iA interní auditor

ČTVRTLETNÍK ČESKÉHO INSTITUTU INTERNÍCH AUDITORŮ

ROČNÍK 25, ČÍSLO 1|2021 (99) 1|2021

ČESKÝ INSTITUT INTERNÍCH AUDITORŮ VÁS ZVE NA MEZINÁRODNÍ KONFERENCI

BUDOUCNOST INTERNÍHO AUDITU

HODNOTA, TRANSPARENTNOST, RESPEKT

Praha 26—27/5/2021

GENERÁLNÍ PARTNER

SKUPINA ČEZ

WWW.CIIACONFERENCE.COM

Vážení přátelé,

s novým rokem přichází i první letošní číslo časopisu Interní auditor. Stejně jako v roce minulém pokračujeme vydáváním časopisu pouze v elektronické formě. Vloni touto dobou jsme si nedokázali představit, že společnost může být po roce v ještě horší situaci. Eskalace rizika pandemie je stále s námi. Doposud nevíme, jaký bude konečný účet. Určitě ne dobrý.

Téma nového čísla je i vzhledem k současné situaci velmi aktuální (podvody a různé formy narušení bezpečnosti a chodu organizace). O pandemii slyšíme denně ze všech stran. Toto riziko tady není osamoceno. S ním se probudila a prohloubila i celá řada dalších rizik. Co s nimi? Která to jsou? To vám napoví již úvodní článek.

Často dnes kolem sebe slyšíme, že současná situace nahrává nekalému jednání vznikajícímu uvnitř organizací a rovněž přicházejícímu z vnějšího prostoru. Může jít o různé formy takového jednání. Od drobných prohřešků jedinců až po velké podvody a útoky organizovaných skupin. O některých slyšíme a čteme často v médiích. O kolika se nemluví? Nevíme. Každý se nepochlubí.

Určitě si v novém rozsáhlém čísle najdete potřebné informace, inspiraci a zajímavosti. Pokračujeme v seriálu v rámci společenské odpovědnosti. V něm vám pravidelně přibližujeme charitativní aktivity, které v naší zemi probíhají. Jsou velmi potřebné, záslužné a často nenahraditelné. Poděkování patří všem, kteří je organizují, jakýmkoli způsobem se na nich podílí, včetně finanční podpory. Nově jsme rovněž zařadili „vzdělávací koutek“. Uvidíme, zda se ujme. Třeba se rovněž zapojíte do jeho přípravy.

Časopis vás rovněž zve na mezinárodní konferenci Budoucnost interního auditu – hodnota, transparentnost, respekt, pořádanou Českým institutem interních auditorů. Nyní jsme se ji, po dvojím přesouvání, rozhodli uskutečnit formou on-line. Nezapomeňte se přihlásit a zajistit si tak nový zážitek a zkušenost. ■

Jan Kovalčík

OBSAH

ROČNÍK 25, ČÍSLO 1|2021 (99)

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

iA interní auditor

RISK MANAGEMENT PŘED PANDEMIÍ A PO NÍ: **od opakujícího se k průběžnému řízení?**

Mgr. Michal Štička, M.A.
Autor je manažerem forenzního oddělení KPMG, kde má na starosti poskytování služeb v oblasti řízení rizika podvodného jednání.
Před nástupem do KPMG byl konzultantem na volné noze. Jedním z jeho klientů byla i společnost kotovaná na americké burze, pro niž realizoval pilotní proces hodnocení rizik compliance.
V letech 2015–19 byl zaměstnán jako globální anti-fraud manažer v interním auditu společnosti Honeywell. Kromě jiného měl na starosti každoroční proces hodnocení rizika podvodného jednání. Pro funkci compliance vytvořil metodologii hodnocení rizika korupce. Podílel se i na pilotním projektu kontinuálního hodnocení rizik.
V minulosti působil i jako vedoucí projektů Transparency International – Česká republika.

CESTA DO MINULOSTI MÍSTO ÚVODU

Nevím jak vy, ale já bych se rád znovu vrátil do poloviny roku 2019. Důvodem není jen to, že bych chtěl opět zažít tu bezstarostnou předpandemickou dobu: interní audity na dálku byly spíše výjimkou, s klientem jste se mohli kdykoliv potkat osobně a home office bývala výsada, nikoliv povinnost.

Vrátit v čase bych se chtěl také proto, abych zjistil, do jaké míry tehdejší systémy řízení rizik předvídaly něco tak dramatického, čeho jsme svědky nyní.

Mám za to, že podniků, které riziko globální pandemie měly ve svých katalozích rizik, mnoho nebylo. A pokud na toto riziko někdo pamatoval, je více než možné, že bylo posuzováno jako riziko, u něhož byla pravděpodobnost výskytu vzdálená a dopady zanedbatelné. Chřipky se prostě tehdy nikdo nebál.

Znamená to snad, že se řízení rizik vinou pandemie definitivně zdiskreditovalo a je zbytečné? V tomto článku budu argumentovat, že samozřejmě nikoliv – naopak. Jen je třeba dodržovat určité praxí prověřené postupy a – hlavně – za pomoci dat, která mají jednotlivé organizace k dispozici, řízení rizik zavést jako kontinuální proces. Některé organizace už to koneckonců nějakou dobu dělají.

PANDEMICKÁ LABORATOŘ ŘÍZENÍ RIZIK

Od oznámení, že je v Česku první nakažený novým typem koronaviru, uplynul v těchto dnech právě jeden rok *(tento článek vznikl na přelomu února a března 2021 – pozn. autora)*. Pandemie přinesla podnikům i veřejným institucím bezprecedentní množství výzev, s nimiž se musely vypořádat. Některé z těchto výzev potrvají zcela jistě i poté, co se snad podaří pandemii porazit. S hořkou nadsázkou lze proto konstatovat, že pandemie vytvořila dokonalou laboratoř na testování efektivity řízení rizik v praxi.

> **„Pandemie vytvořila dokonalou laboratoř na testování efektivity řízení rizik v praxi.“**

Strategická rizika

První úrovní, kterou pandemie zasáhla, je nepochybně strategie organizací. Pokud společnosti dodávaly zboží a služby do sektorů, které byly pandemií zasaženy nejvíce, na obchodním vedení bylo najít alternativy alespoň z části kompenzující snížení tržeb. Klíčovými pro bytí společností se staly online prodejní kanály považované dříve v některých odvětvích spíše za doplňkové (pokud jste zrovna nebyli internetovým obchodem). Časový aspekt byl rovněž klíčový: na změny, které se před krizí chystaly měsíce či roky, měli najednou podnikatelé dny, nejvýše týdny.

Riziko, že otočení kormidlem neproběhne dostatečně rychle, je přímo úměrné kvalitě interní komunikace uvnitř podniků, a to jak shora dolů, tak i zdola nahoru. Změnu ročního plánu a v návaznosti na to často i dlouhodobějšího strategie musela podstoupit většina organizací. Tento proces, pokud byl i před pandemickou krizí správně nastaven a provozně účinný, pomohl a stále pomáhá organizacím uřídit riziko strategického ztroskotání v této výjimečné situaci.

Finanční rizika

Převodní pákou změny strategie se v mnoha případech stalo finanční řízení podniků, reagující na finanční dopady krize.

Na straně výkazu zisku a ztráty museli podnikatelé řešit, jak řídit klesající výnosy, tak i fixní a administrativní náklady, které i přes pokles tržeb „padají“ nezmenšené do výkazů.

Pokud jde o rozvahu, pak se u finančních manažerů diskutuje jistě více než

kdy jindy stárnutí pohledávek z obchodních vztahů a kreditní rizika u některých zákazníků, u kterých ještě před nedávnem pohledávky po splatnosti prakticky neexistovaly. Druhou stranu stejné mince pak představují rostoucí závazky vůči dodavatelům, finančním institucím a nutnost zajištění provozního financování v době přiškrceného provozního cash flow. Výroba mnohde řeší nezvykle vysoký objem rozpracované výroby a zásob, opět negativně dopadající na pracovní kapitál podniku. A investice do dlouhodobého majetku se rovněž odkládají často na dobu, až „tohle skončí".

„Na změny, které se před krizí chystaly měsíce či roky, měli najednou podnikatelé dny, nejvýše týdny."

I zde platí, že čím vyspělejší finanční řízení a robustnější vnitřní kontroly v klíčových procesech organizace má, tím úspěšněji se může vypořádat s dopady krize vyvolané pandemií.

Provozní rizika

Běžný provoz organizací zasáhla pandemie asi nejvíce. Kdo může, musí pracovat z domova. To znesnadňuje běžnou dennodenní operativní komunikaci a řízení, o možnosti popovídat si u pověstného automatu na vodu ani nemluvě.

Oddělení nákupu mnohde řeší výpadky dodávek v dodavatelském řetězci z důvodu nákazy u dodavatele nebo jiných logistických komplikací způsobených pandemií. Vedení musí daleko operativněji plánovat výrobu, ať už z důvodu prevence nákazy, nebo řešení výskytu pozitivně testovaného kolegy na pracovišti. Obchod rovněž vázne, ať už z důvodu nedostatečné koncové poptávky, nebo obecné nejistoty na trhu.

Za této situace se může obcházení existujících kontrol a zakrývaní podstatných informací jevit jako jednoduchá odpověď na složité provozní problémy. Možností jak „přikrášlit" tržby nebo „schovat" náklady ve finančních výkazech je mnoho. Zvláště tehdy, nejsou-li vnitřní kontroly organizace dostatečné a do etického povědomí zaměstnanců vedení před krizí neinvestovalo, jelikož samo nebylo přesvědčeno o přínosech takové investice.

To vše je samozřejmě špatně. Organizace, ať už veřejné, nebo soukromé, by neměly zapomínat na to, že krize, jako je tato, vytvářejí k podvodům vhodné podmínky, a proto by měly provést inventuru, jak jsou na případné nekalé jednání svých zaměstnanců na všech stupních řízení připraveny.

Technologická rizika

Zcela specifickými pro tuto dobu jsou pak rizika používání výpočetní techniky zaměstnanci při práci z domova. Přistupování do podnikových sítí přes domácí připojení k internetu, využívání pracovních počítačů pro soukromé účely (instalace neschválených programů, návštěva rizikových webů), sdílení dokumentů přes neautorizované platformy (např. privátní e-maily a externí úložiště) nebo chybějící šifrování pevných disků na podnikových zařízeních – to všechno jsou způsoby, jak lze nenávratně přijít o podniková data.

Proto je nyní více než dříve nutností, aby jednotliví uživatelé měli omezené možnosti měnit bezpečnostní nastavení svých koncových zařízení. A dále je kromě dalších opatření žádoucí zavádět technologie, které umožňují monitorovat provoz na jednotlivých zařízeních, a chrání tak podniky před ohrožením dat ze strany zaměstnanců (samozřejmě poté, co nasazení takové technologie projde příslušným schválením).

Jiná rizika spojená s nasazením informačních technologií již nejsou ve vztahu k pandemii tak unikátní. Nutnost rychle nasadit některá IT řešení se ale mohla podepsat na kvalitě zabezpečení jednotlivých systémů nebo ochraně dat v těchto systémech, a tím vystavit organizace významným reputačním problémům nebo sankcím ze strany regulátora. GDPR totiž nespí ani v době pandemie.

Konečně výjimečná doba neznamená, že by podniky měly rezignovat na sledování i těch „běžných" vnitřních a vnějších rizik spojených s kybernetickou bezpečností. Mezi vnitřní rizika patří obcházení IT kontrol ze strany superuživatelů, mezi externí rizika pak napadení systémů organizace hackery nebo stále populární phishing.

Rizika související s dodržováním právních předpisů

Poslední skupinou rizik, kterou do značné míry aktivovala pandemická krize, jsou rizika spojená s dodržováním právních předpisů. Nemyslím tím ona tradiční rizika compliance, jako je nedodržování legislativy proti úplatkářství nebo praní špinavých peněz (i zde ovšem může platit, že krize vytváří příležitosti). Spíše mám na mysli specifické regulatorní požadavky spojené jednak s čerpáním (omezené) veřejné podpory na provoz v době pandemie, jednak dodržování dalších opatření, která stát ukládá v souvislosti s bojem proti pandemické krizi. I na řízení těchto nových rizik musí organizace pamatovat.

Fungující řízení rizik jako předpoklad zvládnutí pandemie

Z dosud uvedeného je patrné, že pandemie vystavila podniky a organizace bezprecedentní zátěži. Je pravděpodobné, že z krize vyjdou s minimem ztrát, nebo dokonce posíleni ti, jejichž strategie se dokázala novým podmínkám rychle přizpůsobit a jejichž robustní finanční, IT a compliance kontroly dostatečně účinně snižují provozní rizika, včetně podvodu. Jinými slovy ti, kteří se v době před pandemií dokázali dobře připravit i na nepředvídatelné díky fungujícímu systému řízení rizik.

ŘÍZENÍ RIZIK V MINULOSTI: OPAKOVÁNÍ MATKA MOUDROSTI?

Celopodnikové řízení rizik

V době před pandemií byl proces řízení rizik v mnoha podnicích relativně autonomním subsystémem správy a řízení (corporate governance). Pokud byl na celopodnikové úrovni zaveden, bylo to často kvůli naplnění příslušných regulatorních požadavků (jako např. tzv. Enterprise Risk Management – ERM – vyžadovaný standardem COSO).

„Čím vyspělejší finanční řízení a robustnější vnitřní kontroly v klíčových procesech organizace má, tím úspěšněji se může vypořádat s dopady krize vyvolané pandemií.“

Tento celopodnikový proces řízení rizik měl sice ambici pokrývat všechny shora diskutované oblasti (tedy od strategických rizik přes finanční, operační, technologická až po rizika compliance). Činil tak však na relativně vysoké úrovni obecnosti. Katalog rizik obsahoval pro každou z těchto oblastí relativně generické scénáře, takže například riziko podvodného jednání bylo mnohdy v katalogu rizik vedeno jako jedna položka, přestože typů podvodů je nespočet.

Sběr dat ohledně pravděpodobnosti a dopadů rizik na straně jedné a kontrol, která tato rizika snižují, na straně druhé probíhal formou pohovorů s vybranými členy vedení společnosti, a to obyčejně jen jednou ročně. Data byla spíše kvalitativního než kvantitativního charakteru. Výsledky byly určeny nejvyššímu vedení, případně specializovaným výborům. Praktické dopady (ve smyslu zavádění konkrétních opatření vzešlých z posouzení úrovně rizika) bývaly omezené. A mnoho podniků a organizací na tomto místě – tj. u ERM aktualizovaného na roční bázi – také končilo.

Dílčí posuzování rizik

V hierarchii o úroveň níže, než byl ERM, ovšem stála i dílčí posuzování rizik, a to například podvodného jednání, nebo posuzování rizik spojených s nedodržováním právních předpisů. I v těchto případech vycházela povinnost tato rizika monitorovat z různých standardů. Tak např. posuzování rizika podvodného jednání stojí podle COSO samostatně vedle celopodnikového ERM. Přesto dopady těchto procesů byly, troufám si tvrdit, daleko praktičtější než u ERM. Bylo to dáno zejména následujícími důvody:

Především byla posuzovaná rizika definována konkrétněji než v případě ERM. Šlo zpravidla o specifické scénáře vycházející nejen z veřejně dostupných materiálů, ale i z interních šetření, a tedy vlastní „zkušenosti“ dané organizace.

Přestože posuzování probíhalo jako u ERM také zejména formou pohovorů s vyšším managementem, shromažďovaná data byla na rozdíl od ERM převážně kvantitativního charakteru, a umožňovala tak matematickou analýzu širší populace výpovědí. I přesto zde zůstával prostor pro doplnění kvalitativního hodnocení. To bylo důležité pro další rozšiřování katalogu rizik o nové scénáře.

„Již několik let před pandemií nicméně začalo být zjevné, že posuzovaní rizik v roční, a tím spíš v delší, například dvouleté frekvenci, přestává vyhovovat.“

Charakter dotazování umožňoval přidat do statistického vyhodnocení i další otázky, jako byla třeba tolerance ke konkrétnímu riziku. Tento parametr byl (a je) zvlášť praktický u těch rizik, která sice stávající kontroly dostatečně nesnižují, management si je ale této skutečnosti vědom a riziko přijímá.

Konečně statistická analýza umožnovala extrapolovat celopodnikové výsledky těchto posuzování na jednotlivé organizační součásti podniku, a to až na úroveň základních reportingových jednotek. Na této úrovni totiž byly k dispozici údaje o tržbách, nákladech, majetku a dalších položkách, které jednotlivé rizikové scénáře ohrožovaly.

Vypovídací schopnost výsledků těchto dílčích posuzování byla s to přesvědčit různé interní funkce, jako např. interní audit, compliance nebo internal controls, aby tyto výsledky zohledňovaly při plánování vlastních kontrolních aktivit.

Od opakujícího se k průběžnému posuzování a řízení rizik

Již několik let před pandemií nicméně začalo být zjevné, že pravidelné posuzování rizik v roční, a tím spíš v delší, například dvouleté frekvenci, přestává vyhovovat.

Spouštěčem změny vnímání mohly být v konkrétních případech například změny v top managementu organizace: prosazování agendy nového CEO vyžadovalo i intenzivnější zpětnou vazbu ohledně toho, jak na jeho opatření organizace reaguje a zda tato opatření nepřinášejí některé nezamýšlené efekty, které v posledku ohrozí celou transformaci podniku.

Katalyzátorem této změny pak byla vzrůstající dostupnost relevantních dat v datových skladech a postupné rozšiřování analytického softwaru pro jejich zpracování, včetně vizualizace. Otevřela se tak naplno cesta ke kontinuálnímu posuzování a řízení rizik.

PRŮBĚŽNÉ POSUZOVÁNÍ A ŘÍZENÍ RIZIK: POSTŘEHY Z PRAXE

Indikátory rizik jako klíč k průběžnému posuzování

Průběžné posuzování a řízení rizik v té podobě, jakou jsem zažil rodit se v praxi, je v zásadě kvantitativním hodnocením. Pro rizika, která již byla identifikována například v rámci ERM jako významná, se stanoví klíčové rizikové indikátory (Key Risk Indicators – KRI). Ty jednak musí dostatečně vypovídat o riziku a jeho proměnách v čase. Jednak musí jít o indikátory, které je možné relativně snadno „podchytit" existujícími daty a pomocí těchto dat je definovat.

Uvedu příklad: riziko podplacení zákazníků z veřejného sektoru je zvlášť významné pro společnosti kotované na amerických burzách. Z tohoto důvodu se na toto riziko zaměřují kontroly první, druhé i třetí linie obrany. Jak lze ale toto riziko průběžně monitorovat? Případy podplacení se přeci počítají těžko.

> **„Otevřela se tak naplno cesta ke kontinuálnímu posuzování a řízení rizik."**

Jednou z možností je identifikovat ty druhy transakcí, které jsou z pohledu aktivního úplatkářství rizikové. Patří mezi ně např. výdaje na reprezentaci. Třebaže nejsou jediným a zcela určitě nejsou také nejvýznamnějším typem transakcí, jejichž prostřednictvím lze podplácet, patří mezi „oblíbence" mnoha oddělení compliance. Vedení těchto útvarů si zpravidla vymiňuje udělení předběžného souhlasu s těmito výdaji od určité výše na jednoho příjemce.

Poměr těch výdajů na reprezentaci, u kterých jejich výše přesahuje stanovený limit na příjemce, vůči celkové populaci výdajů na reprezentaci může být určitým indikátorem rizika. Pokud jsou navíc k dispozici data ohledně schválení jednotlivých výdajů na reprezentaci ze strany útvaru compliance, lze tento indikátor rizika dále zpřesnit (neschválené nadlimitní výdaje versus celková populace výdajů na reprezentaci). A co víc: tuto analýzu lze využít pro průběžný monitoring, resp. audit těchto výdajů.

Příkladů významných rizik, u kterých se nabízí průběžné posuzování rizika prostřednictvím KRI, je mnoho; často však jde o finanční nebo provozní indikátory, které sledují jednotlivé funkce (např. controlling, výroba) na opakující se, nikoliv kontinuální bázi a reportují o nich opět v pravidelných intervalech.

Od zdrojů dat k jejich prezentaci

Ve všech těchto případech je největší výzvou učinit z opakování kontinuální proces. To však nejde bez příslušného technologického vybavení a personálu, který toto vybavení dokáže naplno využít.

