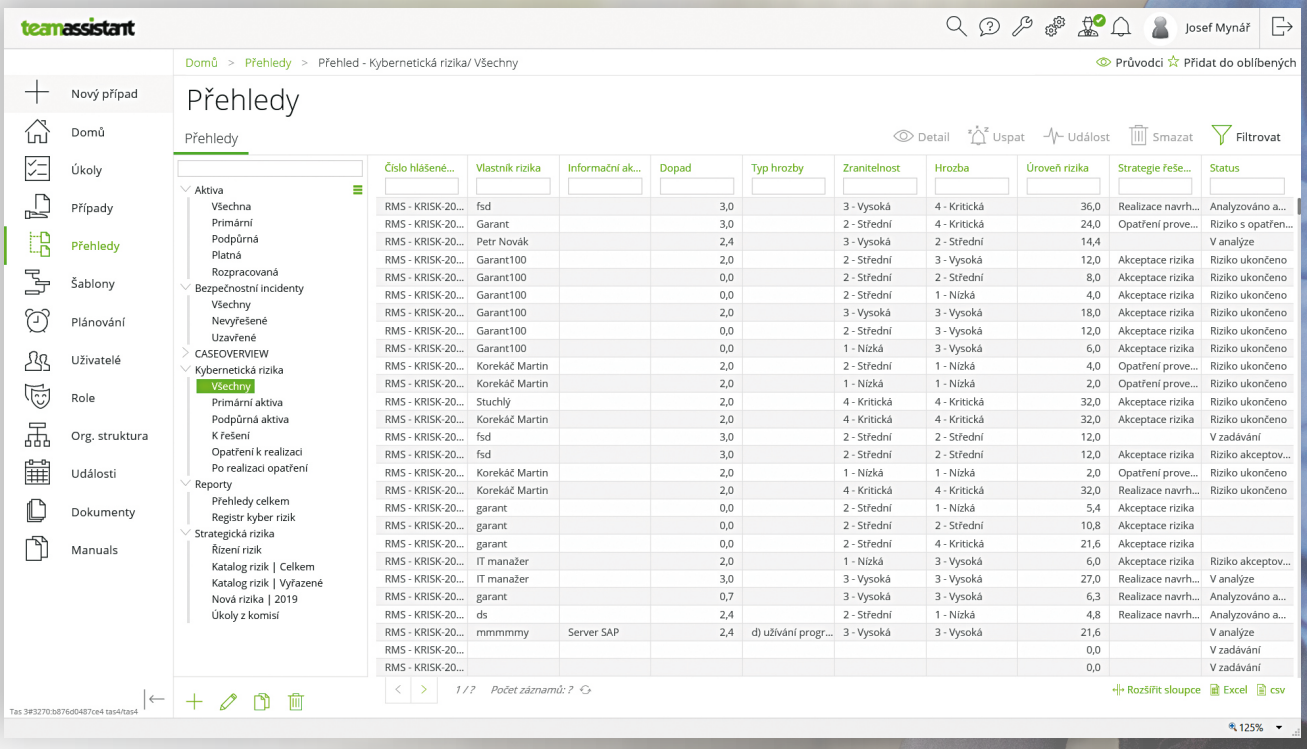
Řešení pro řízení rizik (dále jen RMT) je postaveno na platformě Team assistant. Z technického hlediska se jedná o moderní třívrstvou aplikaci s daty uloženými v relační databázi, aplikační serverovou vrstvou s moderní objektovou architekturou SOA s úplným přístupem prostřednictvím rozhraní webových služeb a klientskou přístupovou vrstvou ve formě webového prohlížeče. Samozřejmostí je autentifikace pomocí LDAP serverů (podpora i pro MS Active Directory).

nutnosti programování a vlastní prostředí pro běh a správu jednotlivých úkolů konkrétních instancí procesů. Napojení na jiné aplikace je možné prostřednictvím datové integrace (přímo jsou podporovány DB linky do obvyklých relačních databází a CSV souborové rozhraní) a prostřednictvím aplikační integrace (přímo je podporována integrace pomocí webových služeb).

„Pokud tedy společnost patří pod ZoKB, má dobu jednoho roku na implementaci požadavků zákona.“

Součástí aplikace Team assistant je nástroj na vlastní modelování procesů, tvorbu tzv. šablon procesů, aplikačních formulářů, tabulkových reportů a tiskových sestav bez

Pro grafický záznam workflow procesu je k dispozici modelovací nástroj s podporou BPMN 2.0.



***Společnost NETIA®** se zaměřuje především na tyto oblasti:*

Projektové řízení – SW Oracle – Primavera – dodávka licencí, školení a implementace, podpora BIM;

Řešení pokrytí Zákona o kybernetické bezpečnosti;

Řízení rizik a interních auditů – SW Risk manager tool – dodávky licencí, školení, implementace – cloudové řešení;

GDPR / Data Protection Officer – konzultace a zastupování firem a úřadů;

Oborová řešení pro řízení rizik – zdravotnictví, strojírenství, veřejná správa;

Řízení rizik – tvorba metodik a směrnic.

Pracovníci společnosti NETIA® s.r.o. mají rozsáhlé zkušenosti z mnohaletého působení v IT a realizace projektů v České a Slovenské republice.

www.netia.cz

Na konci implementace tedy byly v SW řešení pokryty tyto procesy:

- Řízení strategických rizik.
- Práce s incidenty (řízení a evidence incidentů).
- Řízení aktiv, práce s aktivy – primární, podpůrná.
- Řízení kybernetických rizik.
- Práce s hrozbami a protiopatřeními.
- Plány zvládání rizik.

Problematické oblasti:

Implementace požadavků ZoKB klade na každou společnost řadu požadavků, které společnost musí k naplnění zákona zajistit. Tyto požadavky mají dopad do procesů společnosti, ale nesmí mít dopad do hlavních činností společnosti.

Jedná se zejména:

- Personální obsazení – umístění do organizační struktury, odpovědnosti a kompetence.
- Nové interní dokumenty, směrnice, bezpečnostní politiky – jejich implementace do prostředí společnosti.
- Doplnění zavedeného způsobu řízení o řízení pomocí analýzy a řízení rizik, eliminace rizik – jedná se zcela nový přístup v rámci řízení společnosti.
- Proškolení zaměstnanců na požadavky ZoKB – jedná se o velký počet zaměstnanců.

Doporučení:

Po našich zkušenostech s implementací ZoKB je potřeba s přípravou začít co nejdříve, a to v podobě realistické analýzy rizik, která je základním vodítkem pro další kroky. Po rozhodnutí NUKIBu o tom, že společnost patří pod ZoKB, je čas na implementaci opatření pouze jeden rok a s ohledem na limitující parametry v podobě lidských zdrojů, finančních prostředků a v neposlední řadě i kapacitních možností dodavatelských firem se nemusí vše zvládnout v potřebném časovém horizontu.

Současný stav:

Implementace požadavků ZoKB je proces, který zasáhne celou společnost, a to nejenom delším heslem pro přihlášení k PC, ale celkovou změnou přístupu společnosti k oblasti kybernetických rizik. Vyhodnocování bezpečnostních událostí na každodenní bázi pak vede celou společnost k uvědomení o tom, že se za bezpečnostním perimetrem skutečně něco děje a že správná implementace požadavků ZoKB pomůže organizaci ochránit před případnými hrozbami, a to ve všech procesech organizace. Aby se celý proces implementace požadavků ZoKB zpřehlednil, je vhodné jej podpořit SW nástrojem, pro administrativně organizační opatření, např. *http://www.netia-it.cz/?q=cs/nase-reseni.*

Další možnosti rozvoje:

Vzhledem k tomu, že si společnost zvolila univerzální platformu TAS, tak implementací požadavků ZoKB celý proces nekončí a je dále možné platformu TAS rozvíjet. ■

Audit kybernetické bezpečnosti

Audit kybernetické bezpečnosti ověřuje činnosti v oblasti informačních a komunikačních systémů zaměřené na shodu s právními předpisy EU a ČR, vnitřními předpisy organizace a kontrolu hospodaření s prostředky v oblasti provozních výdajů a investic do zabezpečení informačních a komunikačních technologií. Právními předpisy EU jsou:

Mgr. Petr Švéda, CISM, CRISC, CISA, CISSP, CDPO
nezávislý konzultant a auditor.

- Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii;
- Prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný.

Právními předpisy ČR jsou:

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti);
- Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

Tyto právní předpisy jsou ze strany Národního úřadu pro kybernetickou a informační bezpečnost rozpracovány do podpůrného vodítka v podobě auditního checklistu, jehož cílem je

poskytnout souhrnný rámec povinností pro jednotlivé typy subjektů dle požadavků.

Vnitřními předpisy organizace je zejména bezpečnostní politika – tj. soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv – a návazná bezpečnostní dokumentace. V rámci přípravy auditorských činností je třeba, aby auditorský tým přezkoumal platné vnitřní předpisy organizace. Na základě provedené analýzy rizik a podpůrného vodítka auditorský tým identifikuje jednotlivé body kontrolního dotazníku, který bude použit pro ověřování skutečností v rámci prováděného auditu kybernetické bezpečnosti v organizaci.

Při výběru vzorků a jejich ověřování v rámci auditu kybernetické bezpečnosti je třeba dbát i na souvislosti z hlediska Demingova cyklu PDCA. Samotná existence v podobě předloženého dokumentu Zpráva o hodnocení rizik negarantuje, že organizace plně řídí rizika v souladu s požadavky vyhlášky o kybernetické bezpečnosti. Je třeba ověřit, že organizace má pro auditované systémy podléhající zákonu o kybernetické bezpečnosti vypracováno odpovídající Prohlášení o aplikovatelnosti, které obsahuje přehled aplikovaných a vyloučených opatření dle vyhlášky o kybernetické bezpečnosti s ohledem na Zprávu o hodnocení rizik. Rovněž je třeba ověřit, že opatření pro identifikovaná rizika ze Zprávy o hodnocení rizik jsou zahrnuta v revidovaném Plánu zvládání rizik. Na základě Plánu zvládání rizik je rovněž třeba ověřit i sledování a pravidelné přezkoumání rizik. Auditorský tým v rámci auditu kybernetické bezpečnosti na vzorku rizik ověřuje křížovou kontrolou, že jsou v jednotlivých předložených dokumentech relevantní informace.

Trendy a změny legislativy a standardů?

Novelizace legislativy v loňském roce zrušila původní terminologickou nejednotnost „kontrol“ pro významné informační systémy a rovněž se jedná o audit. Rovněž jsou explicitně doplněny požadavky na rozsah a frekvenci auditu:

- v pravidelných intervalech nejméně po 3 letech v případě správců a provozovatelů významných informačních systémů;
- v pravidelných intervalech nejméně po 2 letech v případě správců a provozovatelů kritických informačních systémů;
- a při významných změnách v rámci jejich rozsahu.