V minulosti jsem pracoval v interním auditu globální organizace, který se rozhodl vlastními silami za použití ACL Direct Link vybudovat napojení na účetní data v hlavních systémech ERP, především SAP. Přestože se nakonec datová napojení vytvořit podařilo, šlo o proces relativně složitý a časově náročný.

Poté, co bylo k dispozici přímé napojení na jednotlivé účetní systémy, jsme spustili pilotní projekt kontinuálního posuzování rizik. Sponzorem tohoto projektu byl přímo viceprezident společnosti pro interní audit.

Cílem úvodní fáze projektu bylo určit relevantní rizika, jejich klíčové indikátory a definovat způsob výpočtu těchto indikátorů. Na této fázi se podíleli zástupci několika auditních skupin (IT, finance, compliance), přičemž každá z nich měla za úkol přispět vlastními indikátory na vytipovaná rizika. Hlavním kritériem pro zařazení indikátoru do této fáze projektu byla dostupnost dat pro vytvoření indikátoru.

V následujícím kroku jsme pro jednotlivé indikátory definovali zdroje dat, frekvenci jejich aktualizace, logiku výpočtu indikátoru a v neposlední řadě i vizualizaci zobrazovaných dat. Požadavkem na výstup z kontinuálního posuzování rizik měl být totiž dashboard umožňující hlubší analýzu příčin případných budoucích změn indikátorů.

> **„Příkladů významných rizik, u kterých se nabízí průběžné posuzování rizika prostřednictvím KRI, je mnoho."**

Výsledkem projektu byla sada klíčových indikátorů rizik pro vybraná významná rizika s nadefinovanými datovými zdroji a interaktivním rozhraním umožňujícím analýzu podkladových dat shromážděných v pilotní fázi. Výstupem byla i projektová dokumentace umožňující předání projektu.

CESTA DO BUDOUCNOSTI NA ZÁVĚR

V tomto článku jsem se snažil ukázat, že úspěšně zvládnutý, a nikoliv pouze formální systém řízení rizik je jedním z předpokladů pro úspěšné zvládnutí pandemické krize. Nový typ koronaviru totiž přinesl bezprecedentní rozsah problémů, s nimiž se podniky a organizace musely vypořádat, a to na všech úrovních.

Neustále se měnící situace zvyšující pravděpodobnost negativních dopadů jednotlivých rizik na nepřipravené pak jen podtrhla důležitost průběžného posuzování a řízení rizik v době krize. Trend, kdy podniky a organizace začaly alespoň prozkoumávat možnosti zavádění průběžného řízení rizik, byl však patrný i před covidem-19.

Průběžné posuzování a řízení rizik je do značné míry závislé na existenci relevantních dat, finančních i provozních. Současně ale platí, že tato data musí organizace umět ze stávajících systémů relativně jednoduše „vytáhnout“ a „přetvořit“ je v klíčové indikátory rizik. To je práce pro multidisciplinární tým, který by měl dostat příslušnou podporu od vedení společnosti.

Tím to ale celé nekončí. Pokud organizace zvládnou úspěšně těžit informace z dat, které již v současnosti vlastní, a získávat nová „velká“ data (např. prostřednictvím zapojení technologií na bázi „Internet of Things“), další stupeň, do kterého by měly postoupit, již může zahrnovat využití strojového učení pro řízení rizik.

V úvodu jsem vyjádřil přání vrátit se v čase před pandemii. Svoje přání na tomto místě změním a budu si přát posunout se o rok a půl napřed. Nejenže bych chtěl v budoucnu potkat všechny své blízké zdravé a při síle. Chtěl bych také vidět, jak nejen ty největší, ale i menší podniky a organizace úspěšně řídí svá rizika na kontinuální bázi a pracují přitom s daty v maximální možné míře. Pokud tomu tak bude, pak s námi každá pandemie bude mít mnohem větší práci. ■

Aktivní prevence podvodů vs. pouhá improvizace na pozadí dnešních změn

Dnes již snad my všichni – interní auditoři, forenzní auditoři, compliance officeři či profesionálové z příbuzných oborů – žijeme a přemýšlíme ve struktuře vnitřního řídicího a kontrolního systému a modelu tří linií obrany. Konkrétně v oblasti boje s podvody a nekalým jednáním obecně je tento model často realizován skrze prevenci a detekci v první linii, skrze dodatečnou reakci v druhé linii, kdy nad tím vším bdí nezávislý interní audit, který riziko podvodu bere v každé své zakázce ve třetí linii v potaz.

Filip Zelingr
ředitel Auditu, Řízení rizik, Compliance

Filip má více jak 20 let zkušeností, které strávil ve vedoucích pozicích většinou nadnárodních korporací v oblasti bankovnictví, výroby a neposlední řadě infrastruktury. Od nuly vybudoval dle nejlepší praxe řadu procesů a úspěšných týmů ve druhé i třetí linii obrany, které mají vždy alespoň jedno společné - „rizikový přístup". Filip je ve firmách často „hybatelem změny" poskytující kritický pohled na věc, rizikové ujištění, poradenství a ďáblovu advokacii. Pro vedení společnosti je pak v neposlední řadě Compliance strážným andělem. Jeho specializací jsou zejména Interní audit, Řízení rizik, Etika a Compliance, TOPO, Fraud risk management a Korporátní bezpečnost. Filip je zapálený motorkář, kouč, milující manžel a pyšný otec.

Pavel Javůrek
manažer Compliance a kontroly kvality výstavby

Pavel se nejprve více jak 5 let věnoval internímu auditu ve finančním sektoru v ČR a v Rusku. I v Letišti Praha začínal jako seniorní interní auditor, ale před 5 lety vstoupil do nových vod a nyní vede agendy Compliance a Fraud Risk Managementu. Vedle toho přibral více jak před rokem další výzvu a rozšířil činnost Fraud Risk Managementu a začal se podílet na budování nové funkce v oblasti kontroly stavebních investic, které nejen svým objemem v řádech miliard korun tvoří poměrně významnou část skupinových rizik.

Tento konzervativní přístup, který v sobě nese prvky reaktivní, detektivní i preventivní, byl budován po léta především ve finančním světě a postupně se rozšířil i do dalších oborů. Dnes je považován za nejlepší možnou praxi kontrolního prostředí, kterou většina vyspělých organizací a korporací přebírá do svého fungování. Bohužel ne vždy s důsledným zamyšlením nad konkrétními riziky a srovnáním jejich expozice s náklady a omezeními, které tento přístup jejich řízení přináší.

Řada z nás jistě zaznamenala nový knižní bestseller amerického autora Reeda Hastingse „Pravidlo žádných pravidel. Převratná firemní kultura, díky níž Netflix dobyl svět" popisující příběh světově známé mediální společnosti a její kulturu, kde nikdo neřeší, kolik a za co utratí zaměstnanci z firemního rozpočtu, a kde jediným závazným principem je vždy jednat v nejlepším zájmu společnosti.

Toto fungování „bez řízení a kontroly" či jeho obdoby aplikované zejména ve firmách startupového typu či ve společnostech nových moderních odvětví jsou zřejmě v příkrém kontrastu s výše popsaným, dnes již tradičním přístupem. Předpisy a ověřování jejich dodržování se pak mohou jevit jako přežitek, či dokonce jako zbytečná zátěž pro procesy a v konečném důsledku plýtvání zdroji. O to více by takto mohlo být smýšleno o prevenci a detekci nekalých jednání jako o něčem, co a priori naznačuje, že společnost zaměstnancům nevěří, či je dokonce podezřívá.

> **„Vystačí si firmy s pouze s principem jednat vždy v nejlepším zájmu společnosti?"**

Existují dnes opravdu důvody a obhajoba pro odklon od svázání firem pravidly a kontrolami či pro aplikaci přístupu pouhé reakce, až pokud se už nějaký podvod opravdu stane?

Toto zamyšlení se jeví aktuální nejen kvůli změnám, které jsou s námi již delší dobu, především změny ve společnosti, kultuře či technologiích, ale i v kontextu aktuální pandemie, a především pro přicházející dobu postcovidovou. Věříme, že opravdový život není tak černobílý, a proto se na tyto dva světy podíváme z různých úhlů pohledu.

Náklady

Náklady, které jsou klíčovou proměnnou v rozhodování každé společnosti, jsou generovány oběma modely boje s podvody. Aktivní prevence a detekce (za kterými vedle pasivních předpisů, školení a etických linek vidíme především hodnocení rizik podvodů, analýzy scénářů, vhodná procesní a systémová opatření, podpisová oprávnění, segregace odpovědností, schvalovací workflow, včasná varování, reporty a kontroly) představují paušální fixní výdaje, které vynakládáme, aniž bychom konkrétnímu nekalému jednání čelili. Peníze nás nestojí pouze ti, kteří tato opatření nastavují (druhá linie), ale i výkon daných opatření v první linii, jejíž činnosti jsou o tato opatření komplikovanější.

Model čisté reakce oproti tomu přináší pouze variabilní náklady na řešení konkrétních případů, kdy se riziko skutečně realizovalo, a oproti prvnímu modelu navíc i cenu části rizik, která by při správné prevenci a včasné detekci byla zachycena, a tak ani nenastoupila, nebo alespoň ne v takové míře. Touto optikou se aktivní prevence a detekce mohou jevit jako promarněné zdroje. Tak jednoduché to však není.

Na prevenci a detekci se musíme dívat i jako na investici. Ta má při správnosti prevence a včasnosti detekce vysoký potenciál některým případům úplně předejít nebo alespoň snížit dopady škod těch, které se i přes prevenci stanou. Díky znalosti procesů a jejich rizik získaným při nastavování aktivní prevence a detekce, je navíc firma snadněji schopná sama daný případ vyřešit interními zdroji a může ušetřit na službě externího vyšetřování. V případě incidentů, které by mohly být přičitatelné společnosti v rámci trestní odpovědnosti právnických osob (TOPO), může být samotná existence aktivní prevence, spolu s ostatními opatřeními compliance management systému, podmínkou dokládající, že společnost splnila to, co lze po ní spravedlivě očekávat, a tak i nutné podmínky pro své vyvinění.

Legislativa

Bez ohledu na vše ostatní jsou zde legislativní požadavky, především v podobě trestní odpovědnosti právnických osob a jednání s péčí řádného hospodáře, které nám v zásadě neumožňují vydat se cestou čisté improvizace, aniž bychom jakkoli nekalému jednání předcházeli. To však neznamená, že jsme našli jasnou odpověď na naši otázku.

„Firmy bez kontrol a byrokratického balastu se na první pohled mohou jevit jako flexibilnější a akceschopnější.“

Tyto požadavky jsou totiž obecné a dávají firmám možnost je aplikovat dle charakteru jejich businessu a přiměřeně jejich rizikům. To znamená např. dle požadavků zákona č. 418/2011 Sb. a tzv. spravedlivého očekávání, které vůči dané firmě v oblasti boje proti podvodům můžeme mít pro své případné vyvinění.

Problém spatřujeme v tom, že řada společností částečně alibisticky, někdy z pohodlnosti, či dokonce ze strachu, přistoupila k těmto požadavkům přehnaně s jistou dávkou paranoii, nebo univerzálně, aby si práci usnadnila, a prevenci vystavěla ve stylu jednoho univerzálního opatření à la „one fits all". V takovém případě pak alespoň pro část procesů či transakcí mohou taková opatření působit jako „kanón na vrabce" a nemusí být vždy potřebná, náklady na ně jsou neúměrné a jejich přidaná hodnota diskutabilní, protože často jsou čistě formální bez reálného efektu.

Konkurence a dopad na zákazníky

Z prevence a detekce nekalého jednání, a z kontrolního prostředí obecně, se vzhledem k výše uvedenému stala často věda, která řadu procesů a jejich rozhodovacích mechanismů přímo paralyzovala. Tohoto handicapu si však jsou dnes již některé společnosti i z tradičních odvětví plně vědomy. Vidí totiž, že především dynamické společnosti startupového typu se jim v některých ohledech mohou vzdalovat na ujíždějícím vlaku konkurence. Firmy bez kontrol a byrokratického balastu se jeví jako flexibilnější a akceschopnější v otázce svého rozhodování, reakce na požadavky zákazníků a v otázce obchodu a pokroku obecně.

Můžeme se domnívat, že možná i z tohoto důvodu právě tyto tradiční a konzervativní společnosti v posledních letech přicházejí s inovacemi např. v podobě agilního řízení. To však samozřejmě ze své podstaty neladí se striktním a zkostnatělým kontrolním systémem. Platí snad však, že při agilním řízení či ve startupech nevyžaduje riziko nekalého jednání aktivní prevenci a kontrolu?

Zaměstnanci, firemní kultura a reputace

Agilní řízení jde ruku v ruce i s jiným fenoménem, a to generační obměnou zaměstnanců. Převaha generace X, která vybudovala tradiční a v současnosti používané systémy řízení a kontroly, pomalu oslabuje. Nastupuje generace Y, „mileniálové", která již v roce 2020 tvořila 50 % globální pracovní síly. Mileniálové jsou sebevědomí, draví a vyžadují rovnováhu osobního a pracovního života. Zároveň se pomalu objevuje internetová a online generace Z. Obě tyto mladé generace přicházejí i s jinými hodnotami a potřebami. Chtějí individuální přístup, chtějí mít důvěru zaměstnavatele, chtějí být flexibilní, tvořiví, a nikoli svázaní rigidními složitými rozhodovacími mechanismy a kontrolami.

„Míra rizika podvodu a vhodná opatření budou tedy vždy dvě závaží na miskách vah."

Na druhou stranu ale tyto generace jistě také jsou, respektive v to alespoň vkládáme naděje, senzitivnější vůči nepravostem, chtějí se s firmou ztotožnit a důvěřovat jí, chtějí být na ni hrdí a není jim jedno, co se v ní děje. Věříme proto, že ocení to, že jejich zaměstnavatel aktivně předchází tomu, aby se stávaly věci v rozporu s těmito hodnotami. A jelikož se nebojí ozvat, mohou být v případě vzájemné důvěry, právě tito zaměstnanci přirozenými tvůrci prevence a strážci „compliance".

Technologický vývoj a digitalizace

Aktuálně silně akcelerovaný technologický pokrok, přechod do online světa, digitalizace procesů a jejich obecné zrychlování jistě otevírají prostor pro nové typy podvodů, čímž není nutně myšlen jen cyber crime. Stejně tak jako novým typům podvodů nabízí digitalizace prostor i novým, často efektivnějším a méně zatěžujícím nástrojům zejména v aktivní detekci, která může na vznik podvodu včasně poukazovat, a tedy působit do velké míry i jako prevence. Detekci nekalých jednání lze tak díky tomu významně zautomatizovat například zpracováním oněch digitálních dat za mnohem nižší náklady. Lze pak automaticky kontrolovat nikoli pouhé vzorky, ale rovnou celé datové populace. Kromě toho lze dnes díky nejrůznějším online nástrojům jednoduše vzdáleně, a přesto stále interaktivně, přinášet k cílovému publiku potřebné informace a myšlenky, a efektivně tak školit a neustále udržovat povědomí o otázkách etické kultury, která je nezbytným základem každé účinné prevence.

Pandemie a překotné změny

Realita dnešních dní, kdy provozy jsou utlumeny, transakcí ubylo, lidé se nepotkávají, pracují z domova a řada aktivit se překotně přenesla do online prostředí, jistě často vedla k tomu, že ubylo i standardních podnětů k ověření. Řada administrátorů etických linek jistě zaznamenala pokles v počtu „příchozích hovorů“. Je toto signálem, že výskyt nekalého jednání je menší? Nebo si lidé jen méně všímají, protože řadu věcí fyzicky opravdu nevidí? Nebo řeší snad jiné, hmatatelnější problémy či si jednoduše nestíhají všímat, protože řeší další agendu po kolegovi, který byl v rámci úspor propuštěn?

Změny způsobené současnou pandemií mohou naopak znamenat zesílení proměnných tzv. trojúhelníku podvodů. Transformace činností a jejich nástrojů mohou otevírat příležitost v nových či pozměněných a zatím neusazených procesech. Pod tlakem zklamání zaměstnanců, jejich strachu a tlaku na ně může být zvyšována jejich motivace a zároveň i posouvána subjektivní hranice, kdy si jako pachatel nekalé jednání vnitřně ospravedlní. Pandemii bychom tedy měli stejně jako jakoukoliv významnou změnu prostředí, významný růst či propad ekonomiky vnímat jako zvýšenou hrozbu podvodného jednání a věnovat se revizi kontrolního prostředí, jeho účinnosti a efektivity v reakci na tyto změny. Stejně tak lze tyto změny a krizi vnímat jako příležitost, „srovnat krok“ s podvodníky, a díky chytré prevenci a detekci za nimi nezaostat víc, než je nezbytně nutné.

„Na prevenci a detekci se musíme dívat i jako na investici.“

Závěrem

Ačkoli se může zdát, že legislativní požadavky bez ohledu na ostatní body dávají krátkou odpověď, že cestou čisté improvizace by se firmy ani v dnešní době vydávat zřejmě neměly, širší odpověď tak jednoduchá není. Žádný z extrémů – ani „no rules firma“, ani zkostnatělá a pravidly či kontrolami paralyzovaná korporace – není správným řešením. Optimální nastavení je vždy mixem z obou světů ve správném poměru, unikátním pro každou společnost a její procesy, kdy je riziko podvodného jednání a investice

do vhodného kontrolního prostředí v rovnováze. Je však vždy nutné pečlivě počítat všechny náklady, které s sebou kontrola nese. Přímé ve formě nákladů na její vlastní výkon, ale i nepřímé ve formě zpomalení procesu, snížené obchodní či jiné flexibility, a tedy i možné ztráty potenciálních, či dokonce stávajících zákazníků. Stejně tak je tomu ovšem s výnosy. Vedle existujících výnosů je třeba brát na zřetel jejich nutné snížení o latentní realizované podvody, tedy vlastní cenu rizika podvodu. Některé renomované průzkumy, např. ACFE, hovoří totiž až o 5 % z obratu firmy.

„Optimální nastavení je vždy mixem z obou světů ve správném poměru.“

V konečném důsledku je tedy dle našeho názoru vždy nejefektivnější cesta aplikace všech ověřených složek reakce, detekce, ale i prevence podvodných jednání. Tou klíčovou proměnnou je však již jejich zmíněná přiměřenost a vhodný a unikátní poměr šitý dostatečně chytře a na míru konkrétnímu riziku dané společnosti. Míra rizika podvodu a vhodná opatření budou tedy vždy dvě závaží na miskách vah.

Výše rozebírané změny a fenomény by pro společnosti měly být impulsem pro revizi nastaveného systému, aby vždy reflektoval stav na trhu, vnímání zaměstnanců, technologický pokrok, fázi ekonomického cyklu každé společnosti i další proměnné. Tyto změny tak budou na pomyslných vahách jen dalšími závažíčky, která je budou průběžně překlápět ze strany na stranu. ■

Ing. Jan Bukovský
Vedoucí oddělení Bezpečnost ICT
Česká exportní banka, a.s.

PREVENCE RIZIK KYBERNETICKÉ BEZPEČNOSTI

Základní rizika v oblasti kybernetické bezpečnosti

I když oblast kybernetické bezpečnosti je velmi rozsáhlá, základních rizik není mnoho – zato však obvykle mohou vzniknout mnoha způsoby.
Obecně se jedná zejména o rizika, spojená s níže uvedenými hrozbami *(viz tabulka na konci článku; hrozby uvádí její první sloupec)*.

Rozdělení hrozeb a zranitelností je velmi detailně popsáno v Příloze 3 vyhlášky 82/2018 Sb. (Vyhláška o kybernetické bezpečnosti). Jsou zde zmiňovány i některé hrozby obecného charakteru, v tabulce neuvedené (např. užívání v rozporu s licenčními podmínkami, nedodržení smluvních závazků, nedostatek kvalifikovaných zaměstnanců apod.). Pro provedení analýzy rizik lze využití příloh 1–3 vyhlášky 82/2018 Sb. rozhodně doporučit, a to i tehdy, pokud se na vaši organizaci Zákon o kybernetické bezpečnosti a vyhláška 82/2018 Sb. přímo nevztahuje.

Co je potřeba udělat, aby byla rizika pokryta?

Opatření k pokrytí uvedených rizik je celá řada. Dělí se na:

Měkká – popsaná/předepsaná bezpečnostní politikou, smlouvami, dokumentací apod. (jde též o tzv. režimová opatření, která stanovují postupy činností tak, aby to při dodržení opatření ztížilo možné napadení systému).

Tvrdá – vynucená technickými prostředky.
Při výběru opatření musí mít vždy přednost tvrdá opatření, pokud jsou samozřejmě pro danou oblast dostupná, protože splnění měkkých opatření nelze nikdy plně garantovat.

Kybernetickou bezpečnost je třeba řešit komplexně – podcenění některé oblasti má obvykle fatální následky pro bezpečnost celého IT prostředí.

Základní podoblasti kybernetické bezpečnosti, které je třeba pokrýt:

- **Fyzická bezpečnost prostředí IS/IT**

Jde o zajištění budovy proti neoprávněnému vstupu nebo pohybu fyzických osob.

„Při výběru opatření musí mít vždy přednost tvrdá opatření, pokud jsou samozřejmě pro danou oblast dostupná, protože splnění měkkých opatření nelze nikdy plně garantovat.“

Typická tvrdá opatření jsou montáž ochrany pláště budovy (mříže, turnikety, kamery apod.), montáž ochrany kanceláří a serveroven (zámky, skříně/trezory, zaznamenávání průchodů, EZS – elektrická zabezpečovací signalizace…). Typická režimová opatření jsou zapisování/označování příchodů, postupy pro ostrahu objektu…

Patří sem i obrana proti odposlechu pomocí špionážních technik (bezpečnostní prohlídka prostor organizace).

- **Administrativní bezpečnost IS/IT**

Jde z principu o měkká opatření – zejména vytvoření a kontrola bezpečnostní politiky a další bezpečnostní dokumentace.

Dále sem patří např. různá IT dokumentace, analýza rizik, katalogy objektů…

- **Bezpečnost zařízení**

Jde o zajištění jednotlivých HW aktiv, zejména serverů, uživatelských počítačů, notebooků, smartphonů, tiskáren. Patří sem i přenosná média (CD, DVD, USB flash disky).

Cílem je v první řadě bránit napadení škodlivým kódem (malwarem) – naprostou nutností je na všech zařízeních, kde je to možné, mít nasazen antivir a zajistit jeho pravidelný upgrade na denní bázi. V současnosti bývá antivir doplněn též např. prostřednictvím řešení EDR (Endpoint Detection and Response), které sleduje nejen ukázky virů (signatury), ale i chování koncového zařízení.

Dále je třeba zajistit a stále sledovat aktuálnost důležitého programového vybavení (nasazení záplat, tzv. patchů).

Třetí významnou oblastí je optimální nastavení operačních systémů na těchto zařízeních (ve Windows prostředí obvykle pomocí zásad v Group Policy).

Měkká opatření by v této oblasti měla zakázat uživatelům rizikové chování (např. přístup na nebezpečné stránky na Internetu) a popsat postupy pro případ odcizení nebo ztráty přenosných zařízení a médií. Dále sem patří popis nastavení jednotlivých zařízení (tzv. konfigurační standardy), patchovací plány apod.

- **Personální bezpečnost IS/IT**

Vlastní personální bezpečnost obsahuje pouze měkká opatření. Jde především o prověření minulosti nastupujících zaměstnanců a pravidla, jak postupovat v případech, kdy zaměstnanci poruší některá bezpečnostní opatření (kázeňské tresty). Dále sem patří pravidelná bezpečnostní školení zaměstnanců (udržování „bezpečnostního povědomí“). Někdy se sem též zařazují opatření ze sociální bezpečnosti, včetně např. blokování spamů a phishingu.

- **Bezpečnost komunikací a provozu**

Jde o kritickou oblast, kde je nasazena většina tvrdých řešení.

V první řadě se zde musí vyřešit ochrana tzv. bezpečnostního perimetru, tj. vstupní hranice, oddělující Internet a vnitřní síť (nasazení firewallů a údržba pravidel na nich, vytvoření a správa tzv. „demilitarizované zóny“, kde bývají např. proxy, sandboxy, zařízení pro správu mobilních zařízení a pro vzdálené přístupy a podobné prvky).

Dále sem patří i bezpečné zapojení vnitřní sítě (např. bezpečné a udržované vnitřní aktivní prvky – tj. switche, routery a rozdělení sítě do menších virtuálních sítí – VLAN).

Oblast obsahuje i mnoho dalších řešení – např. bezpečné ukládání a pravidelné vyhodnocování logů, pravidelné zálohování a bezpečné ukládání záloh, případně přídavná řešení pro zvýšení bezpečnosti vnitřní sítě (Intrusion Prevention System – IPS, Data Loss Prevention – DLP, sledování intenzity provozu – NetFlow apod.)

Oblast je velmi rozsáhlá, a její detailní popis se vymyká rozsahu článku (bylo by to spíše na několik knih).

- **Řízení přístupu k informačním systémům**

Cílem tvrdých opatření v této oblasti je jednak zajistit bezpečnou autentizaci uživatele (tedy dostatečně silné heslo, odolné proti prolomení nejméně v rozsahu do tří měsíců, popř. jiný bezpečný způsob autentizace) a jednak přidělení přístupových práv ve všech prostředích a aplikacích pouze v tom rozsahu, který uživatel nutně potřebuje.

„Naprostou nutností je na všech zařízeních, kde je to možné, mít nasazen antivir a zajistit jeho pravidelný upgrade na denní bázi.“

Součástí oblastí je i Active Directory (nebo jiný LDAP systém – Lightweight Directory Access Protocol) – tedy nastavení bezpečnostních skupin, vztahy mezi různými doménami apod.

Zvlášť bedlivě je nutné sledovat, zda nedochází k nadměrné kumulaci administrátorských práv a vůbec aktivity administrátorů.

Mezi měkká opatření patří různé mapy práv a také postupy, které určují, kdo, komu a za jakých podmínek smí práva přidělit.

■ **Zavádění nových produktů do provozu**

V této oblasti tvrdá opatření mohou zajistit hlavně vývojáři – tím, že využívají zásady bezpečného vývoje a předcházejí při vývoji známým zranitelnostem (např. SQL Injection, Cross Site Scripting). Jiným tvrdým opatřením je důsledné oddělení „ostrého" a testovacího prostředí.

Mezi režimová opatření patří např. testování kódu před nasazením, formalizace zásad změnových řízení, školení uživatelů apod.

■ **Bezpečnost při přístupu třetí strany**

Hlavním opatřením je důsledné dodržování zásad pro spolupráci s třetími stranami (obvykle popsáno smluvně – jak z pohledu dodržování SLA – Service Level Agreement, tak z pohledu bezpečnosti). Pokud jsou třetí straně poskytnuty vzdálené přístupy, je nutné je velmi detailně monitorovat, pokud pracují fyzicky v prostředí organizace, je třeba, aby je stále někdo doprovázel a kontroloval.

■ **Řešení výjimečných situací**

Režimově je nutné mít připravené, aktualizované a otestované plány pro případ havárie nebo mimořádné události.

Tvrdým opatřením je zřízení záložního pracoviště, které je schopno převzít provoz v případě mimořádné události (požár, povodeň apod.). Jeho součástí bývá i náhradní zdroj elektřiny, náhradní připojení k Internetu apod. V době pandemie je tvrdým opatřením zřízení velkého počtu vzdálených přístupů pro zaměstnance (to musí být doplněno režimově – popisem náhradních postupů, např. pro porady, pro podpisování, pro náhradu tisků).

■ **Nezávislé prověření IT bezpečnosti**

Je obvykle úkolem interního nebo externího auditu, a to včetně následných prověření odstranění zjištěných nedostatků.

Patří sem však rovněž různé organizací objednané kontroly (penetrační testy, analýzy apod.)

Závěrečný příklad

Pokud se nyní vrátíme k tabulce rizik, můžeme ji snadno doplnit o příklady opatření, která rizika omezují (poslední sloupec):

Hrozba	V tom obsaženo	Vzniká například	Příklady možných opatření
Ztráta/Únik dat	Krádež dat Nepovolená publikace dat Odposlech komunikace Využití špionážních technik Zneužití vyměnitelných nosičů dat	Úmyslným zaviněním zaměstnance Chybou zaměstnance Úspěšným útokem nebo spamem	Školení zaměstnanců, kázeňské tresty IPS (Intrusion Prevention System), virtuální sítě VLAN Bezpečnostní prohlídka (hledání „štěnic") Zašifrovaná média, režimová opatření pro přenášení dat
Ztráta kontroly nad vlastní technikou/ /prostředím	Škodlivé kódy (malware) Selhání ochrany bezpečnostního perimetru Narušení fyzické bezpečnosti Sociální útok	Zavirováním Povýšením práv útočníka na administrátora	Antivir, EDR Firewally a pravidla na nich, proxy, sandbox Mříže, kamery atd. Školení zaměstnanců, obrana mailu proti phishingu
Porušení nebo zničení dat	Odepření služby Neoprávněná modifikace údajů Pochybení zaměstnance	Chybou aplikace Selháním zálohování Úmyslnou aktivitou útočníka	Bezpečný vývoj aplikace, nasazení nových záplat-patchů Sledování logů, v nejhorším forenzní šetření Zálohování
Porušení nebo zničení infrastruktury	Odepření služby Selhání zařízení Ztráta nebo odcizení zařízení	Chybou HW techniky Chybou administrátora	Nasazení nových záplat-patchů Kvalitní údržba, zálohování Fyzická opatření, režimová opatření pro případ ztráty
Neplnění legislativních požadavků	Sankce	Chybou zaměstnanců Nezapracováním požadavků legislativy do postupů organizace	Zejména režimová opatření – dokumentace, Kontrolní činnost a nezávislý audit
Ztráta identity uživatelů	Zcizení autentizačních údajů	Úspěšným útokem nebo spamem Chybou zaměstnance (prozrazením třetí osobě)	Sledování logů, patchování, obrana mailu proti phishingu Školení zaměstnanců
Neoprávněný přístup k aktivům	Chybné přidělení přístupových oprávnění	Chybou administrátorů nebo osob rozhodujících o přístupových oprávněních Úspěšným útokem nebo spamem	Sledování logů (sledování změn práv na denní bázi) Sledování aktivit adminů Kvalitní hesla nebo autentizační mechanismy
Zhroucení organizace v důsledku vnějších vlivů	Neschopnost po dobu dnů provozovat IT systémy	Nezvládnutím úkolů kontinuity podnikání Katastrofickou kombinací vnějších vlivů	Postupy kontinuity podnikání Záložní pracoviště, náhradní zdroj elektřiny

(Jde pouze o příklady, v žádném případě nejde ani o úplný seznam rizik, ani o jejich úplné pokrytí všemi možnými způsoby). ■

PROČ A JAK ÚTOČÍ HACKER?

Kybernetická bezpečnost je v současnosti velmi ožehavé téma týkající se nás všech. Zkusme se tedy na chvíli vžít do role útočníka, abychom lépe pochopili, jak se hacker připravuje, co ho motivuje a jak útok provádí.

Stát se hackerem není tak složité, jak by se mohlo zdát. Stačí logické a kreativní myšlení, a samozřejmě do detailu rozumět technologiím, na které se chce útočník zaměřit. Útočníci se mnohdy specializují na webové aplikace, cloudové služby nebo síťová zařízení. Technologie se dají naučit. Ať už jako samouk – na internetu se dá dohledat spousta kvalitního materiálu – nebo na vysokých školách, kde se obory zabývající se tématem etického hackingu těší čím dál větší oblibě. Etický hacker má tudíž za úkol ověřovat bezpečnostní mechanismy aplikací či infrastruktury za pomocí simulací kybernetických útoků. Tedy pomáhat společnostem identifikovat zranitelnosti, aby případný ilegální útok byl neúspěšný. Může se samozřejmě stát, že etický hacker přejde na druhou stranu a stane se z něj „Darth Vader", ale co ho k tomu může vést? Vidina velkých peněz bývá častou motivací, ale stejně tak se může jednat o pocit volnosti, touhu se zviditelnit, něco ovládat nebo se prostě zabavit.

Pro jednoduchost rozlišme útočníky na dvě skupiny. Ta první útočí více méně náhodně – nemá konkrétní objekt zájmu. Největší motivací jedince z této skupiny bývá vidina finančního zisku. Využívají často technik phishingu a ransomwaru, s pomocí kterých se dá jednoduše zaměřit na velké množství cílů. S rostoucím povědomím o kybernetické bezpečnosti se samozřejmě obranné mechanismy společností i poskytovatelů veřejných služeb stále zdokonalují, tudíž i útočníci musí být kreativnější. V praxi to znamená, že se zaměřují na specifická odvětví, téma nebo regiony.

Druhá skupina má jasný konkrétní cíl. Firmu, osobnost, státní či veřejné instituce. Bývá organizovaná, seskupuje experty na různé technologie a koordinuje svůj postup. Disponuje finančním zázemím a používá kombinaci pokročilých technik. Útok může trvat měsíce i roky, bývá často postupný se snahou být co nejméně viditelný. Využívá technických zranitelností v systémech, ale i metody sociálního

Michal Merta
ředitel Cyber Fusion Centra
Accenture

inženýrství, nebo kompromitaci dodavatelů a jejich služeb či softwaru.

A jak takový útok vypadá? V oblasti bezpečnosti je jedním ze základních pojmů bezesporu zkratka „CIA“ – confidentiality, integrity, availability. Útočník se pokouší alespoň jednu položku z této triády kompromitovat. Pokud se jedná o „*confidentiality*“, tedy důvěrnost, snahou je získat přístup k datům nebo operacím, ke kterým za normálních okolností nemá práva. Může se jednat o krádež citlivých dat, získání administrátorského oprávnění, odposlouchávání komunikace apod. Útočník může využít slabin v kódu aplikace a použít např. techniky jako SQL Injection, Cross-Site scripting (XSS). V oblasti infrastruktury a na úrovni operačních systémů se zneužívá neaktualizovaných či špatně nakonfigurovaných komponent v kombinaci s buffer overflow útoky.

„Může se samozřejmě stát, že etický hacker přejde na druhou stranu a stane se z něj ‚Darth Vader‘.“

Druhou položkou CIA je „*integrity*“ a v takových případech se útočník snaží pozměnit data, přepsat zdrojový kód, poškodit hardware nebo systémy. Jako příklad takového útoku lze uvést ransomware. Jedná se o škodlivý software, který v případě oprávnění zápisu na disk zašifruje data v současné době neprolomitelným algoritmem. A jediná možnost, jak data zpět rozšifrovat, je mít k dispozici dešifrovací klíč.

Třetí položkou je „*availability*“ – dostupnost služeb. Určitě jste slyšeli o takzvaných DoS (Denial of Service) a DDoS (Distributed Denial of Service) útocích. Cílem útočníka je odepřít přístup na službu, aplikaci či server za použití škodlivého kódu a v případě DDoS k tomu využívá armádu již nakažených počítačů, tzv. botnet.

Je třeba se zamyslet nad faktem, že tyto principy nejsou aplikovatelné pouze na svět IT, ale podobným způsobem lze útočit na OT i SCADA systémy. Jako příklad uvedu převzetí kontroly nad kamerou ve veřejných prostorech (porušení principu důvěrnosti), vzdálené ovládání semaforů na křižovatce (porušení principu integrity) nebo ochromení výrobní linky (porušení principu dostupnosti).

Každá společnost by měla být schopna rozpoznat, že se děje něco nekalého. Někdy dostává i podnět od třetích stran nebo samotných útočníků. Ne vždy se ale jedná o kybernetický útok. Situací, kdy útočník deklaruje úspěšný útok a ohání se interními daty společnosti, opravdu přibývá. Ale kde data vzal? Nejsou náhodou dostupná někde na internetu? Proto je třeba každé podezření důkladně vyšetřit a zde přichází na řadu tým vyšetřovatelů. Jedná se o experty na forenzní analýzu, kteří zkoumají, co se opravdu stalo, jaký to má dopad na společnost, a případně sbírají důkazy pro další šetření. Zaměřují se na hledání indicií útoku v síťovém provozu, na pevných discích, ale i v operační paměti. Obvykle pracují ve skupinách, v zabezpečených pracovištích, aby nikdo nemohl důkazy změnit nebo odcizit. Výsledkem šetření by měla být jasná odpověď na otázku, zdali se opravdu jednalo o kybernetický útok, nebo to byl planý poplach.

Pokud víme, že jsme oběti kybernetického útoku, je dobré se obrátit na policii, jelikož mohou mít zkušenosti s velmi podobným typem napadení, využívajícím například stejného malwaru. Pokud dojde k jakémukoliv porušení bezpečnosti osobních údajů, které může mít za následek ohrožení práv a svobod fyzických osob, je třeba případ ohlásit Úřadu pro ochranu osobních údajů. Od roku 2018, kdy vstoupilo v platnost obecné nařízení o ochraně osobních údajů (tzv. GDPR), hrozí firmě v případě narušení bezpečnosti osobních dat i pokuta ve výši až 20 milionů eur. Závěrem bych rád zmínil v poslední době velmi populární „bug bounty“ programy. Jedná se o veřejnou výzvu, kde společnosti nabádají jednotlivce k hledání bezpečnostních zranitelností v aplikacích pod příslibem odměny. Ta může spočívat v samotném uznání, dárku nebo finančním ohodnocení. Výhodou takového programu je, že aplikace je opakovaně testována experty používajícími různé techniky i nástroje a pravděpodobnost odhalení bezpečnostních rizik je samozřejmě vyšší. Ne každá společnost se ale touto cestou vydává, a ne pro každou společnost je bug bounty program vhodný. Vždy je nutné zvážit všechny aspekty a právní dopady. ■

PODVOD, ANEB NOČNÍ MŮRA AUDITORA

**Zdál se mi sen, že se nebe hroutí...
Ne, nebudeme zpívat s kapelou Spirituál kvintet. V sobotu ráno jsem se probudil ze snu, ve kterém si mě zavolali generální a finanční ředitel mojí společnosti a doslova na mě vybafli, že z účtu společnosti zmizelo pár milionů, a že účetní se zhroutila poté, co se jí zeptali kam to poslala. Jako auditor jsem prý liška podšitá a mám rychle přijít na to, kam peníze zmizely a jestli to účetní neposlala na svůj vlastní účet. Samozřejmě tento podvod budeme muset jako společnost nahlásit, ale než se nám to ve firmě začne hemžit policisty, kontrolory různých dozorových orgánů a hlavně novináři, tak mám něco zjistit, ideálně okamžitě.**

Kateřina Schovánková Nejedlá
innogy Česká republika a.s.
Legal&Compliance
Managing Auditor

Martin Dohnal
GasNet, s.r.o.
Regulatory, Legal&Internal Audit
Senior Auditor, Internal Audit

Tento celkem živý sen, a hlavně jeho podstata, mi nešly z hlavy celé dopoledne a začal jsem přemýšlet, zdali by se takový scénář mohl v naší společnosti ve skutečnosti stát a jak bychom na to, jako společnost, mohli reagovat.

Jak by mohl takový podvodný scénář vypadat? Jeden ze scénářů podvodného jednání může spočívat v tom, že se do systému naší společnosti dostane informace o tom, že jeden z našich obchodních partnerů, se kterým dlouhodobě obchodujeme mění bankovní účet s tím, že další platby máme realizovat na nový, aktualizovaný bankovní účet. Pokud navíc je tato informace na papíru s logem společnosti a přijde i z e-mailové adresy dané společnosti, je důvěryhodnost takové informace značná. V tu chvíli nikoho nemusí napadnout, že se jedná o pokus podvodníka odklonit platby našemu obchodnímu partnerovi na cizí bankovní účty.

Jak ale rozlišit podvodníka od obchodního partnera, který doopravdy změnil bankovní účet a upozornil nás na to?

Ve společnosti máme zavedený systematický přístup k identifikaci a hodnocení rizik. Za tuto oblast odpovídá oddělení řízení rizik, které spravuje katalog již identifikovaných rizik a pravidelně jedná s manažery o aktuálních rizicích pro společnost, o jejich dopadech a o opatřeních, které mají snížit pravděpodobnost výskytu. Zároveň platí, že interní auditor pravidelně hodnotí úroveň zvládání rizik v jednotlivých procesech, a pokud narazí na významné riziko, které není systematicky řízeno, tak jej s oddělením rizik komunikuje.