Explicitní doplnění požadavků opomenulo komunikační systémy, základní služby a digitální služby. V tomto směru dle podpůrného vodítka platí pro komunikační systémy a základní služby totožné ustanovení jako pro správce a provozovatele kritických informačních systémů. Není-li možné v odůvodněných případech audit v uvedených intervalech v celém rozsahu provést, je možné realizovat jej po systematických celcích. Systematické celky musejí pokrýt celý rozsah nejpozději do pěti let. Nově legislativa zakotvuje pro provozovatele povinnost předkládat výsledky auditu kybernetické bezpečnosti správci.

„Je třeba dbát i na souvislosti z hlediska Demingova cyklu PDCA.“

Minimální podmínky na osobu auditora kybernetické bezpečnosti, která nezávisle hodnotí správnost a účinnost zavedených bezpečnostních opatření, nově legislativa snižuje. Zejména ustanovení, kdy jsou dva roky prokázání odborné způsobilosti praxí s prováděním auditů kybernetické bezpečnosti nebo auditů systému řízení bezpečnosti informací nahrazeny vysokoškolským vzděláním, se jeví jako spíše nereálné. Jedná se však o minimální požadavky a organizace má možnost

stanovit nároky vyšší. Z hlediska postupů a vodítek pro samotný audit kybernetické bezpečnosti, novelizace platné legislativy v minulém roce žádné změny nepřináší. Je třeba uplatnit zásady dle Mezinárodních standardů pro profesní praxi interního auditu a platných českých technických norem. A to zejména ČSN EN ISO 19011 Směrnice pro auditování systémů managementu, jejíž nové vydání s účinností od 02/2019 přináší tyto změny:

- rozšíření principů auditování o přístup založený na rizicích;
- rozšíření návodu k řízení programu auditů, včetně rizik programu auditů;
- rozšíření návodu k provádění auditu, zejména v části plánování auditu;
- rozšíření požadavků na obecné kompetence auditorů;
- úprava terminologie ve smyslu procesu;
- odstranění přílohy obsahující požadavky na kompetence pro auditování specifických oborů systémů managementu (z důvodu velkého množství jednotlivých norem systémů managementu by bylo nepraktické zahrnout požadavky na kompetence pro všechny obory);
- rozšíření přílohy A, aby poskytovala návod k auditování (nových) konceptů, jako je kontext organizace, vedení a závazek, virtuální audity, soulad se závaznými povinnostmi a dodavatelský řetězec.

A problémy v praxi?

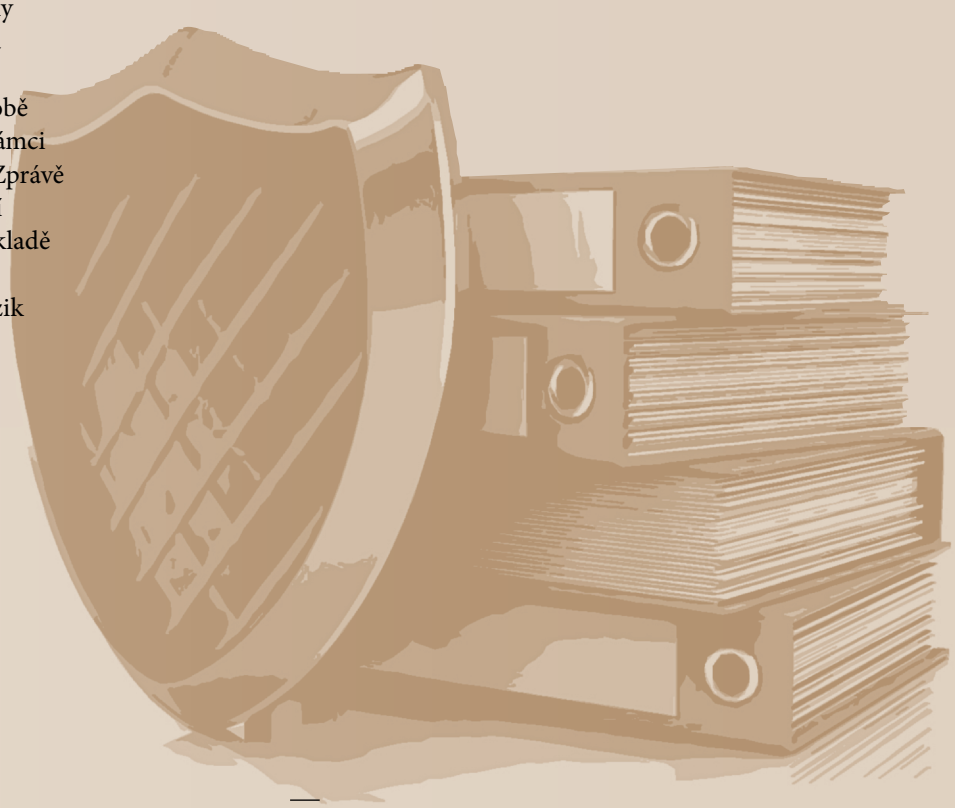
Základním problémem v praxi však zůstávají specifické znalosti, které souvisí s oblastí zabezpečení informačních a komunikačních technologií. A to zejména s ohledem na kontext auditovaného subjektu a jemu příslušné organizace. Stejného výsledku lze dosáhnout při aplikaci různých bezpečnostních opatření a to mnohdy s výrazně odlišnými náklady. Nelze snadno

„Problémem v praxi však zůstávají specifické znalosti.“

a již vůbec ne obecně hodnotit, zdali je auditovaným subjektem zvolené bezpečnostní opatření horší než některé alternativní. Je pouze hodnocena účinnost a efektivnost, a to s ohledem na kontext organizace. Pro tento účel je možné do auditorského týmu v případě potřeby doplnit technické experty, kteří poskytují specifické znalosti či odborné posudky. Tito techničtí experti mají pracovat pod vedením auditora – nejednají a nevystupují v týmu jako auditoři. Auditor má být vždy schopen pochopit a zvážit názory expertů.

Znalosti experta v auditorském týmu jsou v praxi potřeba již v rámci přípravy programu auditu. S ohledem na rizikově orientovaný přístup je při přípravě programu auditu nutné definovat kritéria pro výběr vzorků. A v ideálním případě tak, aby bylo možné ověřit i souvislosti z hlediska Demingova cyklu PDCA, například:

- Přístupová oprávnění uživatelů jsou odpovídajícím způsobem definována vnitřními předpisy a přidělována v jejich souladu na základě platného organizačního řádu či katalogu pracovních pozic, které vymezují činnosti vykonávané danými uživateli. Změna respektive odebírání přístupových oprávnění a rolí pro jednotlivé uživatele je v souladu s vnitřními předpisy realizováno bezprostředně v okamžiku změny pracovní pozice, respektive ukončení pracovně pracovního či služebního poměru. A k jednotlivým změnám existují příslušné schválené požadavky na změny. V rámci kontroly jsou systematicky automatizovaným nástrojem či manuální kontrolou ověřovány aktuálně přidělená přístupová oprávnění. Identifikované rozdíly jsou evidovány v podobě bezpečnostních událostí a v rámci přezkoumání zohledněny ve Zprávě z přezkoumání systému řízení bezpečnosti informací. Na základě výsledků přezkoumání je pak aktualizován Plán zvládání rizik na následující období.
- Dvou či vícefaktorová autentizace je v souladu s vnitřními předpisy vynucována pro všechny uživatele (ať již s využitím tradičních čipových karet vydávaných organizací či prostřednictvím notifikací či hesel zasílaných na mobilní telefon uživatele). Pro odůvodněné případy existují řádně schválené záznamy o výjimkách. O jednotlivých provedených autentizacích jsou vytvářeny relevantní bezpečnostní záznamy. Jsou definovány a důsledně aplikovány postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu. Záznamy o bezpečnostních incidentech jsou v rámci přezkoumání zohledněny ve Zprávě z přezkoumání systému řízení bezpečnosti informací. Na základě výsledků přezkoumání je pak aktualizován Plán rozvoje bezpečnostního povědomí na následující období.
- Organizace má definovánu platnou bezpečnostní strategii, která je v souladu s aktuálními obchodními cíli a dalšími strategickými dokumenty. Platné vnitřní předpisy jsou efektivně vymahatelné pro zaměstnance i externí dodavatele. Jejich aktuální podoba je komunikována odpovídajícím způsobem, který lze nezávisle ověřit (záznamy o školení, historie publikovaných dokumentů na intranetu atp.). Jsou definovány a důsledně aplikovány postupy pro disciplinární řízení při porušení stanovených pravidel. O výsledcích disciplinárních řízení jsou vedeny záznamy, které jsou vyhodnocovány v rámci přezkoumání ve Zprávě z přezkoumání systému řízení bezpečnosti informací. Na základě přezkoumání je pak aktualizován Plán zvládání rizik a Plán rozvoje bezpečnostního povědomí na následující období. ■



Audit kybernetické bezpečnosti – izolovaná disciplína?

Ing. Aleš Špidla,
Manažer kybernetické bezpečnosti
Generální finanční ředitelství
Prezident Českého institutu manažerů informační bezpečnosti

Kybernetická bezpečnost, a vlastně lépe kybernetická a informační bezpečnost, je slovní spojení, které zní naším světem čím dál tím hlasitěji. Promořenost tohoto světa informačními a komunikačními technologiemi (ICT) roste po exponenciální křivce. Zvykli jsme si na tyto technologie tak, že některé činnosti a schopnosti jsme jim úplně předali. Kolik si pamatujete telefonních čísel? Před érou mobilních telefonů jsem si takovýchto čísel pamatoval nejméně padesát. Teď mám problém se svým vlastním. Ale nejde jen o zapamatování si telefonních čísel. ICT vstupuje do procesů, které řídí výrobní technologie, finanční služby, dopravu, distribuci elektrické energie, státní správu, zbraně a mnoho dalších.

Někdy ICT vstupují do procesu řízení přímo, někdy zprostředkovaně tím, že poskytují lidem informace pro řízení. A v tom je často ten problém. Informace. Informace zvyšuje u příjemce míru jistoty. Tedy pokud je pravdivá. Informace má zásadní vliv na kvalitu rozhodování. Abychom se na informaci mohli spolehnout, musí být zajištěny základní bezpečnostní atributy. To, co teď napíšu o informacích, samozřejmě platí i pro celé systémy nebo služby. Musí být zajištěna důvěrnost (D) informací což znamená, že k informaci se dostane (nebo systém může použít) pouze ten, kdo má k tomu oprávnění na základě své role v systému a je jedno, jestli se jedná o člověka, nebo o stroj. Přístup je umožněn na základě zásady need to know. Informace (systém) musí mít dále zachovánu integritu (I), to znamená, že se můžeme spolehnout na její obsah, že ji nikdo nezfalšoval, že chování systému nevede ke generování dezinformací. A poslední z triády atributů je dostupnost (D), což lze vysvětlit tak, že oprávněná osoba (systém) má k dispozici spolehlivé informace v okamžiku, kdy je potřebuje. Představte si nemocnici kdekoliv ve světě. Hackerům se podařilo proniknout do nemocničního informačního systému a zašifrovat jeho databázi. V čekárnách se hromadili pacienti a lékaři nevěděli co s nimi, protože se nemohli dostat k informacím, které pro správnou léčbu potřebovali. Který nebo které ze tří výše uvedených atributů byly narušeny? Odpověď je velmi jednoduchá – všechny.