Máme ve společnosti identifikované riziko neautorizované změny bankovních účtů dodavatelů? Víme, jaká opatření realizuje management ke snížení toho rizika? Ano, máme a víme.

V řídicí dokumentaci týkající se změny kmenových dat dodavatelů je definované pravidlo pro pracovníky, kteří mají v systému dovoleno měnit kmenová data dodavatelů. Změny mohou být činěny pouze na základě prověření bankovního účtu v Administrativním registru ekonomických subjektů (ARES) vedeném Ministerstvem financí ČR (pouze u ekonomických subjektů, které jsou v ČR registrovány k DPH), a pokud to není možné, tak na základě uzavřeného dodatku ke smlouvě s daným dodavatelem. V případě, že se jedná o zahraničního obchodního partnera a uzavřením dodatku ke smlouvě nechceme otvírat možnost jednat o dalších parametrech smlouvy nebo by uzavření dodatku bylo časově náročné a nechceme posouvat splatnost faktur, tak je stanovená výjimka a odpovědní pracovníci (z oddělení nákupu) kontaktují dodavatele a informaci si u něj nechají písemně ověřit. Tyto výjimky jsou monitorovány a nákupčí musí každou výjimku umět zdůvodnit managementu. Kromě daného postupu jsou nákupčí a všichni, kdo mohou měnit kmenová data obchodních partnerů, pravidelně proškolováni a seznamováni nejen s interními předpisy a postupy, ale také se scénáři podvodného jednání a jejich dopady.

Jak může auditor tento podvod odhalit?
Každý auditor musí při uplatňování náležité profesní péče vzít v úvahu mimo jiné pravděpodobnost výskytu významných chyb, podvodů nebo odchylek, tak jak říká standard 1220.A1. Další standard 2060 zmiňuje, že zprávy musí též obsahovat zjištění týkající se významných rizik, řídicího a kontrolního systému, včetně rizik podvodu a dále zjištění ohledně řízení a správy společnosti a dalších záležitostí, které vyžadují pozornost vedení a/nebo orgánů společnosti. Podvodům se věnuje i standard 2120.A2, který uvádí, že interní audit musí hodnotit možnost výskytu podvodu a způsob, jakým společnost řídí riziko podvodu. Při sestavování programu auditu musí auditor zvážit pravděpodobnost výskytu významných chyb, podvodu, odchylek a ostatních rizik (standard 2210.A2). Takže ano, auditor by se měl při plánování každého auditu a při diskusích o konkrétním zaměření auditu zamyslet nad tím, jakým způsobem odhalit případné podvodné jednání a zanést riziko podvodu do hypotéz, které bude během auditu ověřovat.

Jak může auditor poznat, že v rámci auditní zakázky má ověřit konkrétní podvodný scénář? Do jisté míry se jedná o schopnost a zkušenost auditora, ale v daném případě se může opřít o informace z katalogu rizik a v ověřovaných hypotézách posoudit, zda nastavený proces změn kmenových dat je funkční a zda fungují i zavedené kontrolní mechanismy.

Pokud auditor identifikuje nesrovnalosti, které mají věcný potenciál podvodného jednání, měl by si být vědom závažnosti takového zjištění a měl by okamžitě informovat vedení společnosti.

Společnosti se s podvodným jednáním nesetkávají každý den, a proto informace o možném podvodu může vyvolat několik typů reakcí vedoucích zaměstnanců – od pochybovačného „to se nestalo“ až po panické „co budeme teď dělat“. Tam, kde si již podobnou situací prošli, ví, že závažná podezření musí být systematicky prověřena.

Má auditor dostatečnou kompetenci pro takové šetření?
V mnoha případech mohou společnosti nabýt dojmu, že interní auditor, který identifikoval zjištění podezření podvodného jednání je tou správnou osobou, která by měla provést i vlastní šetření. Standard 1210.A2 sice předpokládá kompetenci interního auditora pro hodnocení rizika podvodu a způsob, jakým je dané riziko řízeno, ale zároveň neočekává schopnost podvod odhalit a vyšetřit. Jinými slovy: „standardní“ interní auditor není podle standardu tou správnou osobou a společnost by se měla poohlédnout po specialistech v daném oboru. Na trhu jsou dnes kapacity jak v globálních auditorských firmách, tak i v malých úzce specializovaných společnostech. Ideální je, mít uzavřenu alespoň rámcovou smlouvu nebo vědět, kam se v nouzi obrátit. Nicméně víte, jak to v mnohých společnostech chodí: „… do doby, než někoho najdeme, to povedeš ty“. A najednou je v tom auditor až po uši.

Je třeba si uvědomit, že v mnoha případech se pohybujeme na hraně právního rámce a naše nekompetentnost by mohla vést k negativnímu ovlivnění výsledku šetření nebo až ke konfliktu se zákony. Naštěstí v naší společnosti máme interní auditory vzdělané a zkušené na poli vyšetřování interních podvodů a v obzvlášť komplikovaných případech si můžeme vypomoci forenzními specialisty dodavatele.

Společnost by rovněž měla předem procesně vědět, jak se v případě zjištění podezření podvodného jednání zachová, kdo bude odpovědný za realizaci šetření, komu se bude reportovat, jak se bude komunikovat dovnitř společnosti i ven a jak se naloží s výsledkem šetření.

V naší společnosti tyto instituty máme nastaveny. Identifikované podezření je nejdříve diskutováno v úzké skupině vrcholových manažerů, která posoudí stupeň závažnosti a rizika pro společnost a pokud se dojde k závěru, že je riziko pro společnost neakceptovatelné, jsou aktivovány takové kapacity, které rychle a profesionálně zasáhnou.

Procesy tedy máme v naší společnosti zvládnuté a víme, jak v tomto případě postupovat. Teď ale zpátky k mým úvahám o snu a rozhovoru s plačící účetní. Kromě tzv. „hard skills“ popsaných výše totiž musí interní auditor disponovat i řadou „soft skills“, které mnohdy přímo ovlivňují výsledek šetření. Patří mezi ně i to, jak vést rozhovory se zaměstnanci, když mám podezření na podvodné jednání? Liší se nějak od klasických auditních rozhovorů?

V první řadě je potřeba si položit otázku, co je cílem rozhovorů? Při standardním auditním rozhovoru má auditor za cíl dozvědět se a pochopit, jak funguje

systém nebo proces. Snaha je, vést rozhovor v otevřené, přátelské rovině, naladit se na zaměstnance a dozvědět se od něj maximum o tom co dělá, jak to dělá, zda by to nešlo dělat nějak jinak, jak srozumitelná je mu interní dokumentace.

Při rozhovoru, kde existuje podezření na podvodné jednání je třeba věnovat přípravě daleko větší péči. Dost často není zřejmé, zda je zaměstnanec ten, kdo chce společnost poškodit, zda s takovou osobou vědomě spolupracuje, je to náhodný svědek, kterého, když se auditor správně zeptá, tak se dozví užitečné informace, nebo je to zaměstnanec, který s daným podvodem nemá vůbec nic společného a stal se jen obětí podvodníka. Auditor by si měl promyslet strategii dalšího postupu a uvážit rizika plynoucí z nesprávně vyhodnocených indicií a možné dopady, měl by komunikovat s nejvyšším vedením společnosti a znát případný další postup. Pokud je způsobená škoda v takové výši, že vedení chce podat trestní oznámení, měl by auditor tuto skutečnost zahrnout do svých strategií při rozhovorech. Neobratně vedené rozhovory mohou vyplašit zaměstnance, kteří jsou angažováni v podvodném scénáři a ti mohou začít zakrývat stopy (mazat elektronické dokumenty, skartovat fyzické dokumenty, ovlivňovat kolegy) a tím ztížit následnou práci orgánů činných v trestním řízení. Na straně druhé je potřeba v každé situaci si být vědom skutečnosti, že kompetence auditora není na úrovni orgánů činných v trestním řízení a zaměstnanci s ním komunikují dobrovolně.

Na co se tedy při takovém rozhovoru zaměřit? Rozhodně by takový rozhovor neměl provádět jeden auditor, ale dva. Pokud je to možné, může si auditor takový rozhovor nahrát (měl by se však poradit se svým DPO, aby nedošlo k porušení GDPR). Pokud nechce nebo nemůže rozhovor nahrát, může být dobré přizvat ještě jednoho auditora, který bude mít roli zapisovatele. Jeho jediným úkolem by bylo vše co nejvěrněji zaznamenat. Auditoři by při plánování rozhovoru měli zejména zohlednit tyto parametry/otázky/skutečnosti:

- S kým mluví a jakou informaci jim dotyčný zaměstnanec může dát? (potenciální pachatel, svědek, běžný zaměstnanec atd.).
- Role jednotlivých auditorů – ten, kdo vede rozhovor, druhý pozoruje neverbální komunikaci, případně třetí zapisuje.
- Změna situace/nálady během rozhovorů – co dělat, když auditor, který vede rozhovor není schopen navázat kontakt se zaměstnancem? Co dělat, když se situace během rozhovoru vyhrocuje či eskaluje? Co dělat, když protistrana má emocionální slabou chvilku a buď se rozpláče nebo naopak rozčílí? Druhý auditor by měl být natolik obeznámen s cílem rozhovoru a s připravenými otázkami či tematickými okruhy, že je bez mrknutí oka schopen převzít rozhovor a role si vyměnit.
- Jakou náladu/atmosféru chtějí auditoři nastolit? Pokud je ve společnosti volný dress kód a celkově přátelské prostředí auditoři mohou zvoleným formálním dress kódem, zasedacím pořádkem u jednacího stolu či jinými „doplňky“ navodit takovou atmosféru jakou si pro konkrétní rozhovor zvolí.

Auditoři by se při přípravě rozhovoru měli zamyslet i nad skutečností, že je zaměstnanec může překvapit tím, že se přizná, že podvod spáchal on. Jak by s tím měli naložit? Je dobré myslet na všechna možná „co by, kdyby“ a využít faktu, že s nimi zaměstnanec mluví, a zjistit od něj co možná nejvíce informací. Ve chvíli, kdy se zaměstnanci vše rozleží v hlavě, probere to s dalšími osobami, tak si uvědomí, co všechno může následovat a dost často zaměstnanec onemocní a zaměstnavateli nezbyde nic jiného než čekat kdy a zda se zaměstnanec vrátí z pracovní neschopnosti, aby s ním mohl vést další rozhovor a situaci dál řešit a mezitím může uplynout i několik měsíců.

Auditor si po provedení potřebných analýz a rozhovorů vyhodnotí zjištěné skutečnosti a na základě doložitelných výsledků předloží svůj závěr na danou situaci vedení společnosti. V kompetenci vedení společnosti je pak rozhodnout o případných dalších krocích včetně oznámení podezření na spáchání trestného činu v souladu s platnou legislativou.

Jak jsem si procházel všechny možné scénáře rozhovoru s plačící účetní, došlo mi, že i na tuto eventualitu jsme připraveni. U studené kávy jsem se usmál pod vousy: „u nás bychom to zvládli.“ ■

Vždy připraven?

Klasické vzdělání mi dalo do vínku i pár latinských hesel, která jsou v mé mysli hluboko uložená. Právě jedno z nich mi neustále rezonuje v posledních letech, zní Semper paratus – „Vždy připraven“.

Ing. Radek Ščotka, MBA
Působí ve společnosti Argeus, s.r.o., a to na pozici interního auditora se specializací na Risk Management. Jmenovaný vede projektové týmy při řízení rizik v oblasti ochrany dat a bezpečnosti ICT. Radek Ščotka má dlouholetou praxi v bankovním sektoru se specializací na problematiku cenných papírů a investičního bankovnictví. Další manažerské zkušenosti nabyl na poli auditu. Věnuje se projektům řízení rizik v korporátní sféře českých i nadnárodních společností, vedl implementaci systémů a metodik řízení rizik, interních auditů prostřednictvím sofistikovaných softwarových platforem u mnoha českých i nadnárodních společností. Radek Ščotka je aktivní v lektorské činnosti a zaměřuje se na propojení světa interního auditu, rizik a kontrolních prvků do praxe. Ing. Ščotka je absolventem Ekonomické fakulty VŠB Technické University Ostrava a The Free Swiss University of St. George´s.

Dnešní doba nás nutí se aspoň minimálně zamýšlet nad krizí, která je vyvolána důsledky pandemie covid-19. A všichni jsme jistě značně otráveni stále stejným mediálním tématem, které běží v České republice již přes jeden rok a na světovém poli ještě déle. Ano, je to dlouhá doba, a ne všichni vnímají související rizika a dopady s nimi propojené do života všech lidí, firem a světové ekonomiky. Obávám se, že ještě hodně dlouhou dobu bude pandemie plnit média. Okolnosti mne nutí věnovat souvislostem i tento článek.

Odhaduji, že se nás rizika dnešní pandemické doby dotkla s různou intenzitou, ale v drtivém procentu negativně. Pokud patříte k těm šťastlivcům, kteří na této koronavirové krizi vydělali a měli jste, máte či budete mít z dopadu covidu-19 užitek, máte velké štěstí. Pokud budeme současný stav vnímat jako krizový, a okolnosti tomu napovídají, vytane myšlenka, zda je možné být „vždy připraven“, i na krizi, na nečekané skutečnosti, události a stavy.

Analytická část našeho já může odpovědět: Ano, pokud máme dostatečná data k analýze rizik všech možných hrozeb, okolností, stavů apod.

Ale je tady druhá část našeho já, která může uvažovat s argumenty, že na všechno se připravit nedá, všechna potenciální rizika znát nemůžeme, o všem nemáme povědomí, ani jedinec či lidstvo. A proto je podle někoho lepší nechat věci ležet a běžet

samospádem, a být pouze účastníkem dění. K této myšlence se já osobně nekloním, ale chápu, že je řada osob, kterým tento přístup vyhovuje a nebudu jim v dnešním článku názor vyvracet.

Asi sami vnímáte, milí čtenáři, že nalezení správné odpovědi na otázku, zda můžeme být na vše připraveni, nebude jednoduché. V dnešním zamyšlení nad riziky a možnými kroky, které by měl brát v potaz i interní auditor, se nedobereme k definitivnímu závěru. Už jen z toho důvodu, že každá věc má několik řešení, a ta řešení mohou být různě nákladná, časově odlišně náročná, a s mnoha podmínkami, proměnnými.

„Proč zapomínáme vnímat některá rizika? Protože setrváváme ve velmi komfortní zóně“

Ale na jednom se při hledání možné odpovědi snad shodneme, je dobré se občas nad potenciálními riziky zamyslet, provést analýzu, s kolegy v týmu provést brainstorming. Tato technika skupinové kreativity zaměřená na generování nových nápadů jistě může přinést skvělé nápady na téma, zda můžeme být „vždy připraveni“ na různé krize, zda jsme schopni nastavit obranné scénáře, jestli se podaří některá rizika včas identifikovat a správně ošetřit. Nosnou myšlenkou těchto skupinových porad je předpoklad, že lidé pracující ve skupině vymyslí na základě podnětů ostatních více důmyslné nápady, než by nápady generovali samostatně.

A když se podívám například v rámci České republiky na naše některé čelné představitele vlády a státu, odpovědné osoby, tak mám dojem, že neměli, a asi stále nemají dostatek relevantních dat, neanalyzují rizika, nesnaží se krizové stavy řešit v týmu. Jinak by se nedělo to, co zažíváme nyní:

1. Česká republika je v počtu obětí koronaviru na 100 000 obyvatel v čele pelotonu.

2. Nárůst počtu nakažených nemocí covid-19 na 100 000 obyvatel nás řadí k nejhorším v Evropě.

3. Velmi nízká je zatím v našem státě míra očkování proti nemoci covid-19 (článek jsem psal 11/3/2021, snad se v dalších týdnech výše uvedené hodnoty zlepší v náš prospěch).

Krizové řízení

Dnešní situace nám připomíná skutečnost, že i Česká republika má ve své legislativě relevantní podporu – zákon o krizovém řízení 240/2000 Sb. Dle krizového zákona je krizovou situací mj. situace, při níž je vyhlášen nouzový stav. Zákon užívá definice „krizový stav“. Podle § 2 odst. c) krizového zákona je krizovým opatřením organizační nebo technické opatření určené k řešení krizové situace a odstranění jejích následků, včetně opatření, jimiž se zasahuje do práv a povinností osob.

Můžeme dnes po zkušenostech posledních 12 měsíců konstatovat, že je náš zákon o krizovém řízení připraven na dostatečné množství scénářů, krizových stavů? Domnívám se, že nikoliv. Slabou útěchou nám může být, že se chystá jeho novela.

Vy, kteří umíte vnímat hrozby, rizika, realitu dnešního otevřeného světa, si asi sami umíte odpovědět, zda krizové řízení je v rámci českého

legislativního rámce dostatečně robustní a zda je připraveno na případné těžké časy.

Krize a souvislosti

Zvykli jsme si využívat všech výhod, které nám přináší dnešní otevřená ekonomika, globalizace na všech úrovních, ve všech odvětvích, ale současně se tímto stáváme závislejšími a zranitelnějšími.

„Rizika jsou také spojena se zákonitostí ‚setrvačnosti'. Lidé a společnosti si neuvědomují všechna možná rizika, hodně jsme si zvykli na plně funkční a bezpečný standard evropského žití."

Rizika jsou také spojena se zákonitostí „setrvačnosti". Lidé a společnosti si neuvědomují všechna možná rizika, hodně jsme si zvykli na plně funkční a bezpečný standard evropského žití. Proč zapomínáme vnímat některá rizika? Protože setrváváme ve velmi komfortní zóně a domníváme se, že:

- Vše je samozřejmé.
- Vše bezpečně funguje.
- Vše je správně nastaveno.
- Vše automaticky běží.
- Vše je snadno přístupné.
- Vše je věčné…

U každého z výše uvedených bodů si jistě sami představíte řadu činností, procesů, úkonů, služeb, které souvisejí s naším denním žitím a na něj navázanými riziky, že tomu tak být nemusí. A je jedno, zda na chvíli, nebo na delší čas, vnímání faktu, že se „něco" pokazí a nebudeme schopni na danou situaci reagovat, si musíme opět umět připustit. Dnes jsme řadu měsíců konfrontováni s pandemií a opatření proti dopadu tohoto druhu rizika nejsou ani dokonalá, ani včasná, a už vůbec ne zcela účinná. Pravděpodobnost, že nastane v dalších letech podobný pandemický scénář, roste.

Stejně roste řada otázek, na které bychom měli znát odpovědi:

a) A kdo dnes tato rizika umí vnímat?
b) Kdo je schopen tyto skutečnost předem, a tedy včas analyzovat?
c) Který stát má dnes zpracované kvalitní krizové scénáře pro dopady rizik globálního dopadu? A nejedná se jen o pandemie.

Pokud společnost, stát, jakákoliv instituce, organizační jednotka nepomyslí na výše uvedené hrozby, neřeší rizika, překvapí ji KRIZE ve všech možných podobách, formách.

Na krizi se musíme připravit v dobách růstu

Krizové řízení v každé vyspělé společnosti předpokládá, že taková instituce má pro krizové stavy připravené krizové plány. A v časech dostatku, klidu a blahobytu je teoreticky testuje, zdokonaluje. Děje se tak i ve vašich organizacích? Odpovědi znáte sami, ať z pohledu interního auditora, risk manažera, vedoucího pracovníka, vlastníka, zřizovatele apod.

Aby byla instituce jakéhokoliv druhu připravena na nenadálé situace, měla by mít zpracován havarijní plán. Často se setkáte s označením z angličtiny BCP (Business Continuity Plan) a DRP (Disaster Recovery Plan). Při tvorbě těchto plánů je vhodné postupovat na základě předchozí analýzy rizik.

Samostatnou kapitolu by si zasloužila analýza krizových plánů, scénářů pro státní rozpočet, resp. řízení dluhů. Možná některé korporace mají připravené dostatečným způsobem havarijní plány i pro řízení cash flow v těžkých dobách, ale zatím není příliš mnoho firem, které by si tvořily dostatečné rezervy na krizové scénáře. V případě států je velmi málo rozpočtově odpovědných zemí, kde je tato politika důsledně uplatňována.

Schopnost zvládnout velké katastrofy

Možná si řeknete, že řešení velkých katastrof patří do sfér businessu pojišťoven. Ty přece řeší klientům dopad ledajaké přírodní pohromy, a možná si řeknete, že se v dnešní době dá pojisti vše možné. Není tomu tak.

Pandemie a jiné nemoci nás učí, že by každá odpovědná instituce měla vnímat svůj podíl při zvládání velké katastrofy, resp. jejího dopadu na ni. Zejména je důležitá oblast prevence těchto rizik, nastavení opatření proti dopadu velkých katastrof a havárií.

Interní audit by svou pozornost měl zaměřit na oblast působnosti různých složek státu. Velká role při zvládání krizí a katastrofických scénářů je na bedrech krajů, obcí, komunálních politiků.

Nová rizika a krizové scénáře

Pokud si realisticky uvědomujeme současné skutečnosti, tak by nás měla zajímat některá níže uvedená rizika a možné krize:

- Důchodová krize.
- Inflační rizika.
- Krize na trhu s energiemi.
- Krize světové politiky.
- Krize globálního oteplování.

Na tyto a další oblasti možných rizik s různými krizovými scénáři by neměli zapomínat interní auditoři, risk manažeři, protože dopad některých vybraných krizí může fatálně zasáhnout nejen do života států, vlád, společností, korporací, ale také do občanského života každého z nás. Na našich seminářích se snažíme tyto oblasti s praktickým výkladem osvětlit.

Domníváte se, že na řadu zmiňovaných rizik jste vyzbrojeni? Můžete se připravit?

Závěr

Nemůže být jednoznačný. Prosím vás o krátké zamyšlení se nad skutečností, zda jste ve svém zaměstnání, podnikání, ve své pracovní funkci si schopni říct, že aspoň z části jste ztotožněni s heslem „Vždy připraven".

Každý, kdo má odpovědnost za řízení nějaké instituce by měl věnovat pozornost rizikům souvisejícím s globálními hrozbami, updatovat havarijní a krizové plány a nezbytné je zkontrolovat u vedoucích činitelů jejich odpovědnost, jejich schopnosti a smysl pro realitu dnešních dnů.

Je příliš mnoho proměnných v dnešním světě v krizi, je totiž mnoho povolaných, ale málo vyvolených.

Nobiscum deus!
P.S. latiníci vědí ■

V JEDNÉ Z NEJVĚTŠÍCH NEMOCNIC V ČR SE UMÍME HROZBÁM BRÁNIT

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

Všeobecná fakultní nemocnice v Praze na Karlově náměstí (VFN) patří v současnosti k nejdůležitějším zdravotnickým zařízením v ČR a k největším fakultním nemocnicím v naší zemi. Tvoří ji 43 zdravotnických pracovišť (klinik, ústavů a samostatných oddělení), zaměstnává téměř 6 500 zaměstnanců, ročně je v ní hospitalizováno 45 000 pacientů a ambulancemi projde víc než jeden a půl milionu lidí.

Naše nemocnice poskytuje základní i vysoce specializovanou péči ambulantní a lůžkovou, dětem i dospělým pacientům. Mezi její základní nosné programy patří intenzivní medicína, kardiologie, onkologie a hematoonkologie, péče o matku a dítě, psychiatrie a adiktologie, dědičné metabolické poruchy a jiná vzácná onemocnění.

Ve VFN se tedy rozhodně máme čím pochlubit a co si chránit. Špičkové zdravotníky a všechny ostatní zaměstnance, kteří jsou nepostradatelní pro bezproblémový chod našeho zařízení a stovky pacientů i jejich blízkých.

Kyberútoků na zdravotnická zařízení přibývá

O potenciálu, důležitosti a nenahraditelnosti zdravotnických zařízení dobře vědí i ti, kdo chtějí poškodit fungování systému ochrany obyvatel a péče o zdraví veřejnosti. O tom svědčí i případy z nedávné minulosti. V prosinci 2019 civilní útočník zastřelil sedm lidí ve Fakultní nemocnici Ostrava. Nemocnici Benešov připravil kyberútok o internetový objednávkový systém dárců krve a některá administrativní a ekonomická data. V naší nemocnici se v říjnu 2020 objevily případy podvodných textových i e-mailových zpráv s falešnými výsledky testů na covid-19.

Ochrana uvnitř i navenek

Ostražitost a vysoká míra připravenosti na jakékoli možné narušení bezpečnosti a chodu nemocnice je na místě. Umět rychle a adekvátně reagovat, je rozhodně in.

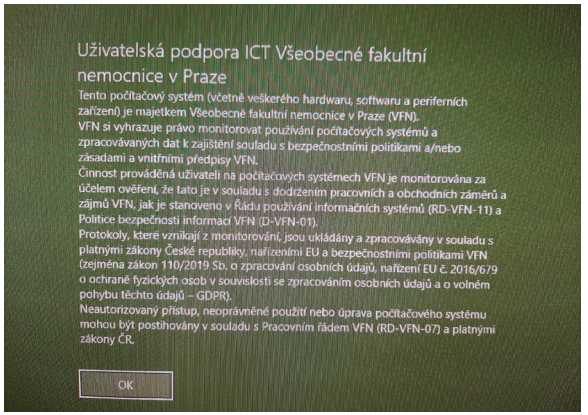
Oblasti kybernetické bezpečnosti je ve VFN dlouhodobě věnována adekvátní pozornost. Systém kybernetické a informační bezpečnosti je budován v souladu s požadavky legislativy. Úroveň kybernetické bezpečnosti je průběžně zvyšována včasnou implementací technických i organizačních opatření, a to s využitím relevantních informací od dodavatelů, Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) i na základě vlastní analýzy rizik. Přijímaná opatření přinášejí neustálé zlepšování naší ochrany.

Na jaře 2020 jsme v průběhu kybernetického útoku na FN Brno od NÚKIB obdrželi a realizovali čtyři sady reaktivních opatření. Důsledkem útoků je v obecném měřítku ale nejen realizace reaktivních opatření a zvyšování bezpečnosti v oblasti IT, ale také zvyšování informovanosti a znalostí uživatelů, kteří jsou důležitou součástí systému řízení bezpečnosti.

Když kterýkoli ze zaměstnanců VFN zapne pracovní počítač, zobrazí se mu následující obrazovka a svou informovanost musí potvrdit tlačítkem „OK“. Tento postup je ve VFN nepřekročitelný.

Ochrana našich zaměstnanců a jejich proškolování

Potenciální rizika umíme identifikovat, nepodceňujeme je, máme velkou motivaci s nimi pracovat a hrozbám systematicky předcházet. Díky souhře všech ochranných složek řídicího sytému VFN se nám to i daří.
Všichni zaměstnanci VFN jsou pravidelně proškolováni v pravidlech bezpečnosti práce a ochrany měkkých cílů. Teoreticky i prakticky je nám opakovaně vštěpováno jednoduché, ale důležité pravidlo: Utíkej, schovej se, bojuj!



V dnešní době se ve společnosti bohužel najdou lidé, kteří mají potřebu ubližovat ostatním. Tito agresoři jsou schopni a připraveni pro dosažení svého cíle způsobit zranění, či dokonce zabít. Obětí se může stát kdokoli. Motivem tohoto jednání může být nenávist, pomsta i duševní porucha. Útok přichází nečekaně, většinou je velmi brutální a šokující. Zdravotnická zařízení patří mezi riziková místa a poslední dobou útoků bohužel přibývá.

Jedné ze vzdělávacích akcí jsem se zúčastnila osobně. Školení bylo určeno všem zaměstnancům nemocnice, kteří se mohou dostat do krizových a konfliktních situací během výkonu svého povolání. Vedli ho dva policejní specialisté se zkušenostmi s krizovým vyjednáváním.

V teoretické části jsme se seznámili s charakteristikou krizových stavů, identifikací možného útočníka a jeho profilací (od agresivní osoby, alkoholika, drogově závislého až po aktivního útočníka), volbou účinné komunikace, preventivními opatřeními a zásadami, jak se v daných situacích zachovat. Následoval popis a rozbor skutečných případů v ČR i v zahraničí s odkazem na platnou legislativu.

Ve druhé praktické části jsme si pomocí modelových situací vyzkoušeli řešení konkrétní situace. Naučili jsme se aplikovat prvky krizové komunikace, používat technické prostředky osobní ochrany, jednoduché prvky sebeobrany a seznámili se s důležitými taktickými zásadami.

Hlavním cílem pořádání obdobných školicích akcí je naučit zaměstnance řešit krizové situace tak, aby se minimalizovaly možné následky.

Kéž by to ale nikdo z nás nemusel ve skutečnosti zažít!

Každý zaměstnanec má na úvodní stránce našeho firemního intranetu k dispozici odkaz „havarijní/krizové situace“, pod kterým je graficky velmi srozumitelně uvedeno, koho a jak v konkrétní krizové situaci kontaktovat.

Na zadní straně identifikační karty všech zaměstnanců VFN jsou uvedena telefonní čísla pro případ nouze (technické havárie, kyberútoku, požáru…).

Vysoká míra zranitelnosti je dána samotným charakterem zdravotnických zařízení. Musí být otevřená a dostupná všem, kdo potřebují akutní a rychlou péči. Není proto reálné, aby v nemocnici existovaly například bezpečnostní rámy na všech vstupech. Tím více je nutné se zaměřit na školení a péči o zaměstnance, dobře nastavený systém bezpečnostních služeb, kamerového systému i traumatologických plánů.

Traumatologické plány jsou vnitřní pravidla, jejichž cílem je aktivovat všechny potřebné složky k zajištění poskytnutí rychlé první pomoci v případě havárie, požáru, přírodní katastrofy a dalších událostí, při nichž je velké množství zraněných osob. Připravenost k zásahu se v naší nemocnici pravidelně ověřuje. VFN nedávno prokázala svou připravenost v praxi například při požáru hotelu v Náplavní ulici v Praze nebo při nehodě linkového autobusu u Drahonic.

A ještě jedno velké pochlubení úplně na závěr. Od února letošního roku se naše nemocnice už potřetí pyšní akreditací, při níž byla posuzována míra kvality a bezpečí poskytovaných služeb v souladu s právními předpisy a akreditačními standardy. ■


Spojená akreditační komise, o.p.s., IČ: 284 88 946

1310
Evidenční číslo

CERTIFIKÁT
O UDĚLENÍ

11.02.2021
Datum vydání

AKREDITACE
Všeobecná fakultní nemocnice v Praze

U Nemocnice 499/2, 128 08 Praha 2 Poskytovatel lůžkové zdravotní péče a zdravotní péče dle § 5 odst. 2, písm. f - h dle zákona č. 372/2011 Sb.
Název akreditovaného zdravotnického zařízení

Výše uvedený poskytovatel zdravotních služeb úspěšně absolvoval akreditační šetření a splnil požadavky akreditačních standardů Spojené akreditační komise, o.p.s. Současně tento poskytovatel splnil požadavky všech minimálních hodnotících standardů řízení kvality a bezpečí v souladu s ustanovením § 105 zákona č. 372/2011 Sb. o zdravotních službách a podmínkách jejich poskytování a s vyhláškou č. 102/2012 Sb. o hodnocení kvality a bezpečí lůžkové zdravotní péče.

Platnost certifikátu do: 10.02.2024

Ředitel SAK, o.p.s.

Předseda správní rady SAK, o.p.s.

SAK

AKREDITOVÁNO

Mgr. Martin Kubš
Ministerstvo financí ČR
vrchní ministerský rada
vedoucí oddělení
Audit OP VVV

Ing. Milan Puszkailer
Ministerstvo financí ČR
vrchní ministerský rada
vedoucí oddělení Audit EÚS

Podvody, podvodná jednání, zjištění při kontrolách – poučení, kuriozity...

Problematika „podvody a podvodná jednání“ je velice komplexní a složitá, a z auditního pohledu lze uvést, že je to jedna z nejtěžších oblastí, které musíme čelit a věnujeme jí zvýšenou pozornost. Je velice podstatné si uvědomit, že klíčovou úlohu Auditního orgánu Ministerstva financí ČR, potažmo úlohu auditora, představuje ochrana finančních zájmů EU v současném období 2014–2020 se zesíleným zřetelem na boj proti podvodům, posuzování rizika podvodů, předcházení podvodům a jejich odhalování. Důkazem toho je i samostatná oblast zaměřená v rámci řídicího a kontrolního systému na posuzování účinnosti a přiměřenosti realizovaných opatření proti podvodům. Auditor v současném období 2014–2020 hraje významnou, ne-li klíčovou, roli při ověřování, zda příslušné subjekty právní rámec pro fondy EU dodržují a jak tyto nové požadavky plní, a to nejen prostřednictvím vydání stanoviska ohledně účinného fungování systému řízení a kontroly.

Podvod a legislativní rámec

Pro účely snadnější orientace v právním rámci této problematiky lze shrnout, že oblast podvodů je pro nás primárně upravena nařízením Evropského parlamentu a Rady (EU) č. 2018/1046, kterým se stanovují finanční pravidla pro souhrnný rozpočet, spolu s Úmluvou o ochraně finančních zájmů Evropského společenství, vypracovanou na základě článku K.3 Smlouvy o Evropské unii. Zároveň je tato oblast Evropskou komisí specifikována v pokynech pro členské státy EGESIF-14-0021-00 z 16. června 2014.

Zde bychom se pozastavili a zmínili to podstatné, tedy definici podvodu[1] podle čl. 1 Úmluvy o ochraně finančních zájmů. Jedná se *o úmyslné jednání nebo opomenutí týkající se použití nebo předložení nepravdivých, nesprávných nebo neúplných prohlášení nebo dokladů, které má za následek neoprávněné přisvojení nebo zadržování prostředků*

[1] Zákon č. 40/2009 Sb., trestní zákoník, definuje v § 212 Trestný čin dotační podvod a v § 260 Trestný čin Poškození finančních zájmů Evropské unie

ze souhrnného rozpočtu Evropských společenství či rozpočtů spravovaných Evropskými společenstvími nebo jejich jménem, neposkytnutí informací v rozporu se zvláštní povinností se stejnými následky, neoprávněné použití těchto prostředků pro jiné účely, než pro které byly původně poskytnuty.

„Oblast podvodů je primárně upravena nařízením Evropského parlamentu a Rady (EU) č. 2018/1046, kterým se stanovují finanční pravidla pro souhrnný rozpočet, spolu s Úmluvou o ochraně finančních zájmů Evropského společenství, vypracovanou na základě článku K.3 Smlouvy o Evropské unii. Zároveň je tato oblast Evropskou Komisí specifikována v pokynech pro členské státy EGESIF-14-0021-00 z 16. června 2014.“

To podstatné, co tvoří tzv. tenkou linii mezi běžnou nesrovnalostí a podvodem, je tedy ono úmyslné podvodné jednání, tj. musí se jednat o zavinění ve formě úmyslu (nestačí zavinění z nedbalosti).

Na Auditním orgánu MF ČR proto problematice podvodů přikládáme vysokou prioritu, a to zejména v oblasti odborné přípravy a osvěty. Za tímto účelem je pro auditory vytvořen v rámci interních postupů Auditního orgánu MF ČR pro výkon nezávislého a objektivního přezkoumávání a vyhodnocování metodický postup zevrubně popisující využití různorodých auditních technik, použití strukturovaných kontrolních listů s otázkami sloužící k úplnému a správnému prověření této oblasti, včetně způsobu vytěžování dat informačními systémy, jako je např. ARACHNE, což je moderní informační technologie pro hodnocení rizik v rámci projektů, smluv, dodavatelů, ale i příjemců. Zároveň jsou auditorům k dispozici výroční zprávy Evropského úřadu pro boj proti podvodům (OLAF), které aktuálně informují o tendencích a hlavních směrech podvodů, a v rámci adaptačního procesu dochází k seznamování se s dokumenty, které vypracovala Komise a Evropský úřad pro boj proti podvodům. Aby bylo možné úspěšně ukončit adaptační proces, musí auditor za pomoci přiděleného mentora prokázat znalost specializovaných dokumentů, mezi které řadíme např. COCOF 09/003/00 z 18. února 2009 – informativní zpráva k ukazatelům podvodu pro EFRR, ESF a FS, dále přehled anonymizovaných případů OLAF ze dne 14. ledna 2011, rovněž OLAF – praktický průvodce střetem zájmů v postupech pro zadávání veřejných zakázek a OLAF – praktický průvodce padělanými dokumenty, ale i Příručka – úloha auditorů členských států při předcházení a odhalování podvodů v oblasti evropských strukturálních a investičních fondů.

Jak identifikovat podezření na podvodné jednání

K tomu, abychom si vytvořili auditorský úsudek, na jaké další rizikové oblasti bychom se měli v rámci výkonu auditu soustředit a jaké kroky, resp. opatření, je nutné učinit, nám napomáhá správná identifikace a vyhodnocení varovných signálů.

Prvotní varovné signály jsme schopni identifikovat již na samotných dokumentech, kdy se zaměřujeme na to, zda nejsou odlišné po věcné stránce a zároveň od běžné či obecné grafické úpravy. Konkrétní signály spatřujeme, pokud faktury, dopisy či dokumenty jsou bez označení společnosti, bez kontaktních údajů, jako je adresa, e-mail, telefon. Zároveň jsou signálem rozdíly ve velikosti, stylu či barvě písma, ručně přeškrtnuté či psané údaje bez podpisů oprávněných osob, absolutní totožnost podpisu osob co do sklonu. Absence dokladů v účetnictví, rozpor informací na internetu vůči předložené faktuře, či dokonce dvojí verze dokumentů, řadíme mezi další možné signály. Rovněž za zmínku stojí velikosti a ostrost úředních razítek, jejich pozice, resp. umístění, či neobvyklé barvy nenaznačující použití tiskárny oproti originální úřední pečeti.

Při následném ověřování fyzického provádění projektu klademe důraz na to, zda nedochází k odlišnostem od smluvní dokumentace a fakturace, resp. nesouladu skutečného s předepsaným. V této oblasti konkrétní signály spatřujeme v nedodání služeb a dodávek, či v jejich dodání ve snížené kvalitě nebo nižším množství oproti počtu fakturovanému.

„Signály podvodů spatřujeme, pokud faktury, dopisy či dokumenty jsou bez označení společnosti, bez kontaktních údajů jako je adresa, e-mail, telefon. Zároveň jsou signálem rozdíly ve velikosti, stylu či barvě písma, ručně přeškrtnuté či psané údaje bez podpisů oprávněných osob, absolutní totožnost podpisu osob co do sklonu.“

U stavebních prací spatřujeme signály v neprovedení prací či nesouladu s technickými požadavky, popř. u faktur od poddodavatelů, které nejsou doložitelné provedenou prací. U vybavení může být jeden z dalších varovných signálů např. absence sériových čísel, jejich nečitelnost či úpravy samotných výrobních štítků z důvodu zamezení ověření novosti, případně známky vyšší

opotřebovanosti při identifikaci záměny starého zařízení za nové apod.

K identifikaci a vyhodnocování varovných signálů používáme mimo jiné veřejně dostupné informace, internet, profily zapojených subjektů a osob, informační systémy jednotlivých operačních programů a moderní technologie sloužící k hodnocení rizik a upozorňování na nejrizikovější projekty, příjemce, ale i smlouvy a dodavatele.

Zároveň provádíme křížové ověření informací o zapojených subjektech, dodavatelích, subdodavatelích, administrátorech veřejných zakázek s využitím nástrojů pro vytěžování dat, jako je např. ARACHNE se zohledněním odvětví generujících výdaje s vyšší náchylností k podvodu – jako jsou odvětví stavebnictví, nakládání s odpady, cestovní ruch či pořádání vzdělávacích aktivit.

Jako auditoři však nezapomínáme na to, že oproti auditu, jehož cílem je posoudit legalitu a správnost realizace projektu, je cíl trestního (forenzního) řízení odlišný se zaměřením na odhalení a prošetření projektu s příslibem zajištění důkazů o existenci podvodného úmyslu. Z uvedeného důvodu při identifikaci podezření na podvod provádíme dle metodického postupu nezbytné kroky, mezi které spadá posouzení daného případu s příslušným přímým nadřízeným nebo právní expertizou pro zajištění řádné supervize. V rámci tohoto procesu je veden auditor k tomu, aby vždy jednal v mezích příslušných právních předpisů, mezinárodně uznávaných standardů a pokynů, včetně interních postupů MF ČR. Auditor nejen díky tomuto dohledu je pak schopen lépe rozpoznat hranici mezi auditní činností a vyšetřováním. Je schopen učinit kvalifikovaný závěr o dostatečnosti audit trailu pro tvrzení, že bylo identifikováno podezření na podvod. Zároveň je auditor veden procesem zpracování a předání oznámení o závažných skutečnostech zjištěných v rámci auditní činnosti na věcně příslušný odborný útvar MF k dalšímu posouzení. Teprve po schválení z úrovně věcně příslušného odborného útvaru MF jsou tyto případy předávány k rozhodnutí orgánům činným v trestním řízení.