Důvěrnost – hackeři se dostali do systému, ve kterém neměli co dělat. Integrita – hackeři zašifrováním změnili podobu databáze a Dostupnost – lékaři se nedostali k informacím, které potřebovali ke své práci. Stejně fatální následky jako žádné informace můžou mít zkreslené nebo podvržené informace. Na příkladu nemocnice si můžeme představit, co se stane, když hackeři napadnou nemocniční informační systém a u vybraných zájmových osob změní medikaci. Rozhodnutí na základě těchto údajů může mít fatální následky. Z jiné oblasti je znám případ, kdy hackeři ovládli systém pro dávkování chemikálií do pitné vody. Přístroje hlásily, že je vše v pořádku a dispečeři přijali na základě těchto informací to nejhorší rozhodnutí – nedělat nic. Ještě než se dostaneme k auditu, si dovolím zdůraznit ještě jeden aspekt ICT. Kromě toho, že ICT je nástrojem pro zvyšování efektivity a přesnosti našeho rozhodování (hovořím o bezpečném ICT) je z mého pohledu bezpečnostního profesionála základní integrační platformou, na které se buduje bezpečnostní kultura instituce. V podstatě všechny typy bezpečnosti od BOZP, požární ochrany, objektové bezpečnosti, fyzické bezpečnosti, informační bezpečnosti, ochrany osobních údajů apod. se sbíhají v nějakém ICT. Bezpečné ICT je tedy prvkem bezpečnostní kultury instituce a zároveň předpokladem pro její správné fungování.
A pokud není zajištěna bezpečnost této platformy, tak se může celá bezpečnostní kultura zbortit.
Co se týká kybernetické a informační bezpečnosti, má Česká republika poměrně příznivou legislativní situaci, protože od roku 2014 máme speciální zákon o kybernetické bezpečnost 181/2014 Sb. Zákon ukládá mimo jiné osobám povinným provádět pravidelně audit kybernetické bezpečnosti. Pro samotný audit je důležitá znalost vyhlášky 316/2014 Sb. resp. její novely 82/2018 Sb., (Vyhláška o kybernetické bezpečnosti). Tomu, kdo zná rodinu norem ISO 27000, jistě neunikne to, že se autoři vyhlášky o kybernetické bezpečnosti nechali touto normou poměrně výrazně inspirovat. Audit kybernetické bezpečnosti je vlastně jako každý jiný audit posouzením shody s touto vyhláškou. Z vlastních zkušeností vím, že je dobré udělat si celkový přehled o tom, jak z pohledu kybernetické a informační bezpečnosti, na tom vlastně je. Prvotní posouzení by se nemělo zaměřit na oddělené oblasti a mělo by vytvořit celkový přehled. A nemusí to být rovnou audit. Při budování bezpečnosti je totiž nejdůležitější přestat si lhát. Pokud si neuděláte přehled o tom, jak na tom jste, tak nemůžete přijímat správná rozhodnutí a čeká vás cesta do pekla. Ale zpět k auditu. Gestorem kybernetické bezpečnosti je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), ten na svých stránkách zveřejnil Pomůcku pro audit kybernetické bezpečnosti, a to jak pro vyhlášku 316/2014 Sb., tak i pro vyhlášku 82/2018 Sb. Zkušenosti s kontrolou, kterou provádějí u osob povinných pracovníci NÚKIB ukazují, že tyto pomůcky nebo chcete-li checklisty, jsou intenzivně využívány. I když kontrola nepostupuje bod po bodu, tak oblasti jsou vhodně voleny tak, že poskytnou poměrně dobrý přehled o tom, jak na tom instituce je. A že dosavadní kontroly ve státní správě nic moc lichotivého neukázaly.

„Informace má zásadní vliv na kvalitu rozhodování.“

A jak je to s tou izolovaností? O integrující úloze ICT už jsem hovořil, takže audit jednotlivých oblastí bezpečnosti se bez auditu kybernetické (i když bezděčném) neobejde. Vezměme si například ochranu osobních údajů. Populární nařízení GDPR ve svém článku č.32 hovoří o tom, že správce nebo zpracovatel osobních údajů musí zajistit důvěrnost, integritu, dostupnost a odolnost systémů, ve kterých jsou osobní údaje zpracovávány. Tady jasně vidíme propojení na základní triádu kybernetické a informační bezpečnosti. Odolnost autoři přidali pro mě z nepochopitelných důvodů, protože je zajištěna zabezpečením této triády. 95 % osobních údajů je zpracovávána v informačních systémech. Audit ochrany osobních údajů bez průniku s kybernetickou a informační bezpečností je nonsens. Zkusme příklad z jiného soudku – finanční audit. Ekonomický informační systém obsahuje veškeré informace, které jsou tímto auditem auditovány. Jak se může ale auditor spolehnout na informace v něm uložené, když není správně nastaven systém pro přidělování přístupových oprávnění, když administrátoři mají neomezená práva v neslučitelných kombinacích? To prostě nejde, takže auditor musí vnímat i takovéto průniky. A proto si myslím, že audit kybernetické bezpečnosti není oddělenou disciplínou, a tak jak více a více pronikají informační a komunikační technologie do našich životů, tak proniká audit kybernetické bezpečnosti do interního auditu celé instituce a posiluje jeho komplexnost. Protože i auditor pro své rozhodování potřebuje informace, u kterých byla zajištěna Důvěrnost, Dostupnost a Integrita.

KYBERPROSTOR aneb když se hovoří o věci mimo chápání většiny z nás

Milan Zolich
vedoucí oddělení interního auditu, Ministerstvo spravedlnosti ČR

Letošní workshop pro interní auditory z veřejné správy se nesl v duchu „jedniček a nul".

Již sám název „Daatování aneb práce s daty nuda je, má však cenné údaje" navozoval u účastníků stav očekávání co z těch „jedniček a nul" vlastně vyplyne.

Jednou z částí nabitého programu byla i panelová diskuze zaměřená na oblast kybernetické bezpečnosti. Aby téma nebylo pouze suchopárné, zvolili organizátoři diskuze širší téma, a to téma KYBERPROSTOR. Cílem tedy nebyla jen debata nad kyberbezpečností, ale v širším kontextu se diskutující zaměřili na pochopení toho, co vlastně kybernetickou bezpečností je, jak je vnímán širokou veřejností a jak se v něm pohybovat, abychom neuvízli v bažině elektromagnetického spektra.

Termín „Kyberprostor" (Cyberspace) použil na počátku 80. let v povídce „Jak vypálit Chrom" W. Gibson a charakterizoval jej jako *„konsenzuální datovou halucinaci, vizualizovanou v podobě imaginárního prostoru, tvořeného počítačovými daty, která nám nabízí mnohem lákavější představu o prostoru, čase nebo skutečnosti, než je ta, ve které reálně žijeme"*.

V úvodní přednášce nás **Mgr. Vladimír Rohel** zavedl právě do tohoto imaginárního prostoru. Asi jsme se všichni podivovali, co vše se pod pojmem „kyberprostor" skrývá. Byli jsme konfrontováni se skutečností, že i chytré domácí spotřebiče (televize, kávovar, lednice…) je možné zahrnout do kyberprostoru. Mnohému z nás vyvstala na mysli možnost, že nás přestane „poslouchat" lednice nebo kávovar. Byli jsme však uklidněni, že tato možnost se „zatím" pohybuje v teoretické rovině.

Abychom však nezůstali pouze v rovině kyberprostoru, v druhé části přednášky se přednášející

zaměřil na problém kritické informační infrastruktury a významných informačních systémů. Což nás celkem uklidnilo, neboť naše domácnosti nebyly v této části zmíněny.

Ve druhé části panelové diskuze jsme se zaměřili na problematiku rolí dle zákona o kybernetické bezpečnosti. **Ing. Petr Grešl** rozebral problémy orgánů veřejné správy při stanovování odpovědnosti za jednotlivé oblasti ochrany informačních systémů. Mnozí z nás pocítili mrazení při popisu odpovědností jednotlivých rolí. Ještě, že jsme interní auditoři, myslel si mnohý z nás. To je však mylná myšlenka.

Při auditu plnění úkolů dle zákona o kybernetické bezpečnosti se budeme, jako interní auditoři, potýkat se znalostmi všech rolí a hodnotit naplnění jejich povinností, tudíž žádná „selanka".

Pojďme však do reálného stavu. Ve třetí části diskuze vystoupil **Ing. Dominik Marek**. Tato část byla zařazena jako obraz reálného stavu na jednom krajském úřadu a jako příklad dobré praxe. Diskutující nás seznámil s tím, jak kybernetickou bezpečnost řeší na krajském úřadu, a mimo jiné i s dokumentací, která musí být vedena dle zákona o kybernetické bezpečnosti. Při pohledu na narůstající stohy dokumentace (vizuálně znázorněno při prezentaci) mnohým z nás „naskočila husí kůže". Když se vrátím k předchozí části diskuze, pak před interními auditory stojí velká výzva. Nejenom znalost zákonů a vyhlášek, rolí v oblasti zabezpečení kybernetické bezpečnosti, ale i dokumentace (papíry a papíry a papíry nebo data a data a data).

A nebyl by to workshop pro interní auditory, kdyby se neprobralo i téma kontroly plnění úkolů dle zákona o kybernetické bezpečnosti. Tohoto úkolu se ujmul **Ing. Aleš Špidla**.

Ve svém vystoupení se zaměřil na praktickou stránku auditu (kontroly) této oblasti, to je plánování a příprava, včetně studia dokumentace, přípravy podkladů pro interview.

Byly prezentovány nejčastější zjištění kontrolních orgánů při kontrole zajištění kybernetické bezpečnosti. S humorem sobě vlastním provedl rozbor jednotlivých negativních zjištění a celou diskuzi zakončil

Tato část byla vysoce ceněna posluchači, jako orientace a zaměření při vlastní auditní (kontrolní) činnosti.

Aby nebyla pozapomenuta vlastní diskuze nad jednotlivými tématy. Po jednotlivých vystoupeních následovala rozsáhlá debata, která pokračovala i na závěr celé panelové diskuze. A pokud bychom hodili za hlavu časový rozvrh workshopu, tak se diskutuje celý jednací den.