Zjištění při auditech

Auditní orgán v rámci své auditní činnosti identifikoval v období 2014–2020 několik oblastí zjištění, které obsahovaly riziko znaků podvodných jednání, zejména účelových aktivit ze strany příjemců dotace pro získání osobního či majetkového prospěchu. Nejčastěji zjištěnou oblastí bylo proplacení neprovedených stavebních prací, služeb nebo pracovních činností u příjemce dotace. Stavební práce byly většinou nárokovány k proplacení bez řádného zdokumentování realizace, dostatečných záznamů ve stavebním deníku při absenci řádné kontroly ze strany investora (příjemce), technického dozoru investora a dodavatele. Auditor se při hodnocení takové oblasti zjištění zaměřoval zejména na subjektivní stránku zjištění, konkrétních aktivit jednotlivých zúčastněných osob a při identifikaci znaků vedoucích k závěru o výskytu rizika podvodu se snažil zajistit potřebné argumenty, důkazy či materiály, které by bylo možné předat pro samostatné forenzní šetření. Samotný výdaj dotčený takovou nesrovnalostí je označován za nezpůsobilý. Charakter takových zjištění obvykle spočíval buď v prostém neprovedení stavebních prací, nebo v provedení prací jiných, které nebyly smluvně uzavřeny. Obvykle se jednalo zejména o takové činnosti, které jsou hůře přezkoumatelné, protože jejich kontrola je možná pouze v určitých realizačních fázích samotné stavby. Dalším častým nedostatkem v rámci výše uvedené oblasti zjištění byly nepovolené změny parametrů, množství, materiálů nebo technologického způsobu řešení stavebních prací. Některé nepovolené změny byly zaměřené na účelové obcházení smluvně uzavřených cen za objemové jednotky např. změnou pouhých rozměrových parametrů a množství kusů při stejně zvolené technologii, přičemž takové změny již nebyly dodány ve smluvně uzavřených cenách z řádného výběrového řízení, ale dle cen vyšších, které kdyby byly nabídnuty uchazečem již v rámci podané nabídky, nebyla by v rámci hodnocení taková nabídka vyhodnocena za vítěznou.

Další rizikovou oblastí, se kterou se auditoři v rámci prováděných auditů setkali, byla problematika realizace nákupu již používaného zařízení jako nového. Přestože byla v rámci veřejné zakázky v předmětu veřejné zakázky stanovena podmínka nového zařízení, byla realizována dodávka zařízení staršího a již používaného. V jednom případě bylo takové zařízení dokonce již zapůjčeno zadavateli několik roků před realizací veřejné zakázky a zadávací podmínky byly stanoveny pro zvýhodnění tohoto zařízení.

„Auditor vždy jedná v mezích příslušných právních předpisů, mezinárodně uznávaných standardů a pokynů, včetně interních postupů MF ČR.“

Významně častou oblastí byla dále zjištění různých duplicitně nárokovaných výdajů, přičemž jako obvyklá praktika byla identifikována skutečnost nárokování proplacení výdajů souvisejících s jedním výstupem u jednoho projektu ve více projektových žádostech, zejména v různých regionálních oblastech působení. Výstupem byly většinou totožné metodické materiály, analýzy nebo zpracované pracovní či technické postupy.

Nejvíce sledovanou problematikou v posledních letech je rovněž výskyt střetu zájmů způsobený propojeností osob z hlediska poskytovatele a příjemce

dotace a z hlediska zadavatele a dodavatele v rámci realizace veřejných zakázek. V obou oblastech se uplatňuje jak přímý, tak i nepřímý (většinou zprostředkovaný) zájem na ovlivnění výsledku hodnocení a výběru projektu či vítězného uchazeče. Příkladem takového osobního vlivu je poskytnutí výhody sobě / rodinnému příslušníkovi / osobě blízké za účelem získání neoprávněného prospěchu pro sebe nebo tuto jinou fyzickou či právnickou osobu, kupř. ve formě předčasného poskytnutí informací o záměru vyhlášení veřejné zakázky, jejich konkrétních podmínkách, včetně přizpůsobení těchto podmínek danému uchazeči, ovlivnění výsledku hodnocení při samotném posuzování podaných nabídek atd. Shodně tak v procesu hodnocení výběru podpořených projektů u příslušného poskytovatele dotace.

Složitou problematikou je pro zhodnocení prokázaného vlivu střetu zájmů zjišťování propojenosti osob a jejich vztahu k předmětu samotného projektu, projektového procesu nebo související veřejné zakázky. Hodnocení vztahů propojených osob by nemělo být založeno na pouhé hypotetické spekulaci, ale na kvalifikovaném hodnocení rizikového potenciálu, konkrétně realizovaných aktivit. Při takové činnosti se auditoři zaměřují zejména na hodnocení rizik možnosti negativního vlivu na záměrné ovlivnění samotného procesu výběru. Samotná propojenost osob automaticky bez dalšího neznamená, že došlo k ovlivnění, a z uvedeného důvodu je nutné se při přezkoumávání zaměřit na zjišťování právě těchto skutečností, aby mohlo být riziko střetu zájmů kvalifikovaně a důkazně podloženě identifikováno.

„Doporučujeme jak poskytovatelům, tak i příjemcům, věnovat se boji proti podvodům a korupci velice intenzivně tím, že se minimalizují příležitosti k podvodnému jednání – a to aktivním, cíleným a spolehlivým hodnocením, včetně ochoty předávat případy příslušným orgánům k řádnému šetření. Tím bude vyslán jasný signál všem!“

Poučení, závěr

Naši roli v kontrolních systémech operačních programů nepodceňujeme, a přestože jsou naše činnosti vykonávány zpravidla ex-post, jsme zastánci preventivních kroků, než následného řešení ex-post následků. Zajišťujeme výkon nezávislého auditu v souladu s legislativou EU a ČR prostředků z ESI fondů, který mimo jiné má ověřit, zda je možné vydat stanovisko k tomu, že kontrolní systém funguje účinně a poskytuje i přiměřené ujištění, že dle článku 72 písm. h) Nařízení Evropského Parlamentu a Rady č. 1303/2013[2], dochází k předcházení a odhalování podvodů. Což také znamená nutnost ověřit, že ze strany Řídicích orgánů jsou dle článku 125 odst. 4 písm. c) odkazovaného Nařízení zavedena účinná a přiměřená opatření proti podvodům. Za tímto účelem se v rámci preventivních opatření při auditu systému zaměřujeme na propustnost a náchylnost zkoumaného kontrolního systému vůči podvodům a jejich odhalování, tak aby i riziko podvodu bylo dostatečně řízeno a minimalizováno. Uvědomujeme si, že žádný systém není 100% účinný, jde však o to riziko snížit a předcházet mu. V rámci prevence se dále zaměřujeme na osvětovou a přednáškovou činnost např. v rámci konference AO či seminářů „Dotace EU a AUDITY“. **Doporučujeme jak poskytovatelům, tak i příjemcům, věnovat se boji proti podvodům a korupci velice intenzivně tím, že se minimalizují příležitosti k podvodnému jednání – a to aktivním, cíleným a spolehlivým hodnocením, včetně ochoty předávat případy příslušným orgánům k řádnému šetření. Tím bude vyslán jasný signál všem!** Závěrem je však dobré sdělit i něco pozitivního. Snad tedy to, že tento boj současným programovým obdobím nekončí, naopak o to intenzivnější práce nás čeká v nadcházejícím období 2021–2027, nicméně jsme na něj s ohledem na vzrůstající míru erudice a zkušeností lépe připraveni, protože nejen auditor bude hrát v celém procesu klíčovou roli! ■

[2] Nařízení Evropského Parlamentu a Rady č. 1303/2013, o společných ustanoveních o Evropském fondu pro regionální rozvoj, Evropském sociálním fondu, Fondu soudržnosti, Evropském zemědělském fondu pro rozvoj venkova a Evropském námořním a rybářském fondu, o obecných ustanoveních o Evropském fondu pro regionální rozvoj, Evropském sociálním fondu, Fondu soudržnosti a Evropském námořním a rybářském fondu a o zrušení nařízení Rady (ES) č. 1083/2006

Podvody v oblasti poškozování finančních zájmů Evropské unie

Ing. Ondřej Novák
vrchní ministerský rada
Centrální kontaktní bod AFCOS
Ministerstvo financí ČR

Podvody, na které bych se chtěl v následujících řádcích zaměřit, jsou takové podvody, u nichž došlo k poškození finančních zájmů Evropské unie při implementaci projektů spolufinancovaných z prostředků evropských fondů na území České republiky a jejichž protagonisté byli za své činy pravomocně odsouzeni.

Finanční prostředky, které Evropská unie jednotlivým členským státům poskytuje, mají být bezvýhradně využity v souladu s vytyčeným a jasně definovaným cílem a za podmínek stanovených národní a evropskou legislativou. Ne vždy tomu tak však je, ať už v důsledku opomenutí, pochybení, nebo nekorektního/protiprávního jednání ze strany příjemců či jiných zapojených subjektů. Evropská unie si je této skutečnosti vědoma, a proto jak sobě, tak členským státům ukládá bojovat proti všem formám protiprávního jednání, jež poškozují nebo ohrožují její finanční zájmy.

Bojem proti podvodnému jednání – od specifikace podmínek čerpání finančních prostředků z jednotlivých operačních programů přes řízení rizik až po kontrolní a auditní činnost – se zabývají instituce na různých úrovních státní a veřejné správy, Ministerstvo financí nevyjímaje.

Úloha Centrálního kontaktního bodu AFCOS

V rámci ochrany finančních zájmů Evropské unie a boje proti podvodům ve správně-právní oblasti byl usnesením vlády ze dne 5. září 2007 č. 1010 zřízen na Ministerstvu financí Centrální kontaktní bod AFCOS (dále jen „CKB AFCOS“). Jeho role je rovněž definována v čl. 3 odst. 4 nařízení Evropského parlamentu a Rady (EU, EURATOM) č. 883/2013 ze dne 11. září 2013, o vyšetřování prováděném Evropským úřadem pro boj proti podvodům (OLAF) a o zrušení nařízení Evropského parlamentu a Rady (ES) č. 1073/1999 a nařízení Rady (Euratom) č. 1074/1999, ve znění pozdějších předpisů.

Kromě poskytování součinnosti při šetřeních prováděných Evropským úřadem pro boj proti podvodům v České republice či hlášení nesrovnalostí Evropské komisi zajišťuje CKB AFCOS i výkon styčného místa pro ústřední databázi pro vyloučení, respektive pro systém včasného odhalování rizik a vylučování hospodářských subjektů. Tento systém byl Evropskou komisí zaveden k posílení ochrany finančních zájmů unie a zajištění řádného finančního řízení. Umožňuje zejména včasnou detekci hospodářského subjektu, který pro finanční zájmy představuje určitá rizika, vyloučení hospodářského subjektu s ohledem na možnost vymožení neoprávněně vyplacených finančních prostředků unie zpět, uložení finanční sankce hospodářskému subjektu a v nejzávažnějších případech také zveřejnění informace související s vyloučením / finanční sankcí na internetových stránkách Evropské komise k posílení odrazujícího účinku.

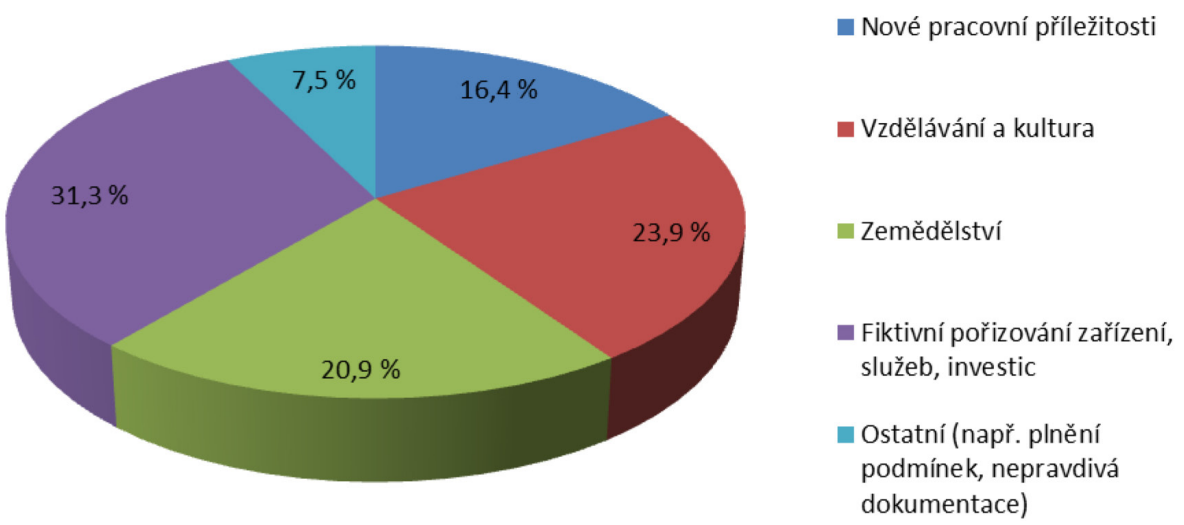
CKB AFCOS v této souvislosti analyzuje pravomocné rozsudky týkající se porušení ustanovení § 260 trestního zákoníku (zákon č. 40/2009 Sb. – dále jen „TrZ“) – „Poškození finančních zájmů EU“, které mu v návaznosti na usnesení vlády ČR ze dne 20. července 2009 č. 941 zasílají příslušné soudy. Na základě vyhodnocení pravomocných rozsudků, jejich relevantnosti a příslušnosti poskytuje informace také v jednotlivých případech generálním ředitelstvím Evropské komise k případným dalším opatřením.

Oblasti, ve kterých došlo k podvodům, a porušená ustanovení trestního zákoníku

CKB AFCOS analyzoval dosud celkem 67 pravomocných rozsudků, kde byly fyzické či právnické osoby odsouzeny dle § 260 TrZ. Při detailnějším zaměření na podvodná jednání, která se v rámci těchto rozsudků vyskytují, lze rozlišit čtyři hlavní oblasti porušení předpisů: fiktivní pořizování zařízení, služeb, investic; vzdělávání a kultura; oblast společné zemědělské politiky a nové pracovní příležitosti.

Z pohledu porušení ustanovení trestního zákoníku se kromě samotného porušení ustanovení § 260 TrZ nejčastěji vyskytují kombinace s porušením ustanovení § 212 TrZ (dotační podvod) a dále kombinace s porušením dalších ustanovení (např. trestný čin padělání a pozměnění veřejné listiny, podvod, zkrácení daně, poplatku a podobné povinné platby).

Oblasti porušení předpisů



Posun od jednoduchých podvodů k podvodům sofistikovaným

Z analytických výstupů CKB AFCOS je možné identifikovat oblasti, na které je vhodné se při boji proti podvodům zaměřit a formulovat doporučení pro kontrolní orgány.

> **„To je spojeno s předchozí domluvou mezi zadavatelem a účastníky výběrových řízení.“**

Lze konstatovat, že v posledních letech došlo k posunu od podvodů spáchaných jednotlivci k podvodům páchaným více pachateli, kteří spolu vzájemně kooperují; od podvodů, které jsou snáze prokazatelné k sofistikovaným činům, při kterých pachatelé vytvářejí účelové fakturační řetězce a využívají finanční prostředky k jejich zastření. Do takového procesu bývá zahrnuta řada firem, často s nejasnou vlastnickou strukturou nebo skrytě vzájemně propojených. Dalším průvodním indikátorem takových subjektů je, že často mají krátkou nebo žádnou hospodářskou historii, nevykonávají žádnou nebo téměř žádnou ekonomickou činnost, nelze u nich dohledat účetní závěrky, dokumenty dokládající finanční zdraví apod. Na základě uvedeného **je vysoce žádoucí, aby** byl při kontrolách u subjektů tohoto typu **brán zřetel také na prověření případné majetkové nebo personální propojenosti** a dalších indikátorů, které mohou napovědět, že se jedná o podvodné struktury.

V konkrétních případech je možné se ve fázi žádosti o dotaci setkat s deklarováním dostatečného množství finančních prostředků na zajištění vlastního spolufinancování, kdy tyto prostředky jsou na účet subjektu poukázány pouze účelově a zpravidla na krátký časový úsek od jiného subjektu, či prokazováním požadované odbornosti nebo zkušenosti, kdy subjekt tyto podmínky nenaplňuje.

U výběrových řízení dochází často k manipulaci s doklady, které mají prokazovat jejich korektní průběh nebo vůbec jejich konání a výběr vhodných firem, které mají zakázky realizovat. To je spojeno s předchozí domluvou mezi zadavatelem a účastníky výběrových řízení.

U pořizování zařízení se lze setkávat s vydáváním použitého zařízení za nové či jeho fiktivním pořízením. U investic do rekonstrukcí, budov či investičních celků dochází k nadhodnocování investic, objemu prací, zahrnování nerealizovaných či neuznatelných akcí do nákladů k proplacení. S pořizováním zboží, služeb či investic je též často spojené vytváření účelových fakturačních řetězců prostřednictvím dalších subjektů s cílem předstírat reálné finanční toky za nakupované zařízení či služby, a deklarovat tak korektní využití prostředků v souladu se schváleným projektem. Prověření skutečného stavu spojeného s případným praktickým ověřením provozuschopnosti příslušného zařízení fyzickou kontrolou na místě je v mnoha případech jedinou možností, jak ověřit tvrzení uváděná v korespondujících dokladech. Je známa řada případů, kdy starší, zejména technická zařízení a stroje, jsou, často nepříliš sofistikovaným způsobem, vydávána za nová. Děje se tak např. novým nátěrem nebo přestříkáním, výměnou výrobních štítků, přeražením evidenčních či výrobních čísel atp. Známy jsou rovněž případy, kdy vzhledově shodné nebo velmi podobné zařízení levnějšího typu nebo provedení je vydáváno za typ dražší. Tyto skutečnosti však nelze pouze ze samotných dokladů zpravidla spolehlivě zjistit. **V případech pořízení nového zařízení nebo strojů je vhodné maximálně upřednostnit ověření skutečného stavu kontrolou na místě před pouze administrativním ověřením, protože tak lze relativně snadno odhalit případný podvod.**

U vytváření nových pracovních příležitostí se často jedná o skutečnost, že osobám na těchto pracovních místech nebyla vůbec nebo pouze částečně vyplácena mzda a dále, že za ně nebyly řádně odváděny úhrady na veřejné zdravotní pojištění, sociální pojištění a příspěvek na státní politiku zaměstnanosti. V oblasti vzdělávání dochází také často k porušení podmínek programů, kdy se vzdělávací akce vůbec neuskutečnily nebo se konaly jinou formou a následně na základě fiktivních dokladů (prezenční listiny, falešné fotodokumentace) je předstírán jejich řádný průběh a vykonání. V takových případech je při běžné kontrole, bez konkrétního podezření, velmi obtížné či prakticky nemožné podvod odhalit. K odhalení dochází většinou pouze díky přímému oznámení některého z účastníků školení nebo zaměstnanců (často bývalých) subjektu, který vzdělávání pořádá. V případě, že kontrolní orgán pojme jisté podezření o pravdivosti prezenčních či jiných listin a údaje v nich uvedené (jméno, příjmení, datum narození) to umožní, **je doporučeno prověřit existenci účastníka v registru obyvatel. Další variantou může být porovnání shody podpisů účastníků vzdělávacích akcí na prezenčních listinách s jejich podpisy na jiných dokumentech**, např. pracovních smlouvách.