Že je popis panelové diskuze velmi stručný? O problému kybernetické bezpečnosti by se dalo psát a nad tématem diskutovat dlouhé hodiny. Účastníci workshopu jistě ocenili profesionalitu vystupujících (diskutujících) i atmosféru, ve které panelová diskuze probíhala.

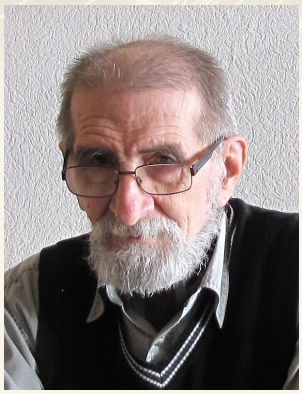
A pokud chcete více? Přijďte příště mezi nás. Třeba na jiné téma a v jiném prostředí, nicméně „více hlav, více ví".

A ukončíme metaforou:

„Kyberprostor jako ráj, tedy místo bez hranic, otevřené všem bez ohledu na rasu či národnost, obývané entitami bez těla, příslib nesmrtelnosti."

Panelová diskuze, Workshop ČIIA, Hradec Králové 2019

Z virtuálního prostoru až do nejvyšších pater politiky



PhDr. Václav Peřich, člen Čestného prezidia ČIIA od roku 1996

„Nesmíme přitom podléhat dojmu, že péče o bezpečnost v této oblasti je pouze v působnosti IT odborníků, techniků a specialistů na kódování.“

Málokdo by asi vznášel námitky proti aktuálnosti tématu, jemuž je věnováno právě toto číslo Interního auditora. Nemohu si nicméně odpustit poznámku, že jsme při volbě zaměření tohoto čísla nejspíš netušili, jak vysoce naléhavým se právě v těchto týdnech a měsících otázky kybernetické bezpečnosti stanou. Nemohu se k tomu vyjadřovat z nějakých zasvěceně odborných pozic, to musím přenechat povolanějším. Na druhé straně je však někdy účelné u složitějších problémů dát zaznít hlasu těch, kdo se dané specializaci sice nevěnují soustavně, kdo však na vlastní kůži zažili onen vpád digitálního světa do dnešní každodennosti. Pravda, nejsem pamětníkem dob, kdy ještě žádné počítače nebyly, avšak ještě poměrně nedávno byl počítačový svět dost zřetelně oddělen od toho „reálného“. Svět mimořádně složitých vědeckotechnických výpočtů a zpracování rozsáhlých souborů dat se vyznačoval též striktním oddělením prostor, používáním kódovaných nosičů dat a rychlým nárůstem výskytu tajuplných a imponujících strojů. Určité přemostění mezi oběma světy obstarávali respektovaní matematici, analytici usilující o modelování k tomu vhodných činností a samozřejmě také vizionářští autoři vědecko-fantastické literatury. Bylo to poutavé, lákavé a doprovázené takřka překotně rychlým technickým vývojem. Stačilo několik desetiletí a ostrovy tohoto digitálního světa se vytvořily téměř ve všech významnějších odvětvích – a stále se rozrůstaly a postupně přebíraly další a složitější úkoly od řízení technologických linek až po simulace postupů potřebných třeba k výcviku pilotů či kosmonautů. Přibývalo také způsobů propojení takových ostrovů a možností, jak využívat synergie z toho vyrůstající.

Velká část světa se proměnila. A tak, jako chodec procházející rušným velkoměstem musí počítat nejen s rychlostí a různorodostí dopravy, nýbrž i s nástrahami probíhajících stavebních prací, s manévry nezodpovědných řidičů a všudypřítomností pouliční zločinnosti, musí každý z nás v nějaké míře počítat s tím, že nás tu a tam může zaskočit cokoli z narušení té části našeho pobývání na světě, která je svěřena či podřízena režimu nul a jedniček. Nesmíme přitom podléhat dojmu, že péče o bezpečnost v této oblasti je pouze v působnosti IT odborníků, techniků a specialistů na kódování.

Jistě, jejich úloha při zajišťování kybernetické bezpečnosti je klíčová a zcela nezastupitelná, ale obdobně důležité je také odpovědné chování nás všech ostatních. Rádi využíváme výhod nákupů v e-shopech, systémů rezervace letenek, přístupu ke globálním zdrojům informací a zábavy, zdaleka ne vždy si však přitom počínáme s náležitou obezřetností. Jednou se necháme zlákat neodolatelnou slevou k zakoupení úžasného udělátka od e-shopu „U bílého koně“, jindy nás rozohní alarmující foto s titulkem ohlašujícím konec starého světa. Námětů a příležitostí bezstarostně naletět podvodníkovi či pozvat do vlastního soukromí trojského koně je doslova nepočítaně.

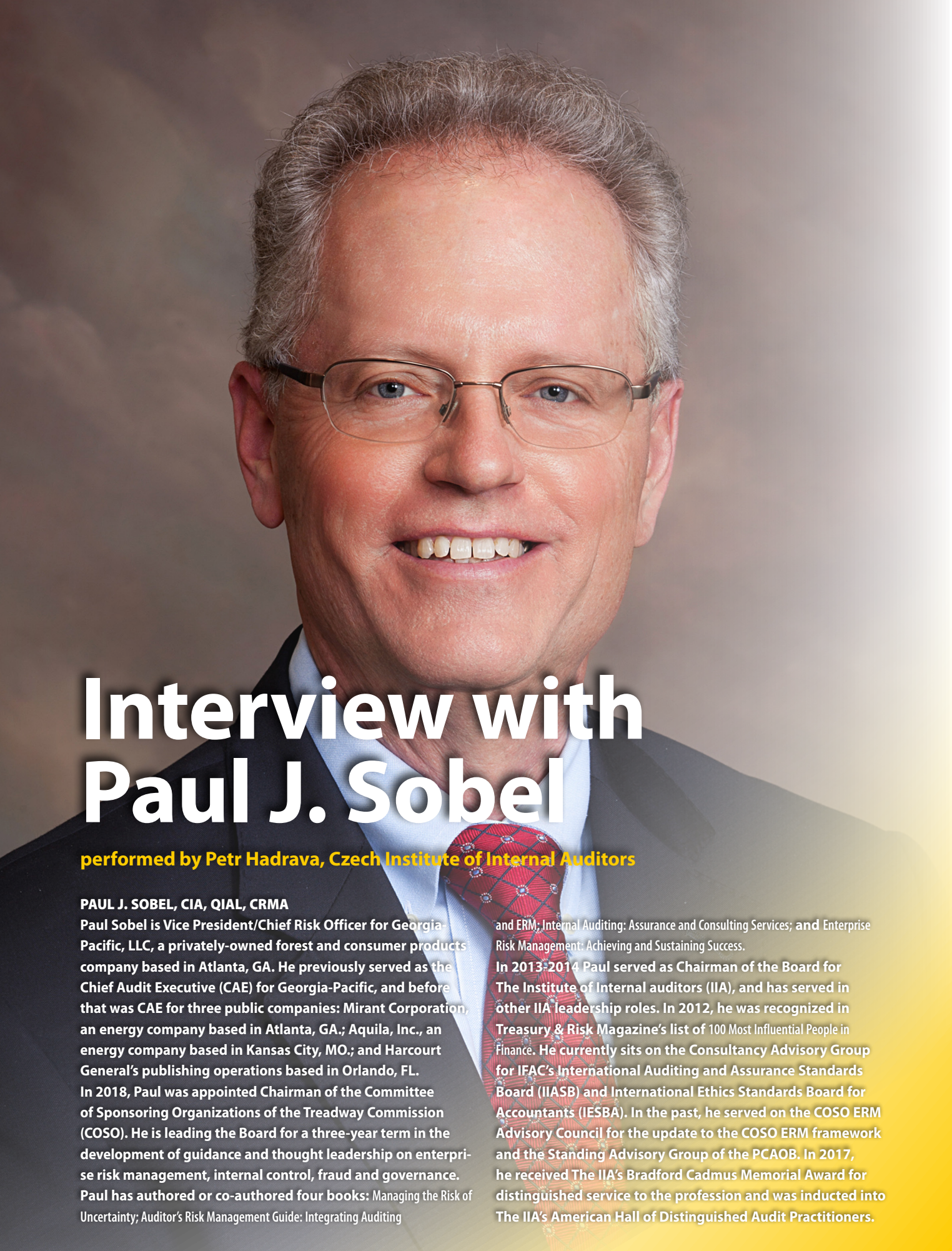
„Důležité je také odpovědné chování nás všech ostatních.“

Ale dokud jednáme jen sami za sebe, zdaleka to ještě není ten opravdový mumraj, jaký se odehrává v nejrůznějších typech organizačního prostředí. Vystupujeme a jednáme jako podnikatelé, živnostníci, činovníci a funkcionáři spolků, stran a odborových organizací, zaměstnanci veřejné správy, vědci, výzkumníci, učitelé, vojáci i policisté a také jako zaměstnanci veškeré korporátní sféry. S tím jsou však zpravidla spojeny rozmanité role uživatelů informačních systémů či zpracovatelů dat v působnostech těch institucí, s nimiž jsme propojeni. A v těchto rolích jsme chtě nechtě nositeli spoluodpovědnosti nejenom za náležité zacházení se svěřenou technikou, ale také za zabezpečení ochrany dat, s nimiž pracujeme, a za předcházení všem druhům komunikačních incidentů. Všude tam, kde se v informačních systémech organizací potkávají chráněně zdroje firemních uživatelských systémů a dat s internetovou sítí www, může docházet k těžko předvídatelným střetům mezi vnitřní ochranou a mezi nezodpovědným jednáním některých uživatelů. A vůbec nejde jen o ochranu před vnějšími útoky. Někteří uživatelé totiž z netrpělivosti či v časové tísni obcházejí bezpečnostní pravidla a i zcela služební záležitosti „vyřizují“ po „soukromé“ osobní linii, přičemž takto získané externí zdroje následně zapojují do své služební agendy, aniž by je podrobili náležité bezpečnostní analýze. Snad nejslavnějším příkladem takového jednání jsou úniky e-mailů někdejší prezidentské kandidátky Hillary Clintonové z roku 2016 a členů jejího volebního štábu.