> **„Je známa řada případů, kdy starší, zejména technická zařízení a stroje, jsou, často nepříliš sofistikovaným způsobem, vydávána za nová.“**

Co zmínit závěrem? CKB AFCOS v oblasti pravomocných rozsudků průběžně spolupracuje s Nejvyšším státním zastupitelstvím a jednotlivými soudy, pozorně sleduje a vyhodnocuje data a trendy. Analyzované informace v rámci boje proti podvodům v oblasti evropských fondů prezentuje na školeních určených pro subjekty zapojené do ochrany finančních

zájmů Evropské unie v České republice, na pracovních skupinách a zprostředkovává je rovněž řídicím orgánům odpovědným za implementaci operačních programů a řádné finanční řízení pomoci. Za účelem zlepšení situace v boji proti podvodům promítá CKB AFCOS poznatky získané ze svých aktivit také do metodických stanovisek, doporučení a zpráv o své činnosti, které zveřejňuje na webu Ministerstva financí. V neposlední řadě prezentuje CKB AFCOS své závěry a zkušenosti i na zahraničních odborných fórech zaměřených na ochranu finančních zájmů a boj proti podvodům na výdajové stránce rozpočtu Evropské unie.
Pro detekování protiprávního jednání vnímáme jako důležité i nadále zefektivňovat kontrolní mechanismy, při kontrolách se zaměřovat zejména na „osvědčené" typy podvodného chování. Současně je však nutné nepodceňovat invenci těch, kteří nemají při čerpání pomoci jen ty nejlepší úmysly. Z tohoto důvodu je proto třeba neustále sledovat nové formy a vzorce podvodného jednání a zajišťovat kontinuální důslednou kontrolní činnost na všech úrovních řízení v rámci celého procesu poskytování evropských i národních finančních prostředků. ■

Plnění oznamovací povinnosti ve vztahu k porušení rozpočtové kázně a trestní odpovědnosti

Strategickým posláním Nejvyššího kontrolního úřadu (dále jen „NKÚ“) je poskytovat objektivní informace o hospodaření státu s veřejnými prostředky. Výsledky v podobě kontrolních závěrů, stanovisek k plnění státního rozpočtu a dalších výstupů činnosti poskytují důležitou zpětnou vazbu o legalitě, hospodárnosti, efektivnosti a účelnosti při nakládání s veřejnými prostředky a majetkem státu.

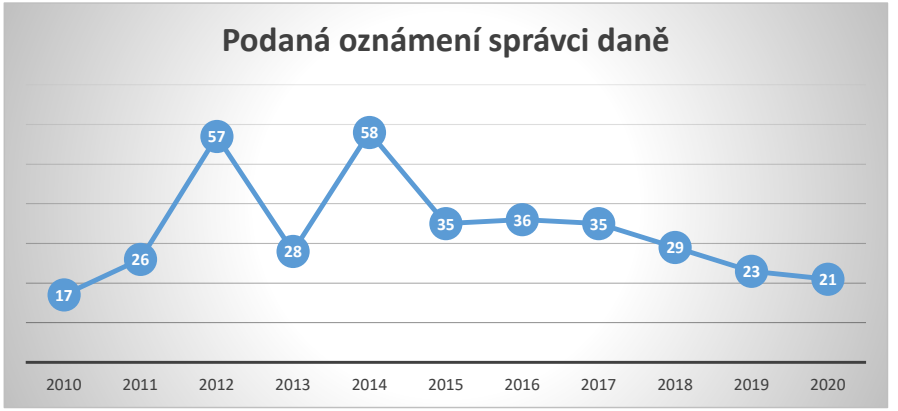
JUDr. Ing. Zdeňka Liv Prokšová
Absolventka národohospodářské fakulty VŠE Praha, obor ekonomická statistika a fakulty práva PEVŠ v Bratislavě. Má bohaté praktické zkušenosti ze státní správy, např. Český statistický úřad, Ministerstvo vnitra ČR nebo od roku 2010 Nejvyšší kontrolní úřad, kde pracovala na různých úrovních řízení. Profesně se věnuje především veřejnosprávní kontrole a internímu auditu. Od roku 2014 je členkou zastupitelkou obce a zároveň i členkou rady obce. Jako členka rady obce se zabývá především závazkovým právem. Má bohaté zkušenosti z lektorské činnosti.

K nejdůležitějším dopadům činnosti NKÚ patří zejména působení na příslušné orgány za účelem odstraňování zjištěných nedostatků a realizace navrhovaných opatření. Výsledky kontrol představují zároveň preventivní účinek v podobě vyvarování se obdobných chyb v řízení a kontrole. V neposlední řadě kontroly NKÚ přinášejí efekt v podobě plnění oznamovací povinnosti ve vztahu k porušení rozpočtové kázně či trestní odpovědnosti.

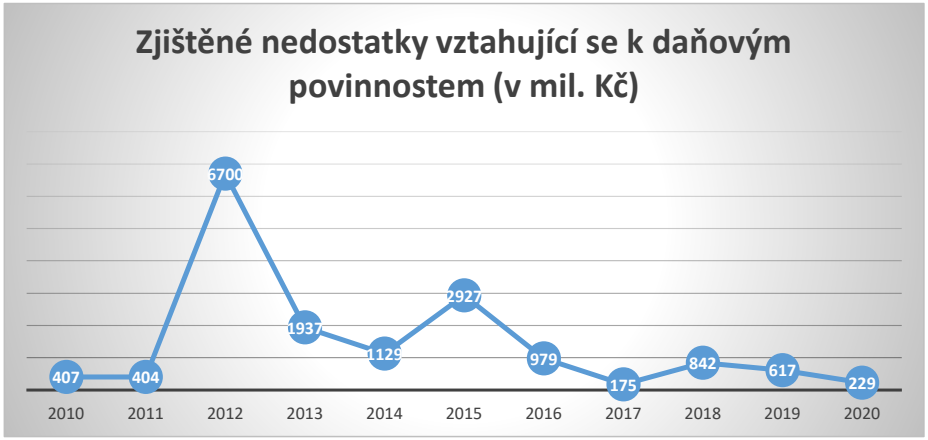
V souladu s ustanovením § 59 odst. 1 zákona č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů, předává NKÚ příslušným správcům daně údaje o zjištěných skutečnostech uvedených v kontrolních protokolech, které mají vztah ke správě daní. Konkrétní kontrolní zjištění týkající se porušení a nedostatků mohou být využita příslušnými správci daní k zahájení daňové kontroly k ověření, zda nevznikla odvodová povinnost za porušení rozpočtové kázně. V roce 2019 bylo příslušným správcům daně odesláno celkem **23** oznámení ze **17** kontrolních akcí, která souvisela se správou daní a daňovými povinnostmi kontrolovaných osob. Celková částka peněžních prostředků v těchto oznámeních činila téměř **617 milionů Kč**. Oznámení se týkala zejména:

- porušení povinností zjištěných u příjemců dotací;
- porušení povinností organizačních složek státu a státních příspěvkových organizací.

V loňském roce bylo v rámci oznamovací povinnosti příslušným správcům daně odesláno celkem 21 oznámení z 9 kontrolních akcí, která souvisela se správou daní. Celková částka finančních prostředků vyčíslená v těchto oznámeních činila přes **229 mil. Kč**. Oznámení se týkala porušení stejných povinností jako v roce 2019. Vývoj podaných oznámení správci daně a finančního vyjádření zjištěných nedostatků vztahujících se k porušení daňové povinnosti je uveden v následujících grafech.



Graf č. 1 **Zdroj: výroční zprávy NKÚ**



Graf č. 2 **Zdroj: výroční zprávy NKÚ**

Z výše uvedeného grafu č. 2 vyplývá, že nejvyšší částku související s porušením daňové povinnosti, vyčíslil NKÚ v roce 2012. Tato částka souvisela zejména s oznámením porušení rozpočtové kázně při realizaci silničního okruhu kolem Prahy.

V souladu s ustanovením § 8 odst. 1 zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů je Nejvyšší kontrolní úřad jako státní orgán povinen vyhovět dožádání orgánů činných v trestním řízení a neprodleně oznamovat státnímu zástupci nebo policejním orgánům skutečnosti nasvědčující tomu, že byl spáchán trestný čin.

V roce 2019 podal NKÚ na základě zjištění z **5** kontrolních akcí **6** oznámení nasvědčujících tomu, že byl spáchán trestný čin. Tato oznámení se týkala podezření ze spáchání trestného činu:

- porušení povinnosti při správě cizího majetku;
- porušení povinnosti při správě cizího majetku z nedbalosti;
- poškození finančních zájmů Evropské unie;
- podvodu;
- dotačního podvodu;
- zjednání výhody při zadání veřejné zakázky, při veřejné soutěži a veřejné dražbě;
- porušení předpisů o pravidlech hospodářské soutěže.

Orgány činné v trestním řízení si v roce 2019 vyžádaly součinnost NKÚ celkem v 9 případech. Na základě těchto žádostí poskytl NKÚ kontrolní materiály ze 3 kontrolních akcí. Prezident NKÚ v roce 2019 v souladu se zákonem č. 166/1993 Sb., o NKÚ, ve znění pozdějších předpisů, zbavil z důvodu důležitého veřejného zájmu celkem 5 zaměstnanců povinnosti mlčenlivosti.

V loňském roce podal NKÚ na základě zjištění ze **4** kontrolních akcí **4** oznámení nasvědčujících tomu, že byl spáchán trestný čin.
Tato oznámení se týkala podezření na spáchání trestného činu:

- dotačního podvodu;
- porušení povinnosti při správě cizího majetku;
- porušení povinnosti při správě cizího majetku z nedbalosti;
- zkreslování údajů o stavu hospodaření a jmění;
- zneužití pravomoci úřední osoby.

„V loňském roce podal NKÚ na základě zjištění ze 4 kontrolních akcí 4 oznámení nasvědčujících tomu, že byl spáchán trestný čin.“

Orgány činné v trestním řízení si v roce 2020 vyžádaly součinnost NKÚ celkem v **7** případech. Na základě těchto žádostí poskytoval NKÚ kontrolní materiály ze **2** kontrolních akcí. Povinnosti mlčenlivosti zbavil prezident NKÚ v uvedeném roce celkem **9** zaměstnanců, a to z důvodu důležitého veřejného zájmu.

Vývoj podaných trestních oznámení v uplynulém desetiletí zobrazuje následující graf.

Graf č. 3 **Zdroj: výroční zprávy NKÚ**

Z uvedeného grafu je patrný nárůst podaných trestních oznámení v letech 2010 až 2015 (s výjimkou stagnace mezi roky 2011 a 2012) a dále následný strmý růst mezi rokem 2017 a 2018. Absolutně nejvyšší počet trestních oznámení podal NKÚ v roce 2015. Podání se týkala např. oznámení, jehož předmětem bylo neoprávněné použití finančních prostředků z rozpočtu hlavního města Prahy a Evropské unie přidělených městské části, v důsledku proplacení prací, které ve skutečnosti provedeny nebyly. Dále se jednalo o případy poskytnutí dotace ze státního rozpočtu žadateli v rozporu s pravidly pro získání dotace, použití prostředků dotace na jiný než stanovený účel a uvedení nepravdivých a hrubě zkreslených údajů v žádosti o dotaci, nebo skutečnosti související s neoprávněným výdejem prostředků poskytnutých ze státního rozpočtu, a to úhradou faktur za konzultační služby, přičemž nebylo možné spolehlivě ověřit, zda plnění předmětu uzavřených smluv bylo uskutečněno.

Od roku 2018 počet podaných trestních oznámení opět klesá. Doufejme, že tento trend souvisí se změnou chování kontrolovaných osob, resp. preventivním účinkem provedených kontrol, a vydrží i v následujících letech. ■

Chytrá karanténa a eRouška z pohledu GDPR

Ing. Tereza Pavlíčková
Vedoucí oddělení Interního auditu
Pověřenec pro ochranu osobních údajů
Ministerstvo zdravotnictví České republiky

V souvislosti s pandemií covid-19 jsme na Ministerstvu zdravotnictví museli čelit řadě výzev, a to nejen zdravotních, ale také technologických. Procesy, které byly standardní pro běžné infekční nemoci, již nebyly dostatečné a muselo se začít pracovat na nových, efektivnějších a hlavně robustnějších systémech. V návaznosti na to vznikl, mimo jiné, projekt „Chytrá karanténa".

Chytrá karanténa

Projekt Chytré karantény 1.0 vznikal na jaře loňského roku v době nouzového stavu za mimořádných okolností. Cílem bylo v co nejkratším možném čase vytvořit nové nástroje, které by napomohly orgánům ochrany veřejného zdraví nejen při rychlém dohledávání kontaktů, ale i v plánování rozvolňování opatření na základě analýz a predikcí dalšího vývoje.

V květnu 2020 navazoval projekt Chytrá karanténa 2.0, který je logickým navazujícím souborem opatření, postupů a nástrojů, který je po plné implementaci a za stálého rozvoje digitalizace dostatečně robustním systémem, který umí velmi rychle reagovat i na skokové nárůsty náhlých ohnisek nákazy.

Projekt Chytré karantény 2.0 je rozdělen do těchto hlavních oblastí: dohledávání rizikových kontaktů a jejich izolování, testování, data a centrální monitoring. V současné době se jedná také o oblast očkování.

Hlavní nástroje Chytré karantény

EPI Dashboard – webová aplikace pro analýzu dat a sdílení poznatků na jednom místě v reálném čase a jejich vizualizaci o průběhu pandemie covid-19 v ČR i ve vybraných státech světa.

> **„Nástroje Chytré karantény jsou moderní a sofistikované nástroje, které mají velký přínos pro řízení samotné pandemie, avšak mohou představovat zásah do ochrany soukromí osob. Z tohoto důvodu byly všechny nástroje již při jejich vývoji detailně analyzovány z pohledu ochrany osobních dat."**

Situační mapa – mapový portál zobrazující jednotlivé datové vrstvy poskytované ostatními nástroji (Covid Forms App), aktuální polohy mobilních odběrových týmů a také denně

aktualizované vrstvy epidemiologické situace.

Covid Forms App – webový portál, který zabezpečuje shromažďování dat a informací z laboratoří, odběrových míst a KHS.

eŽádanka – nová funkcionalita, která digitalizuje proces žádosti o provedení testu od indikujícího lékaře nebo KHS až po vyhodnocení v laboratoři.

Jednotný informační systém KHS pro podporu call centra – komunikační nástroj, který je vystavěn na platformě call centra. Toto centrum je propojeno s dalšími komunikačními kanály a s informačními systémy KHS.

Vzpomínkové mapy – vzpomínkové mapy slouží k vizualizaci a k analýze dat nad mapovým podkladem. Hlavním cílem využití vzpomínkových map je pomoci pozitivnímu pacientovi vzpomenout si na místa, kde se pohyboval.

Mobilní aplikace eRouška – mobilní aplikace pro chytré telefony, která pomáhá snadněji, efektivněji a rychleji upozornit osoby, s nimiž v poslední době nakažení přišli do styku a u nichž je vysoké riziko nákazy.

GDPR a Chytrá karanténa

Nástroje Chytré karantény jsou moderní a sofistikované nástroje, které mají velký přínos pro řízení samotné pandemie, avšak mohou představovat zásah do ochrany soukromí osob.

Z tohoto důvodu byly všechny nástroje detailně analyzovány z pohledu ochrany osobních údajů a byla k nim zpracována veškerá dokumentace. Dle rozsahu zpracovávaných osobních údajů se jednalo o záznamy o činnostech zpracování a také o rozsáhlé Posouzení vlivu na ochranu osobních údajů – DPIA. Situace byla však velmi složitá, a to nejen kvůli nedostatku času, ale také inovativnosti některých nástrojů, se kterými veřejná správa neměla zkušenost. Jedním z takových nástrojů je mobilní aplikace eRouška.

Mobilní aplikace eRouška

K využití moderních technologií, zejména pak chytrých telefonů, přistoupila řada států po celém světě, za účelem efektivního dohledání potenciálně nakažených osob. Jednotlivé přístupy se liší jak využitými technologiemi, tak systémem sběru a uložení dat až po respektování principů ochrany osobních údajů.

Česká republika, respektive Ministerstvo zdravotnictví, vyvinulo také trasovací mobilní aplikaci – eRouška. Aplikace pomáhá upozorňovat potenciálně nakažené osoby onemocněním covid-19. Na rozdíl od jiných aplikací, eRouška nesleduje a nesbírá informace o poloze subjektu údajů, ale pouze anonymně zjišťuje, se kterými dalšími uživateli aplikace přišel uživatel do bližšího kontaktu. Aplikace má přidanou hodnotu zejména v identifikaci rizikových kontaktů, které nakažená osoba nezná, a nemůže je tedy nahlásit v rámci epidemiologického šetření. Například pokud jste jeli autobusem s lidmi, které neznáte, eRouška je ten správný nástroj, který tyto osoby může informovat o tom, že se pohybovaly u nakažené osoby a následně tuto informaci využít k tomu, že v této době například nenavštíví svou babičku, která patří do rizikové skupiny.

Aplikace eRouška je neustále vyvíjena a inovována. eRouška měla vyvinuty postupně dvě verze, které fungovaly na odlišném principu. Tyto principy měly významný dopad také na zpracování osobních údajů.

eRouška 1.0

První verze aplikace fungovala na částečně decentralizované architektuře, což znamená, že uživatelé a data o uskutečněných kontaktech byla skryta pouze před ostatními uživateli a třetími stranami; server však mohl de-anonymizovat pozitivně testované uživatele. Systém měl také funkci odeslání dat, díky níž nakažení uživatelé mohli rozhodnout o sdílení své historie uskutečněných kontaktů pro účely epidemiologického výzkumu. Pokud uživatel data odeslal, provozovateli a ostatním zúčastněným autoritám se zviditelnili potenciálně pozitivní kontakty uživatelů. Telefonní číslo zadané při registraci využila hygienická stanice, aby mohla co nejdříve kontaktovat uživatele, pokud bude mít na základě informací z eRoušky u nakaženého člověka podezření, že s ním byli v rizikovém kontaktu. Kontakty se nedozví, kdo je mohl nakazit, ani kde a kdy. Identita nakaženého je ochráněna.

Níže jsou uvedeny zásadní rozdíly mezi verzemi aplikace eRouška:

eRouška 1.0	Zásadní změny u eRoušky 2.0:
Technické problémy s během na pozadí na iOS	Spolehlivé fungování na iOS a Android
TraceTogether protokol (Singapur)	Protokol Apple/Google Exposure Notification API
Vyhodnocení rizikových kontaktů na serveru	Vyhodnocení rizikových kontaktů přímo na mobilech, nikoliv na serveru
Server zná identitu i vazby mezi nakaženým a kontakty	Anonymní schéma – server ani identifikovaný kontakt nezná identitu nakaženého
Pomůcka pro hygieniky při vyhledávání kontaktů	Varovný systém pro občany
Nemožnost interoperability s distribuovanými systémy	Mezinárodní interoperabilita
	Informační karta

Z pohledu GDPR byl tento **přístup založen na souhlasu uživatele aplikace**, tedy dle čl. 6 bod 1 písm. a) a čl. 9 bod 2 písm. a) obecného nařízení GDPR. Samozřejmě i samotná instalace aplikace byla zcela dobrovolná. Uplatnění práv subjektu údajů bylo zajištěno, odvolání souhlasu bylo možné kdykoliv samotným uživatelem, a to odinstalováním aplikace.

eRouška

eRouška 2.0

V návaznosti na celosvětový, a zejména evropský vývoj trasovacích aplikací bylo přistoupeno k úpravě eRoušky, a to jak z technického, tak procesního pohledu. Nová verze aplikace přinesla také **výrazný pozitivní dopad na ochranu osobních dat**, kdy je fungování ryze decentralizované a ke zpracování osobních dat dochází pouze nepřímo. Nové fungování eRoušky 2.0 klade větší důraz na odpovědnost občanů, protože již do procesu nevstupují hygienické stanice, upozornění na rizikový kontakt je zasláno pouze samotnému uživateli. Uživatel je instruován, jak má v tuto chvíli postupovat a je na něm, zda tak učiní. Stručně je fungování eRoušky 2.0 pospáno v níže uvedeném schématu.

Aplikace eRouška 2.0 byla vyvinuta tak, aby neprováděla přímo identifikaci subjektu údajů a aby minimalizovala zpracování osobních údajů na nejnižší možnou úroveň. Aplikace samotná neobsahuje osobní údaje. Ministerstvo zdravotnictví ani Hygienické stanice v tomto novém technickém řešení v rámci aplikace nemohou ztotožnit konkrétního uživatele aplikace.