Když už jsem zmínil tak svrchovaně politickou souvislost s naším tématem, musím postoupit ještě o další krok dál. Kybernetická bezpečnost není zvažována jen u těch systémů, které jsou aktuálně provozovány nebo budovány. Musí být velmi vážně posuzována u všech důležitých investičních rozhodnutí, jejichž důsledky se mohou projevovat po delší časové období, zejména když se jedná o infrastrukturní projekty typu řízení telekomunikačních, dopravních nebo energetických systémů. A zde narážíme na onu vystupňovanou aktuálnost debat o budování komunikačních sítí páté generace. Z hlediska sektorů ekonomiky půjde o korporátní investory v nestátním vlastnictví, ale ti budou muset získat pronájem kmitočtů od státního orgánu. Jak však má takový státní orgán stanovit podmínky pro uchazeče o licenci k provozování, když uplatnění čistě cenových a výkonových hledisek nemusí dostatečně zohledňovat bezpečnostní rizika vyplývající z možnosti podřídit některé technologické dodávky zájmům cizího státu? Na konci dubna a na začátku května letošního roku shodou okolností proběhly dvě události, které sice na tuto otázku nepřinesly odpověď, ale vyzdvihly její důležitost. Ve Spojeném království bylo 25. dubna zahájeno vyšetřování úniku informací z tajné porady NSC (Rada národní bezpečnosti) právě o tomto problému. Nikoli přímým výsledkem tohoto vyšetřování, avšak v jasné souvztažnosti s ním, bylo odvolání ministra obrany z vlády Spojeného království dne 1. května. Nezávisle na tom byla následujícího dne na pražském MZV zahájena dvoudenní konference 150 účastníků z více než 30 zemí světa,

„Námětů a příležitostí bezstarostně naletět podvodníkovi či pozvat do vlastního soukromí trojského koně je doslova nepočítaně.“

která se zabývala bezpečnostními aspekty budování sítí 5G. Účastníci konference se shodli na tom, že na bezpečnost v kyberprostoru by se nemělo nahlížet jako na čistě technickou záležitost a že je nutno brát v potaz „všechny relevantní faktory, včetně aplikovatelnosti práva a dalších aspektů dodavatelova prostředí“. To se samozřejmě týká nás všech, a proto bychom také měli všichni pozorně sledovat nadcházející vývoj.



Interview with Paul J. Sobel

performed by Petr Hadrava, Czech Institute of Internal Auditors

PAUL J. SOBEL, CIA, QIAL, CRMA

Paul Sobel is Vice President/Chief Risk Officer for Georgia-Pacific, LLC, a privately-owned forest and consumer products company based in Atlanta, GA. He previously served as the Chief Audit Executive (CAE) for Georgia-Pacific, and before that was CAE for three public companies: Mirant Corporation, an energy company based in Atlanta, GA.; Aquila, Inc., an energy company based in Kansas City, MO.; and Harcourt General's publishing operations based in Orlando, FL.

In 2018, Paul was appointed Chairman of the Committee of Sponsoring Organizations of the Treadway Commission (COSO). He is leading the Board for a three-year term in the development of guidance and thought leadership on enterprise risk management, internal control, fraud and governance. Paul has authored or co-authored four books: Managing the Risk of Uncertainty; Auditor's Risk Management Guide: Integrating Auditing and ERM; Internal Auditing: Assurance and Consulting Services; **and** Enterprise Risk Management: Achieving and Sustaining Success.

In 2013-2014 Paul served as Chairman of the Board for The Institute of Internal auditors (IIA), and has served in other IIA leadership roles. In 2012, he was recognized in Treasury & Risk Magazine's list of 100 Most Influential People in Finance**. He currently sits on the Consultancy Advisory Group for IFAC's International Auditing and Assurance Standards Board (IIASB) and International Ethics Standards Board for Accountants (IESBA). In the past, he served on the COSO ERM Advisory Council for the update to the COSO ERM framework and the Standing Advisory Group of the PCAOB. In 2017, he received The IIA's Bradford Cadmus Memorial Award for distinguished service to the profession and was inducted into The IIA's American Hall of Distinguished Audit Practitioners.**

Hi Paul, thank you for your willingness to spend some time with the readers of the Czech Internal Auditor Journal! I am sure your insight shared will be much appreciated.

Thanks for asking me; it's a pleasure to be given this opportunity.

Paul, you are the Chairman of COSO. Can you please tell us what COSO is and what is the purpose of this initiative?

COSO is short for the Committee of Sponsoring Organizations of the Treadway Commission. It has a long history dating back into the mid-1980s. It was established as a private sector initiative driven by incidents of fraudulent financial reporting at the time. The COSO Mission is to *provide thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations.*

COSO is issuing guidance in the area of Governance and Operational Performance, Internal Control, Enterprise Risk Management and Fraud Deterrence. Who is the intended recipient of this guidance and are the materials relevant to internal auditors? Can this be used by internal auditors during risk assessment exercise or during planning and/or executing audits? If yes, what is the most effective way for internal auditors to use the COSO materials?

As mentioned, enterprise risk management, internal control and fraud deterrence are the key focus areas in our Mission. Dealing with those focus areas effectively will help promote good governance and operational performance. The frameworks and guidance are written for many different recipients. At a broad level, the components and principles are designed to help inform boards and executives. The more detailed guidance is intended to help management who are responsible day-to-day for managing risk, executing internal controls and deterring fraud.
Given that internal auditors do risk-based auditing and focus on the effectiveness of internal controls as well as fraud deterrence, all COSO materials are relevant and useful to them. I encourage interested readers to refer to a short book I wrote for the Internal Audit Foundation titled *Managing Risk in Uncertain Times: Leveraging COSO's New ERM Framework.* I provide several examples in that book of how internal auditors can leverage the new framework during annual audit planning, project planning, project reporting, and providing advice to management on ERM. I think it's important for every internal auditor to have a fundamental understanding of ERM and internal control, and COSO has a variety of guidance, much of it free of charge, to help with that understanding.

We could see some development in terms of a famous COSO cube and now we can see some DNA like picture :-). Can you please describe the main thoughts behind these?

I've heard comments from people who miss the COSO cube, but it's still alive and well in the Internal Control – Integrated Framework. The cube does a good job of depicting internal control. However, for the updated ERM framework COSO believed a different graphic was necessary. COSO wanted to depict that ERM was woven through all activities of the company, starting with its mission, vision and core values, through all activities, which ultimately leads to better performance and enhanced value. By showing the components of ERM as ribbons weaving through the graphic, somewhat like a DNA strand, we believed it better shows the key messages in this updated framework.

In your book *Managing Risks in Uncertain Times: Leveraging COSO'S New ERM Framework* ***you say that*** *"The framework, if fully understood and incorporated by internal audit, will help improve the performance and value of internal audit in the development and execution of a risk-*

based approach." ***Can you describe how can internal auditors incorporate this Framework into their activities?***

At a high level, internal auditors must understand the strategies and business objectives for their organization. Those are what create the risks that we audit. By starting at the business level, then considering the objectives in the specific areas being audited, internal auditors can better put their audit findings in a context that management will relate to. For example, instead of telling management that the procurement policies weren't followed, it is more impactful to say there are no assurances that purchases were made at the best price and of the right quality to ensure success. I've found that relating the outcomes of audit deficiencies to business objectives helps management and the board better appreciate the importance of devoting resources to address those deficiencies.

The mission of internal audit is to enhance and protect organizational value. This encompasses focusing on achievement of business objectives. Do you think that internal auditors should expand their perspectives to not only focus on risks, but also to help their companies utilize opportunities? Could this help with a more visible presentation of the internal audit work as value adding to the key stakeholders?

Internal auditors must stay true to their charter, but increasingly such charters have a component focused on enhancing value, as opposed to the traditional internal audit focus on protecting value. The key is to find the right balance. We don't want existing value prematurely destroyed, which is why we still must consider the downside of risk, or threats to objectives. However, the skills that make internal auditors successful can also be used to help management better pursue the upside of risk, or opportunities to objectives. That way the value of internal audit will be more evident to all stakeholders – those who focus on protecting existing value, such as audit committee members, and those who strive for the creation of new value. I believe internal auditors can enable of both.

Some auditors when preparing the audit plan are starting their thinking at the level of the risks, i.e. what can go wrong. In your opinion should the auditors start with the vision/mission/strategy/ objectives of the company first and during the next step think about what can prevent the company being successful in meeting the vision/mission/strategy/ objectives? This could in my opinion lead to a more relevant auditing and supporting partnership of auditors with management. What is your opinion?

By definition, risk has no context without considering the related objectives. The COSO definition of risk is "the possibility events will occur and affect the achievement of strategy and business objectives." Thus, if internal auditors start first with risk, they will likely identify many, but not all, of the risks to those strategies and business objectives. In fact, they will probably identify the bad things (negative events) that can happen but will likely overlook the good things (positive events) that can help promote achievement of strategies and business objectives. That's why I believe it's important for internal auditors to understand ERM and think like a risk professional. They're much more likely to have the right mindset to both enhance and protect organizational value.

Auditors are striving for not being just a must have cost center but to bring a real value to the company. What would be your advice how to achieve this?

Follow the advice from above. A must have internal audit function may help protect value, but much of the real value of internal auditing comes from the assurance and advice that helps enhance existing and future value. Every internal audit function should strive to be seen as a value creating center, not just a cost center.

I often ask my guests a question – If there is a competition to find a real star in internal audit, who should win in your opinion?

During my time as a volunteer for The IIA, I've been fortunate to work with some great internal auditors throughout the world. However, the one name that immediately jumps to mind is Richard Chambers. He's been in his role as President and CEO of The IIA for a decade now, and he's been outstanding in that role because of all he learned during his tenure as an internal auditor. His continued ability to provide thought leadership as well as valuable lessons to internal auditors, whether through his blogs, presentations or books, has helped advance the profession more than any other single individual I can think of.

Are we going to see you in the Czech Republic in the near future?

I hope so. I've been blessed with the opportunity to visit many countries during my term as IIA Chairman and now as COSO Chairman, but I've never been to the Czech Republic. I've heard so many wonderful things about your country. It's one of my top destinations to try and visit during my three-year term as COSO Chairman.

What would be your last words to the readers of the Internal Auditor Journal in the Czech Republic?

We live in a world where the pace of change is accelerating very quickly. It's always easiest to stick with what you're comfortable doing. But I encourage you to be a life-long learner, periodically reinvent yourself, and strive to be uniquely relevant in the future. I think the future will be very exciting for those internal auditors who are prepared to make a difference.

Thank you for your time and answers today and I hope to see you in the Czech Republic soon.

Thank you.

Workshop pro interní auditory z veřejné správy

Ing. Šárka Nováková, MBA
vedoucí Odboru vnitřního auditu a kontroly
Všeobecná fakultní nemocnice v Praze

Rok se s rokem sešel a my, interní auditoři z veřejné správy, jsme se dočkali svého workshopu pořádaného Českým institutem interních auditorů. Letos se konal 10.–11. dubna v Hradci Králové a zázemí nám poskytl osvědčený hotel Černigov. Realizaci workshopu podpořil náměstek ministra financí ČR Tomáš Vyhnánek a generální ředitel sekce auditu a kontroly Ministerstva financí SR Vladimír Urmanič.

Hned po registraci účastníků, distribuci písemných podkladů a malém občerstvení na uvítanou následovalo oficiální zahájení a první prezentace, která nepatřila nikomu jinému než Tomášovi Vyhnánkovi, který nás příjemnou a srozumitelnou formou zasvětil do reálných zkušeností s aplikacemi nad otevřenými daty a jejich vizualizací „Supervizor“ a „Cityvizor“. Zopakovali jsme si známou pravdu, že mezi pojmem data a informace nemusí být rovnítko a že klíčový není pouze detail a konkrétní údaje, ale i přehledová data, která dodají našim zjištěním nezbytný kontext.
Následovala přednáška Davida Slámy, který nejednoho z nás překvapil formou a rozsahem využívání dat (včetně dat od mobilních operátorů) ve veřejné správě pro analytickou činnost Ministerstva vnitra ČR.

DĚKUJEME PARTNERŮM

ORGANIZÁTOR

HLAVNÍ PARTNER

PARTNER

MEDIÁLNÍ PARTNER

Hovořil o tvorbě veřejných politik založené na datech místo emocí a nepodložených předpokladů, o ročním hodnocení veřejné správy prostřednictvím 42 ukazatelů nebo o analýze komunálních voleb v roce 2018.

Dopolední blok zakončila kvalitní a poutavě pojatá panelová diskuze na téma kyberprostor, kterou zkušeně moderoval kolega Milan Zolich z Ministerstva spravedlnosti ČR. Účastníky byli Petr Grešl (konzultační společnost Rogit t, s.r.o.,), Dominik Marek (Kraj Vysočina), Vladimír Rohel (Národní agentura pro komunikační a informační technologie , s.p.) a Aleš Špidla (Generální finanční ředitelství Praha), který mě pobavil trefným arabským příslovím: „V Alláha věř, ale velblouda přivaž."

V rámci odpolední části workshopu jsme se měli možnost, každý podle svých preferencí, rozdělit do tradičních pracovních skupin, přičemž témata byla opravdu lákavá: interní audit založený na datové analytice, praktické využití MS Excel a dalších nástrojů firmy Microsoft (PowerPivot, Power BI) v datových analýzách, finanční kontrola a dodržování principu kontroly čtyř očí nebo GDPR.

Přednáškové dopoledne následující den zahájila Martina Smetanová, která nám představila činnost a častá zjištění Rady pro veřejný dohled nad auditem. Přednášku zaměřenou na prevenci trestní odpovědnosti právnických osob si pro nás připravil Miloslav Kvapil ze společnosti Dynatech a prezentaci na téma „Interní audit pro řízení kvality" Štěpánka Cvejnová z Ministerstva vnitra ČR.

Workshop zakončila série vystoupení Evy Janouškové (Kraj Vysočina), Blanky Štefankové (Moravskoslezský kraj), Ivy Göttingerové (statutární město Brno) a Tomáše Domeckého (hlavní město Praha). Představili nám činnost a hmatatelné výstupy komise pro primární systém dohledu v rámci Sekce veřejné správy ČIIA. Všichni jmenovaní si (i nám ostatním) kladli otázku, zda interní auditor ve veřejné správě potřebuje znát metody a nástroje řízení. Společně jsme také zalistovali v pomyslném slabikáři interního auditu, připomněli si principy vnitřního kontrolního systému podle COSO, hovořili o nutnosti řízení rizik, procesním řízení (kdy je procesní mapu vhodné tvořit „shora dolů"), o tvorbě strategií krajů, měst a úřadů i o robotické automatizaci procesů, kdy softwarový robot (už skutečně v praxi) úspěšně vykonává rutinní činnost místo zaměstnance (viz agenda „kotlíkových dotací" v Moravskoslezském kraji).

Kdo dočetl moje ohlédnutí za workshopem až sem, už jistě správně tuší, že jsem si otevřenost a blízkost svých kolegů opět užívala s neskrývaným nadšením a plnými doušky. Vždyť co je víc než možnost vzájemně sdílet starosti i radosti. Takových chvil si upřímně vážím a svých milých kolegů naladěných na stejnou notu si nesmírně cením. ■

Noví členové

- Ing. Michal Badura, Západoslovenská energetika, a.s.
- Ing. Pavel Bátora, Západoslovenská energetika, a.s.
- Jiří Běloušek, Fio banka, a.s.
- Ing. Martin Burkoň, ČSOB Pojišťovna, a. s., člen holdingu ČSOB
- Ing. Šárka Feketová, Československá obchodní banka, a. s.
- Ing. Aneta Hermannová, Česká spořitelna, a.s.
- Bc. Thuy Lam Hoang, Komerční banka, a.s.
- Ing. Josef Kubš, AGEL a.s.
- Ing. Tomáš Kunz, Komerční banka, a.s.
- Ing. Jan Laš, Česká geologická služba
- Ing. Jiří Marek, Individuální člen
- Ing. Ema Matějů, Individuální členka
- Ing. Michal Pintek, AGEL SK a. s.
- Ing. Petr Putnioř, Zdravotní ústav se sídlem v Ostravě
- Ing. Andrea Slouková, Ministerstvo vnitra ČR
- Ing. Helena Stuchlíková, Univerzita Karlova
- Bc. Michaela Urbánková, Kooperativa pojišťovna, a.s., Vienna Insurance Group
- Ing. Marcel Váňa, Individuální člen

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

Čeho si *Andrea* povšimla *aneb* **co se děje na mezinárodní scéně**

Na webových stránkách Mezinárodního institutu interních auditorů (IIA) se opět objevila řada užitečných informací:

- Jednou z nich je publikace Internal Auditors' Response to Disruptive Innovation (Odpověď interního auditora na inovace, které mohou způsobit útok z vnějšku a narušení vnitřního prostředí). Toto téma bývá často diskutováno na různých fórech, nedávno jsem se účastnila přednášky na téma audit umělé inteligence. V publikaci IIA si můžete přečíst výsledky mezinárodního průzkumu mezi vedoucími útvaru interního auditu a seznámit se s problémy, které v této oblasti obvykle řeší. Publikace je ke stažení na stránkách www.theiia.org.

- Ráda bych také upozornila na blog Richarda Chamberse, kde se pravidelně objevují zajímavé postřehy týkající se interních auditorů. Jeden z posledních blogů se týká postavení a vnímání interního auditora v organizaci. Richard Chambers říká, že je důležité, aby byl interní auditor vnímán jako leader a aby jeho rada byla žádaná mezi členy vedení společnosti. Více se dočtete zde: https://na.theiia.org/news/Pages/Blog-To-Be-Good-Leaders-Internal-Auditors-Must-Also-Follow.aspx

- Pokud byste se chtěli dovědět více o roli interního auditu v poskytování ujištění o funkčnosti systému na prevence podvodů, pak doporučuji stanovisko IIA (Position Paper) na toto téma – https://na.theiia.org/about-ia/PublicDocuments/Fraud-and-Internal-Audit.pdf. Další stanoviska na různá témata, která vám mohou při každodenní praxi naleznete opět na stránkách IIA zde: https://na.theiia.org/about-us/about-ia/Pages/Position-Papers.aspx

- Většina z vás už asi slyšela o sítích páté generace a ti z vás, kteří pracují v sektoru telekomunikací nebo jejichž oboru se telekomunikace dotýkají, se této oblasti budou muset dotknout při své auditní práci. Užitečné informace vám může poskytnout přiručka 5G a čtvrtá průmyslová revoluce. https://global.theiia.org/knowledge/Pages/Global-Perspectives-and-Insights.aspx

Je INTERNÍ AUDIT připraven na očekávanou krizi?

„Spouštěcím mechanizmem nové krize může být fakticky cokoli.“

Prof. Ing. Jiří Dvořáček, CSc., je absolventem Vysoké školy ekonomické v Praze (VŠE). Patří mezi zakladatele Českého institutu interních auditorů. Byl členem rady Institutu a viceprezidentem pro vzdělávání. Řadu let lektorsky v ČIIA působil. Na VŠE zavedl kurz interního auditu, který zde má více než dvacetiletou tradici, a inspiroval k této výuce i jiné vysoké školy. K problematice interního auditu napsal několik knižních publikací a článků, úzce v této oblasti spolupracoval s podnikovou praxí. Nyní se zaměřuje zejména na otázky změn podnikatelského prostředí v souvislosti s tzv. 4. průmyslovou revolucí. Pracuje na katedře strategie VŠE.

Ing. Josef Tyll, CSc., je absolventem VŠE v Praze. V letech 1992–2010 pracoval jako vedoucí úseku interního auditu v Creditanstalt a.s., Bank Austria Creditanstalt a.s., HVB Bank a.s., UniCredit Bank CR, a.s. V letech 2011–2013 působil jako konzultant IA v UniCredit Bank Austria. Od r. 2011 do současnosti je ombudsmanem UniCredit Bank CR and Slovakia, a.s. Od r. 2014 pracuje externě v Radě pro veřejný dohled nad auditem; od r. 2016 je předsedou Komise pro koordinaci vzdělávání a profesní zkoušky. Patří mezi spoluzakladatele ČIIA, v letech 1995–1998 byl viceprezidentem. Mnoho let se aktivně podílel na činnosti Komise pro vnitřní audit ČBA, 15 let byl jejím předsedou. V průběhu své více než dvacetileté praxe v IA publikoval o interním auditu řadu statí v Hospodářských novinách, časopise Bankovnictví a Interní auditor.

Od velké finanční krize, která propukla v roce 2008, uplynulo již deset let a někteří ekonomové začínají varovat, že nová krize je na spadnutí. A jestliže ta velká z roku 2008 měla svůj původ v bankovnictví, odkud se přelila do ostatních odvětví, spouštěcím mechanizmem nové krize může být fakticky cokoli. Počínaje globalizací, která se projevuje v tom, že firmy začaly spoustu svých činností přenášet tam, kde je levná pracovní síla, produkty se vyrábějí ve vzdálených lokalitách, nikoli co nejblíže zákazníkovi, mezinárodním obchodem, novou hypoteční krizí, přehřátou ekonomikou, očekávaným brexitem, možnou obchodní válkou mezi USA a Čínou, resp. mezi USA a EU, a podobně. Úvahy o potenciální nové krizi se objevují ve zvýšené míře v posledních dvou letech. Faktický vývoj v řadě ekonomik, včetně české, vykazuje známky nižší dynamiky růstu hrubého domácího produktu a tím i možné recese, která bývá předstupněm krize.

Hospodářský cyklus – atribut tržní ekonomiky

Ponecháme-li stranou možné důvody, které mohou ke krizi vést, nesmíme zapomínat, že pro tržní ekonomiku jsou hospodářské cykly, ve kterých se střídají fáze konjunktury s fází deprese, resp. krize, jejich součástí. Střednědobé hospodářské cykly přicházejí s průměrnou délkou kolem deseti let. Přestože lze po letech prosperity celosvětovou krizi očekávat, jednotlivé organizace čelí hrozbě možné krize prakticky každodenně. Krizi lze chápat jako náhlé zhoršení situace v organizaci. Signálem krize může být např. pokles tržního podílu, pokles tržeb, snižování ziskových marží, pokles dosahovaných cen, snižující se schopnost uhrazovat krátkodobé závazky (pokles likvidity), omezení nebo zmrazení výplat dividend, omezování investic… Současně s tím může docházet k nárůstu fluktuace zaměstnanců, vzrůstu režijních nákladů, růstu tržeb u produktů s nízkou marží, rostoucím nákladům na splácení dluhů, většímu tlaku věřitelů na splácení dluhů apod. Krizové řízení organizace se od běžného řešení liší zejména tím, že jeho cílem je zabránit dalšímu negativnímu vývoji výše uvedených ukazatelů a obnovit dlouhodobé zdraví organizace.

„Pro tržní ekonomiku jsou hospodářské cykly, ve kterých se střídají fáze konjunktury s fází deprese, resp. krize, jejich součástí.“

Pokud krize zasáhne jednotlivé organizace, periodicky se opakuje otázka, jakou roli v krizi má či může sehrát interní audit. Zde se odpovědi zpravidla pohybují mezi dvěma krajními stanovisky – první chápe interní audit jako nákladovou funkci, která v podstatě organizaci nic nepřináší, ale pouze hodně stojí, a proto bude nejlepší, v rámci úsporných opatření, činnost útvaru interního auditu utlumit, nebo jej dokonce zrušit. Druhé stanovisko optimisticky povyšuje interní audit do role zachránce organizace a spojuje s jeho činností nereálná očekávání.

Byť interní audit může mnohé, tak zpravidla býval povolán k řešení již nastalé krize, a to bylo z pohledu interního auditu pozdě, neboť interní audit není náhrada krizového managementu. Interní audit by měl být využíván spolu se svou ujišťovací funkcí především jako nástroj prevence před krizemi. A to jako součást strategického managementu a nezastupitelný prvek správy a řízení společnosti (corporate governance). Protože se zvyšuje provázanost činností jak uvnitř organizací, tak mezi organizacemi navzájem, stávají se hrozby a dopady obtížně předpověditelnými, a to i přes fakt, že rostou možnosti komunikace. Ale vrcholový management organizací musí být připraven na nepředvídatelné, aby jeho rozhodování bylo adekvátní.

Uplynulých deset let umožňuje provést podrobnější analýzu toho, jak interní audit v krizi obstál a jaké jsou možnosti pro jeho účinné využití před propuknutím krize nové. Samotné propuknutí krize v r. 2008 vyvolalo diskuzi o roli interního auditu (viz např. i časopis Interní auditor č. 4 z r. 2009), v letech krize i po jejím skončení se požadavky na efektivní interní audit výrazně prohloubily.

Zaměření na procesy správy a řízení společnosti (corporate governance)

Stává-li se interní audit součástí strategického managementu organizace, pak se musí IA zaměřit na analýzu a ocenění stávajícího stavu corporate governance ve společnosti, a to zda je v souladu s mezinárodní i národní legislativou, ostatními regulatorními směrnicemi, jakož i tzv. best practice.

Cílem auditu procesů správy a řízení společnosti

musí být identifikace slabých míst a nutných zlepšení, které pomohou organizaci přežít krizi. Týmy interních auditorů by měly zejména zhodnotit roli představenstva a dozorčí rady (správní rady a statutárních ředitelů) ve společnosti. Pozornost by měly věnovat v prvé řadě odbornosti a nezávislosti jejích členů a hodnocení jejich výkonu.

„Interní audit by měl být využíván spolu s ujišťovací funkcí především jako nástroj prevence před krizemi.“

Ze stejných hledisek by interní audit měl hodnotit roli výborů společnosti (výbor při řízení rizik, výbor pro audit, výbor pro odměňování, nominační výbor). V neposlední řadě by měl rozebrat a zhodnotit úroveň vzájemných vztahů akcionářů a orgánů správy a řízení společnosti, zejména zde existuje dostatečný prostor pro výkon práv akcionářů. Ve srovnání s minulým obdobím by měl být systém odměňování ve společnosti podroben auditu každý rok s důrazem na dodržování příslušných směrnic EU a národních právních předpisů.

Přidaná hodnota interního auditu

Očekávání tzv. stakeholderů interního auditu rostou, zejména v předkrizovém období. Podle našeho názoru lze přínosy interního auditu charakterizovat takto:

- posouzení strategických plánů společnosti zejména z hlediska orientace společnosti na udržitelný rozvoj, robotizaci, přiblížení výroby konečnému zákazníkovi;
- vypracování pohotovostních plánů pro případ krizové situace a posouzení, zda jsou tyto plány pro jednotlivé krizové situace adekvátní;
- re-design řídicích a kontrolních procesů mezi jednotlivými účastníky správy a řízení společnosti (představenstvo, dozorčí rada, výbory společnosti, valná hromada, akcionáři) směrem k transparentnosti a posílení odpovědnosti za efektivní a udržitelné řízení společnosti;
- zabezpečení kybernetické hygieny;
- účinné a efektivní řízení potenciálních rizik;
- výrazné snížení byrokratické, administrativní zátěže systému řízení.

Zaměření IA na riziko

Řízení rizik je jednou z hlavních součástí řízení správy a řízení společnosti. Ještě před velkou krizí z r. 2008 byl, v reakci na finanční skandály velkých firem jako Enron, WorldCom, Parmalat…, přijat zákon Sarbanes-Oxley, který položil důraz především na vnitřní kontrolní mechanizmy a na výbor pro audit. Čas však ukázal, že omezovat roli interního auditu pouze na prověřování vnitřního kontrolního prostředí nestačí a je nutné, aby interní auditor více pracoval s riziky. Přitom riziko bývá v auditorské praxi chápáno jako pravděpodobnost, že určitá událost či jev bude mít negativní dopad na organizaci. Každé riziko je nutné posuzovat z hlediska možnosti jeho vzniku, významu rizika pro organizaci a četnosti, se kterou se riziko může vyskytnout.

Na systém řízení rizik na podnikové úrovni byl, a to na základě celosvětové diskuze, v r. 2004 pod hlavičkou COSO (Committee of Sponsoring Organizations) publikován materiál představující rámec integrovaného řízení rizika na podnikové úrovni (Enterprise Risk Management – Integrated Framework). Ten měl sloužit jako prostředek pro dosažení dvou cílů.

Prvním cílem byla identifikace kritických rizik, kterým je organizace vystavena, včetně dobrého jména, etiky nebo zdravotních, bezpečnostních a environmentálních rizik. Nikoliv tedy pouze finančních nebo pojistitelných rizik.

„Cílem auditu procesů správy a řízení společnosti musí být identifikace slabých míst a nutných zlepšení, které pomohou organizaci přežít krizi.“

Druhým cílem bylo řízení a optimalizace portfolia rizik, která jsou vlastní všem činnostem s dopadem na zisk organizace. Rámec z r. 2004 byl v r. 2017 novelizován a publikován COSO pod názvem Enterprise Risk Management—Integrating with Strategy and Performance, zaměřuje se na význam rizik ve spojení se strategií organizace a její výkonností. Důvodem novelizace byla především skutečnost, že v praxi se začala objevovat nová rizika a docházelo k jejich komplexnímu působení. Managementu i interním auditorům může usnadnit práci s riziky i doplněk k původnímu materiálu z r. 2017, který zahrnuje, v podobě případových studií, jednotlivé složky celého systému ERM.

V roce 2009 byly vydány ISO normy zaměřené na řízení rizika, na jeho posuzování a techniky řízení. Tyto normy jsou českému čtenáři k dispozici v podobě norem ČSN ISO 31000 „Management rizik – Principy a směrnice“ a ČSN EN 31010 „Management rizik – Techniky posuzování rizik.“ Celkový proces posuzování rizika je složen ze tří částí: 1. identifikace rizik. 2. analýza rizik. 3. hodnocení rizik. Úroveň (míra) rizika je kombinací následků a pravděpodobnosti jejich výskytu. V hodnocení rizik jsou tato zařazována do některé ze tří skupin, a to 1. nevýznamná rizika, 2. středně významná rizika, 3. významná rizika.

Aby při řízení rizika byly používány stejné pojmy všemi účastníky, kteří se rizikem zabývají (manažeři, risk manažeři, auditoři, výbor pro audit, výbor pro řízení rizika…), byl následně vydán Slovník zaměřený na management rizika (TNI 01 0350).

Pro oblast bankovnictví a pojišťovnictví má z hlediska řízení rizik klíčový význam Směrnice a nařízení Evropského parlamentu z r. 2013 k posílení finančního systému. Směrnice i nařízení jsou obsaženy ve vyhlášce ČNB z r. 2014 (tzv. obezřetnostní vyhláška).

Důraz na řízení rizika je obsažen i v novelizovaných mezinárodních standardech pro profesní praxi interního auditu, platných od r. 2017. Konkrétně se jedná o standard 2010, zaměřený na plánování interního auditu, a standard 2120, který se týká řízení rizik. Plán interního auditu musí být rizikově zaměřený, být v souladu s cíli organizace a musí stanovit priority interního auditu. V řízení rizik musí interní audit hodnotit účinnost procesů řízení rizika a přispívat ke zdokonalování těchto procesů.

Z výše uvedeného stručného přehledu je zřejmé, že pro předvídání možné krize a práci s riziky má interní audit k dispozici dostatek vhodných metodických materiálů, které mu mohou jeho práci usnadnit a přispět k tomu, že interní audit bude na možné změny připraven a bude v jejich řízení hrát pro-aktivní roli.

Interní audit by se měl především zaměřit na rizika, kterým je organizace vystavena, a poskytovat ujištění, že tato rizika jsou známa a jsou pod kontrolou. Řízení rizika je odpovědností managementu, kterou na sebe interní audit nemůže brát. Ale interní audit může přispět k vymezování oblastí, na které by se management měl zaměřit. A měl by

v rámci organizací pořádat workshopy, zaměřené na rizika. Velkou chybou pro organizaci může být, že výstupy interního auditu z oblasti posuzování rizik budou managementem ignorovány. Ale ještě větší chybou bude, pokud interní audit nebude oblast rizika považovat za důležitou, resp. bude o svých zjištěních informovat management pozdě.

Působení interního auditu jak v předkrizovém, tak i krizovém období organizace nelze omezovat pouze na problematiku rizika. Neustálou pozornost musí věnovat jak vnitřnímu kontrolnímu systému, tak přidávané hodnotě jednotlivých činností, adaptaci organizace na měnící se podmínky v okolí a kvalitě vnitřní a vnější komunikace.

Autoři zastávají názor, že IA jako nezbytná součást strategického managementu – má-li být pro společnost prospěšný v předkrizových a krizových dobách – se musí soustředit na výše uvedené oblasti. Jinak bude interní audit ztrácet své těžce vydobyté postavení. ■

„Očekávání tzv. stakeholderů interního auditu rostou, zejména v předkrizovém období.“

Závěrem

Krizi v organizaci nelze jednoznačně chápat jenom jako ohrožení. Krize může pro organizaci představovat i příležitost k dalšímu rozvoji. A to podle toho, jak se organizace s krizí vyrovná. Buď bude krize silnější než připravenost organizace a organizace pak svou činnost ukončí, nebo management, ve spolupráci s interním auditem, příjme taková opatření, že krizi úspěšně překoná. Zvládnutí krize s pomocí interního auditu bude v jednotlivých organizacích závislé i na počtech pracovníků interního auditu, rozpočtu interního auditu a na stabilitě útvaru interního auditu.

Autoři jsou si vědomi toho, že nastolují velmi náročný úkol pro interní audit. Správa a řízení společnosti představují velmi komplikovanou oblast vztahů, která vyžaduje adekvátní postavení interního auditu ve společnosti. Mohou totiž vznikat námitky, zda na to IA má, jak z hlediska odbornosti, tak zejména nezávislosti.

Pracovní snídaně:

„Kybernetická bezpečnost – další odpovědnost pro správní orgán?“

V úterý 14. května 2019 se uskutečnila v hotelu Mandarin Oriental v Praze pracovní snídaně na téma kybernetické bezpečnosti, kterou organizovaly společně Český institut interních auditorů a Institut členů správních orgánů.

Pracovní snídani uvedli za Institut členů správních orgánů jeho výkonná ředitelka, paní Monika Zahálková a Tomáš Pivoňka, prezident Českého institutu interních auditorů.

Poté vystoupili tři přednášející:

Tomáš Grznár, vedoucí speciálních auditů ve společnosti ČEZ;

Jozef Paštrnák, bezpečnostní architekt ve společnosti Novartis;

Vladimír Rohel, ředitel sekce Bezpečnosti, NAKIT (Národní agentura pro komunikační a informační technologie).

První vystupující, Tomáš Grznár, se ve svém příspěvku zaměřil na Zákon o kybernetické bezpečnosti (dále „ZKB“) z pohledu auditora. Tomáš Grznár zmínil, jaké jsou základní povinnosti společností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, účinného od 1. 1. 2015, vč. požadavků vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti. Velmi zajímavá byla i další oblast, kterou Tomáš věnoval sdílení praktických zkušeností s prováděním auditů podle ZKB ve společnosti ČEZ.

Druhý vystupující, Jozef Paštrnák, nazval svůj příspěvek „Od nálezu k nápravě“ a zabýval se designem efektivní bezpečnostní ochrany. Podrobněji rozebral jednotlivé prvky Průvodce kybernetickou bezpečností z roku 2018, který vydal Národní institut pro standardy a technologie USA. Těmito prvky jsou (a) Identifikace zdrojů, které podporují kritické obchodní funkce, a související rizika kybernetické bezpečnosti, (b) Návrh ochranných prvků eliminujících nebo snižujících dopad potenciálních událostí kybernetické bezpečnosti, (c) Návrh detekčních prvků k efektivní detekci negativních anomálií a událostí kybernetické bezpečnosti, (d) Návrh reakčních prvků k zastavení negativní události kybernetické bezpečnosti a omezení dopadu, (e) Návrh procesů a postupů zotavení se z výskytu negativní události kybernetické bezpečnosti.

Třetí vystupující, Vladimír Rohel, se ve svém příspěvku zaměřil na to, že bezpečnost není vůbec brzdou pokroku, jak je jí někdy nesprávně přičítáno. Detailně také rozebral, v jaké fázi IT projektů by měli být přizváni specialisté na IT bezpečnost – čím dříve jsou tito odborníci přizváni, tím lépe. Dále byly diskutovány nejbližší výzvy v oblasti bezpečnosti, a to zejména ve spojení s fenoménem ‘Internet of Things’.

Po vystoupení následovala živá diskuze mezi účastníky. Osobně považuji toto setkání za velmi užitečné, a to zejména kvůli nutnosti neustále zvyšovat povědomí o oblasti kybernetických hrozeb. Doufám, že Český institut interních auditorů a Institut členů správních orgánů budou s těmito workshopy pokračovat i do budoucna. ■

Petr Hadrava

Interní auditoři a kontroloři z Moravy se sešli na svém XI. tradičním odborném setkání

V rekreačním středisku Baldovec se ve dnech 16.–17. května 2019 sešlo 42 účastníků odborného setkání auditu a kontroly z pozvaných zástupců 25 moravských měst a městských částí. Hostitelem bylo tentokrát statutární město Prostějov a záštitu nad setkáním převzal primátor Prostějova Mgr. František Jura.

Celé setkání proběhlo v přátelské pracovní atmosféře a jednoznačně splnilo svůj cíl, kterým je předávání odborných zkušeností a výměna dobré praxe mezi účastníky.

Po krátkém úvodním představení hostitelského města Prostějova zhlédli účastníci prezentaci tajemníka Uherského Brodu Ing. Kamila Válka „Inovace v interním auditu CCM (Continuous Control Monitoring)“, za kterou převzalo město Uherský Brod v roce 2018 ocenění v soutěži Cena za inovaci v interním auditu. Předmětem prezentace byla kontinuální kontrola a monitoring dat u smluv, které město a příspěvkové organice vkládají do Registru smluv, a průběžné monitorování všech kroků v procesu elektronického oběhu účetních dokladů. Prezentace vedoucí útvaru interního auditu a kontroly statutárního města Brna Ing. Ivany Göttingerové představila účastníkům „Program pro zabezpečení a zvyšování kvality interního auditu na oddělení IA“ na Magistrátu města Brna. V diskuzi mimo jiné připomněla, že v dnešním světě, plném informací, starostí o kybernetickou bezpečnost i o ochranu osobních údajů, je důležité zachovat si zdravý rozum.

Součástí odborného programu bylo představení současných aktivit a plánů ČIIA, které nastínil přímo Ing. Daniel Häusler. Ing. Dana Ratajská představila kompletní přehled programů národních dotací, které Ministerstvo pro místní rozvoj ČR nabízí, a zaměřila se na kontroly příjemců dotací a nejčastější zjištění, která pracovníci při těchto kontrolách řeší.

S aktuálními informacemi ze setkání interních auditorů krajských úřadů nás seznámila Ing. Marta Filipcová, pověřená vedením interního auditu KÚ Olomouckého kraje.

V odpolední, neformální části setkání se účastníci vypravili do nedalekého Moravského krasu na prohlídku Punkevních jeskyní, Audit trail na dno Macochy a plavbu podzemní říčkou Punkva. ■

Ing. Petr Šilhánek
interní auditor statutárního města Prostějov

Členové Rady ČIIA a Kontrolní komise ČIIA po zasedání 24. Sněmu ČIIA

RADA ČIIA

Ing. František Beckert, CIA
Ministerstvo financí ČR
VICEPREZIDENT ČIIA

Mgr. Tomáš Pivoňka, CIA, CRMA
ČEZ, a. s.
PREZIDENT ČIIA

Ing. Zuzana Háková, CIA, CISA, CPA
UniCredit Bank Czech Republic a Slovakia, a.s.
VICEPREZIDENTKA ČIIA

Ing. Vadim Beneš, Ph.D., CIA, CRMA
PricewaterhouseCoopers Audit, s.r.o.

Ing. Michal Čup, CIA, FCCA
KPMG Česká republika, s.r.o.

Ing. Miloslav Frumar, CIA
Česká spořitelna, a.s.

Ing. Petr Hadrava, CIA, CISA, CFSA, FCCA
Sberbank CZ, a.s.

Ing. Jitka Kazimírová, CIA, FCCA
Allianz pojišťovna, a.s.

Ing. Eva Klímová
Úřad městské části Praha 2

Ing. Jan Kovalčík, CIA
Česká spořitelna, a.s.

Ing. Michaela Kubýová, FCCA
Raiffeisenbank a.s.

Ing. Dana Ratajská
Ministerstvo pro místní rozvoj ČR

Ing. Ladislava Slancová
Nejvyšší kontrolní úřad

Ing. Petr Vácha, CIA
ČD Cargo, a.s.

Mgr. Filip Zelingr
Letiště Praha, a. s.

KONTROLNÍ KOMISE ČIIA

Ing. Martin Bubeník, Ph.D.
ČEZ, a. s.

Mgr. Petr Švub, CIA, CISA
Česká spořitelna, a.s.
PŘEDSEDA

Mgr. František Orság, CIA
Ministerstvo vnitra ČR

English Annotation

Jakub Hlavica, Josef Mynář – Practical Experience from the Implementation of the Administrative and Organizational Measures in Pražská teplárenská

The authors explain to the readers individual steps if the implementation of the requirements of the Cybersecurity Act in one of the important heat stations, use of the project approach and SW tools.

Petr Švéda – The Audit of Cybersecurity

The author introduces the main pillars of the audit of cybersecurity, mainly in relation to the valid legislation. Further he deals with the current trends and issues in the practice.

Aleš Špidla – The Audit of Cybersecurity – Isolated Discipline

The idea, that the audit of cybersecurity is separated discipline, needs to be immediately changed, because the penetration of the IT in the audited areas and whole audit universe is more and more large and deep. One article does not give enough room for more detail specification and description of the whole topic, so the author mentioned only few easily understandable areas.

Václav Peřich – From the Virtual Space to the Highest Politics

The author discusses the area of cybersecurity and its topicality nowadays in the current complicated world.

Petr Hadrava – Interview with Paul J. Sobel

Sobel Interview with Paul J. Sobel performed by Petr Hadrava.

Jiří Dvořáček , Josef Tyll – Is Internal Audit Prepared for the Expected Crisis?

The authors deal in their article with the economic cycle as with the attribute of the market economy and the role the internal audit should play in this area. Wha is its role, to what it should pay its attention, what are the expectations of its stakeholders, what tools and supporting materials it has to make the make the job easier and to fulfill the expectations.

ČESKÝ INSTITUT INTERNÍCH AUDITORŮ NABÍZÍ

ČESKÝ INSTITUT INTERNÍCH AUDITORŮ

AKADEMIE ÚSPĚŠNÉHO VEDENÍ **INTERNÍHO AUDITU I.**

Co je klíčem k úspěchu interního auditu?
Práce s lidmi.

PRO KOHO JE AKADEMIE URČENA?

- Vedoucí interního auditu (CAE)
- Vedoucí týmů interního auditu (Leading auditor)
- Manažery interního auditu
- Talenty interního auditu

TĚŠÍ SE NA VÁS TÝM LEKTORŮ:

Mgr. Pavla Pavlíková, PCC
Ing. Ivo Středa