Vzhledem k novému technickému řešení aplikace, analýzám právních titulů a také na základě konzultací s odbornou veřejností bylo přistoupeno ke změně právního titulu zpracování osobních údajů. eRouška 2.0 již není provozována na základě souhlasu, ale ve veřejném zájmu dle čl. 6 odst. 1 písm. e) a čl. 9 odst. 2 písm. i) GDPR jako nástroj pro splnění úkolu prováděného ve veřejném zájmu, kterým je pověřen správce v oblasti veřejného zdraví, při ochraně před vážnými přeshraničními zdravotními hrozbami.

„Nové fungování eRoušky 2.0 klade větší důraz na odpovědnost občanů, protože již do procesu nevstupují hygienické stanice, upozornění na rizikový kontakt je zasláno pouze samotnému uživateli.“

Celý systém je záměrně navržen tak, aby se naprosto minimalizovalo riziko zneužití údajů a aby všichni ti, kdo se na provozu aplikace podílejí, včetně společností Apple a Google, získali jen nezbytné množství údajů.

Z pohledu principů GDPR k identifikaci konkrétní osoby může dojít pouze nepřímo a ve velmi omezených případech – např. pomocí tzv. výběru vyčleněním z pohledu správce (recitál 26 GDPR) nebo formou zpětné reidentifikace subjektů údajů ze strany adresáta notifikace (jde o teoretickou možnost reidentifikace subjektů údajů s využitím přiměřených prostředků pro identifikaci, zejména informací o tom, s kým se v inkriminované době

setkal); tyto situace mohou nastat pouze v případě kombinace pseudonymizovaných údajů v aplikaci eRouška, vzájemné kombinace znalostí o procesu sdílení informací a kontextu z pohledu uživatele aplikace.

Česká republika se s eRouškou 2.0 zapojila do skupiny zemí využívající server Federation Gateway (EFGS), který je technickým řešením interoperability mobilních aplikací pro trasování v EU. Státy musí splnit technické požadavky, ale rovněž je nutné projít oficiální procedurou pro udělení povolení. Česká republika zaslala Evropské komisi žádost, na jejímž základě proběhne audit, resp. posouzení vlivu na ochranu osobních údajů (DPIA). Aktuálně byly všechny tyto kroky splněny a eRouška 2.0 již čeká na schválení a v nejbližších dnech začně využívat server Federation Gateway a bude přeshraničně interoperabilní.

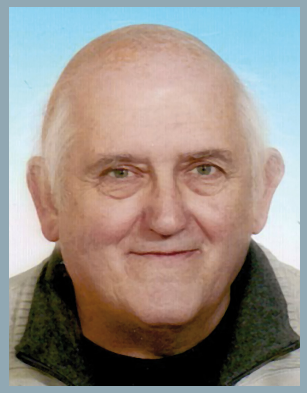
Aktuální statistiky

- Aktivované aplikace – přes 1,5 milionu
- Pozitivně testovaní, kteří varovali ostatní – přes 71 000
- Upozornění na riziková setkání – necelých 300 000

Závěr

Aplikace eRouška je významným pomocníkem v rámci celého systému vyhledávání a upozorňování rizikových kontaktů. Oblast ochrany soukromí a osobních dat byla při jejím vývoji prioritou, a jedná se tedy o velmi bezpečný nástroj pro veřejnost. Veškeré nástroje chytré karantény jsou průběžně konzultovány s Úřadem pro ochranu osobních údajů, který je pro Ministerstvo zdravotnictví v tomto ohledu klíčovým partnerem. ■

Přežije interní audit současnou pandemii?



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.

Zvládnutí pandemie nemoci covid-19 se stalo politickým, sociálním i ekonomickým úkolem 21. století. V roce 2020 se bez jakýchkoliv pochyb prokázalo, že pandemie zastihla nepřipravené – až na výjimky – všechny vědní obory a disciplíny, všechny vlády, parlamenty a politické strany, všechny lidské činnosti. K velkému překvapení se zjistilo, že není k dispozici propracovaná teorie, jak si počínat za mimořádné situace. Teorii krizového managementu v době pandemie tak suploval, více či méně úspěšně, selský rozum.

Opět se potvrdilo, že lidé nesmí pasivně čekat na změny, které za ně někdo vymyslí a rozhodne. Svůj život musí měnit aktivně, než jim ho někdo v rozporu s jejich představami a nadějemi změní. Změny nařízené shora se však uskutečňují velmi pomalu. Oproti tomu změny prováděné odzdola mají větší naději na úspěch. Příkladů, kdy se organizace vzájemně dohodly, jak společně postupovat v řešení problémů, je celá řada. Je tak třeba rozvíjet kvalitní management změn, být jejich iniciátorem, nejenom pasivním realizátorem.

Ačkoliv většina organizací umí identifikovat hrozby současných i nových rizik a má k dispozici plány pro případy mimořádné události (tzv. business continuity plans), na pandemii zareagovaly velmi pomalu a velmi nejistě. Velkou slabinou byla skutečnost, že takový plán rekonstrukce a rozvoje (co dál dělat jinak) neměly ani vlády. Přitom vlády se do takového úkolu musí pustit co nejdříve.

Ke škodě věci řádná analýza spolu s vyvozením závěrů a opatření u nás i v řadě jiných zemí z první tzv. jarní vlny nebyla provedena. Je pravdou, že některé

země byly připravenější, zejména asijské, jiné méně než ČR. Nicméně druhá, resp. třetí vlna by měla vést ke konkrétním plánům, jak se v případech mimořádné události chovat. Musíme být připraveni na další vlny i na nové pandemie. V každém případě je jisté, že i po zvládnutí té současné mnohé již nebude tak, jak bylo dříve.

„Pandemie zastihla nepřipravené – až na výjimky – všechny vědní obory a disciplíny.“

Pandemie urychlila rozvoj technologií, jako je umělá inteligence, automatizace, digitalizace, které přinášejí revoluci ve všech oblastech hospodářského života. Mizí celé kategorie pracovních míst a mění se samotná struktura společnosti i její názory na to, jaký ekonomický systém je pro ni nejlepší.

Čas pandemie covidu-19 jasně ukázal mnohé z výhod digitalizace. A to i těm lidem, kteří nejsou zrovna technologičtí nadšenci. Nositelem digitalizace byl v prvé řadě soukromý sektor. Novým jevem je skutečnost, že si lidé rychle uvědomili, že aplikace jako eRecept nebo eNeschopenka jim usnadňují komunikaci s lékaři a přinášejí i ochranu před rizikovými kontakty. Na druhé straně je třeba zdůraznit, že náš veřejný sektor ve srovnání s jinými zeměmi stále zaostává. Zdaleka nevyužívá možností, které moderní technologie a digitalizace přinášejí. Např. by mělo, v souvislosti s digitalizací státní správy, docházet k výraznému snižování počtu úředníků, což se zatím neděje.

Neměli bychom být pesimisty. Krize, způsobená pandemií, otevírá dveře novým příležitostem pro nová odvětví jako výroba nanovláken či 3D tiskáren. Naopak, některá odvětví, která prosperovala před rokem 2020, jako byla kongresová turistika, lázeňství, resp. turistika vůbec, provozování hotelů či letecká doprava, budou mít značné problémy. Lze očekávat poměrně velké změny ve světové ekonomice. Např. dojde k prudkému rozvoji průmyslu 4.0 a spolu s tím k širokému uplatnění nehierarchického, agilního řízení v organizacích.

Projevy pandemie a dopad na interní audit a v čem se musí interní audit přizpůsobit

Pokud vedení interního auditu zvažuje, jak bude interní audit fungovat po pandemii, musí začít oceněním rizik způsobených pandemií.

Určení nejlepšího přístupu, jak zvládnout příští krize, se neobejde bez rozboru minulých správných a špatných rozhodnutí. Interní auditoři musí v první řadě rychle získat zpětnou vazbu o budoucích cílech, úkolech a potřebách organizace. Jako vhodný nástroj se jeví šetření a dotazníky, kterými osloví vedení organizace, Výbor pro audit a ostatní klíčové třetí strany. Výsledky takových šetření poskytnou hodnotný input pro následné analýzy rizik a plánování auditní činnosti.

Interní auditoři musí dát přitom pozor na potencionální specifická rizika, týkající se vztahů s třetími stranami, dodavatelskými a odběratelskými řetězci. Pandemie covid-19 otevřela prostor pro využití robotizace, digitalizace, vzdálené elektronické komunikace. Ruku v ruce s tím stoupá enormně riziko výskytu technologické zranitelnosti organizace a podvodů. Na jedné straně se interní audit musí zabývat oblastmi, jako jsou kybernetická bezpečnost, business continuity management, IT bezpečnost. Na druhé straně auditoři musí zhodnotit adekvátnost připravenosti organizace, dovedností zaměstnanců, potenciálu organizace k působení pákového efektu technologií, jakož i opatření ke zmírnění rizik a působit k identifikaci a zmírnění rizika kybernapadení.

Zatímco není vždy možné anticipovat faktory, které mohou vést ke krizi, audit musí hledat odpověď na otázku, zda je organizace dostatečně flexibilní, aby přenastavila a znovu posoudila priority, pokud jde o obchodní cíle a komplexně řešila rizika. V každém případě však přístup k rizikům musí interní audit spojovat se strategií organizace. Je nutné počítat s tím, že frekvence ujišťování o riziku se zvýší. Interní audit musí s novými riziky počítat při tvorbě, resp. úpravě svých plánů.

Covid-19 demonstroval organizacím, jak je důležité disponovat vlastním robustním systémem řízení rizik. Podle našeho názoru v budoucnu uspějí ty organizace, jejichž interní auditoři se zaměřují na zkoumání dostatečnosti jejich systémů řízení rizik z hlediska zvládnutí krize a jejich schopnost uchopit potenciální příležitosti, které se projevují prostřednictvím inovačních podnikatelských modelů, např. dodávky online, internetový trh.

„Teorii krizového managementu v době pandemie tak suploval, více či méně úspěšně, selský rozum.“

Jedním z dalších kroků interního auditu by mělo být prověření přiměřenosti business continuity managementu z hlediska dopadu pandemie prostřednictvím testování efektivnosti tzv. business continuity (BC) plánů. Zkušenosti ukazují, že před pandemií postrádaly BC plány řady organizací náležitý rozpočet a trpěly nedostatkem zdrojů. Nelze se ani divit, když se organizacím daří, potřeba plánovat z hlediska příštích krizí není na pořadu dne.

Covid-19 rovněž odhalil systémové slabiny v tom, že interní audit nebyl zapojen do řešení dopadů pandemie včas. Např. průzkumy IIA (viz výsledky publikované na webu theiia.org) poskytují smíšený obrázek role interního auditu v pandemické krizi. Zatímco většina

vedoucích interního auditu (CAE) informovala, že byli zapojeni do reakcí organizací na covid-19 v době průzkumu, 37 % uvedlo, že měli být zapojeni do diskuse, jak reagovat na rizika a potenciální reakce, dříve. Pouze 43 % CAE bylo přesvědčeno, že byli zapojeni včas. Tato čísla musí vést interní auditory k tomu, aby zhodnotili, zda po nich management žádal prověřit BC plány organizace i jednotlivých úseků včas.

„Musíme být připraveni na další vlny i na nové pandemie.“

Zkušenosti z pandemie by měly přimět CAE k tomu, aby si našli čas i na vytváření, resp. přehodnocení jejich vlastních BC plánů. Takové plány by měly umožnit jejich týmům, aby byly dobře obeznámeny se vzdálenými auditními technikami a používanými technologiemi. Podle našeho názoru je však důležité, aby se našly zdroje pro identifikaci a řešení překážek v používání takových technologií.

Interní audit v těchto plánech musí počítat s tím, že bude méně auditů na místě (in situ) a bude se více opírat o analytická data, u kterých musí být ošetřena jak jejich věrohodnost, tak i kyberbezpečnost. A vzdálený přístup k auditům se nevyhne tlaku na úsporu nákladů na pracovní cesty interních auditorů. Asi se však ne vždy podaří zamezit momentu tzv. „strategického překvapení“, kdy z řady důvodů (např. vládními regulačními opatřeními) nebude možné plánované audity dokončit, resp. ani je nebude možné zahájit.

Interní auditoři by neměli opomenout posoudit dostatečnost a pružnost politiky lidských zdrojů organizace, zejména zda odráží zájmy zaměstnanců. Během pandemie totiž dochází ke změnám či přesunům podnikatelské činnosti nebo ke změnám dodavatelů. Důležité rovněž bude zhodnotit dopad pandemie na organizační strukturu organizace. Stranou zájmu interních auditorů nesmí zůstat ocenění odolnosti zaměstnanců adaptovat se na překotně se vyvíjející rizikové prostředí prostřednictvím osvojení pracovních modalit na dálku.

Auditoři rovněž musí prověřit, zda existují postupy organizace pro bezpečnost a hygienu zaměstnanců a zda zaměstnanci mají dovednosti pracovat v prostředí s limitovaným či žádným osobním kontaktem, včetně zvážení potenciálních sociálních společenských vzdálenostních restrikcí.

Práce z domova (tzv. home office) s sebou přináší i nové nároky na kvalitní a účinný vnitřní kontrolní systém. Interní auditoři musí sehrát aktivní roli při zavádění samokontroly a při ověřování produktivity práce při práci z domova. I když se jedná o práci z domova, její výkon v praxi se odehrává v řadě ubytovacích zařízení, často i v zahraničí. Základním kritériem jejich výběru se stává možnost napojení na internet. A často je tato práce spojována s rodinnou rekreací. V souvislosti s prováděnými samokontrolami nelze proto zapomínat na internetovou bezpečnost a na možnost vykazování neoprávněných výdajů, neboť každá krize zvyšuje rizika podvodného jednání. Ta se mohou např. objevit i v souvislosti s tlakem na snižování mezd a snahou zaměstnanců výpadek příjmů něčím nahradit na úkor organizace. Jiná rizika přinášejí i změny v dodavatelsko-odběratelských vztazích, které mohou dávat prostor pro úplatky. Při práci z domova často vázne vzájemná komunikace odpovědných pracovníků. Navíc nemusí být v potřebné době na pracovišti přítomni ti pracovníci, kteří mají oprávnění organizaci zastupovat a odsouhlasení výdajů či jiných dokumentů se mohou ujmout neoprávněné osoby. Jako podvodné se v čase může ukázat i přijímání různých státních podpor spojených se snižováním dopadů pandemie, pokud se zjistí, že organizace na tyto podpory neměla nárok. Interní auditoři by proto neměli na rizika možného podvodného jednání zapomínat.

Paralelně se musí interní audit zaměřit na fungování vnitřní správy a řízení (governance) organizace, zejména managementu. Pandemie ukázala, že 30–50 % činností, které firma nebo organizace standardně prováděla, dělat vůbec nemusí. Např. služební cesty, účast na konferencích a seminářích, pracovní schůzky. Osobní kontakty by se neměly rušit, nicméně je třeba ke zvýšení efektivity využít online kontaktů. Naše zkušenost je taková, že videokonference, teleworking jsou dobrým nástrojem na předání informací, ale špatným nástrojem na řešení problémů.

„Hlavní důraz klademe na implementaci strategie štíhlého ale zcela profesionálního týmu interních auditorů.“

V neposlední řadě centrem pozornosti interního auditu musí být transparentnost, konzistentnost a spolehlivost informací. Primárně se jedná o informace, vydávané vedením organizace, které umožní zaměstnancům, klientům a investorům, aby byli seznámeni s jeho rozhodnutími v době krize. Pandemie ovlivňuje přístup interního auditu zejména tím, že klade jiné nároky na komunikaci s managementem i Výborem pro audit. Ta nabývá především elektronické podoby a je nutné zajišťovat její bezpečnost. Zkušenosti z pandemie též poskytují příležitost CAE vytvořit nebo prověřit jejich vlastní přístupy, jak proaktivně komunikovat s vedením organizace a Výbory pro audit o dopadu pandemie na byznys, změnách v rizikovém profilu a výsledcích přehodnocení plánů interního auditu a o nových auditních zakázkách.

Směrem k příští normální situaci

Nikdo neví, jak dlouho krize bude trvat, ale její dopad může nadále ovlivňovat světovou ekonomiku na měsíce, či dokonce roky. Podaří-li se internímu auditu prověřit účinnost opatření, kterými se organizace snaží pandemii čelit, bude mít zároveň příležitost se sám posunout do role většího poskytovatele přidané hodnoty. Může nejen předávat zkušenosti, získané během krize, ale i pomoci narýsovat cestu k příští normální situaci.

S ohledem na projevy pandemie covid-19 musí vedení interního auditu v prvé řadě aktualizovat rozvojovou strategii IA. Hlavní důraz klademe na implementaci strategie štíhlého, ale zcela profesionálního týmu interních auditorů. Současně zdůrazňujeme nutnost aktivního působení interního auditu ke zvýšení spolupráce s druhou obrannou linií. Nicméně bychom se – a v tomto bodě nesouhlasíme s jinými interními auditory – bránili integraci s některými funkcemi druhé obranné linie (např. compliance). Vedlo by to totiž k tomu, že by interní audit neposkytoval pozitivní přidanou hodnotu organizaci ve formě kvalitního poradenství. Vycházíme ze skutečnosti, že interní auditor zná nejlépe vnitřní prostředí organizace, a může tak fungovat jako nepostradatelný interní poradce v oblasti správy a řízení, včetně strategického řízení rizik, jejích procesů a činností.

Pokud má v organizaci IA plnit roli manažerského nástroje, vyžaduje dostatečné finanční zdroje, moderní technické prostředky a profesionální tým interních auditorů. Kvalifikace, výběr a rotace interních auditorů, jejich průběžné vzdělávání a osobní rozvoj musí reagovat nejen na dynamický rozvoj vnitřního prostředí organizace, ale i na vnější okolí. Vzhledem k tomu musí být osobní rozvoj interních auditorů zaměřen především na školení v oblasti ověřování nových přístupů k řízení rizik, znalost informačních technologií, kybernetickou a technologickou bezpečnost organizace, digitalizaci, různé datové analytické služby, oblast ověřování a zabezpečování interní i externí komunikace a robotizace procesů uvnitř organizace. Jedině tak lze zabezpečit, že interní auditoři budou schopni identifikovat a vyhodnocovat nová rizika a hrozby.

Definice zůstává, ale organizace interního auditu se musí změnit

V žádné z krizí neschází tlak na snižování nákladů, který často vede k úvahám o možném zrušení interního auditu v organizaci, neboť interní audit je chápán jako nákladová funkce, nepřispívající ke zvyšování hodnoty organizace. Interní audit proto svou nezastupitelnost pro organizaci musí trvale prokazovat. Musí řešit i rozpor mezi tlakem na snižování nákladů na vzdělávání interních auditorů, který bude silný v řadě organizací, a nutností kvalifikačního rozvoje interních auditorů, jak se o tom zmiňujeme v předchozím odstavci.

Profese interního auditu se musí podle našeho mínění urychleně přizpůsobit novým výzvám, které pandemie klade. I když se definice interního auditu nemění, nadále platí, že interní auditoři musí být flexibilní, jednat odpovědně a úzce spolupracovat s obrannými liniemi a různými zúčastněnými stranami. Interní audit musí reagovat zejména na budoucí rizika v reálném čase a na nové výzvy.

> **„Stoupá enormně riziko výskytu technologické zranitelnosti organizace a podvodů.“**

Podle našeho názoru je blízko doba, kdy dojde k transformaci útvarů interního auditu na tým, který poskytuje organizaci ujištění, zda dostatečně čelí hrozícím rizikům, a tým, který poskytuje organizaci poradenské služby, tj. vytváří pozitivní přidanou hodnotu a zlepšuje fungování organizace. Kromě měnícího se portfolia auditorských služeb musí interní audit zachovávat svou nezávislost a objektivitu, mít potřebnou autoritu a být důvěryhodný.

A co nezávislost interního auditu v době krizového dopadu covid-19 na role a odpovědnosti IA?

Od mnohých CAE se požaduje, aby delegovali několik členů týmu do jiných útvarů, a pomohli tak vedení organizace v boji s pandemií. V souvislosti s tím se CAE musí postarat o udržení nezávislosti interního auditu. Další otázkou je skutečnost, zda by neměli v době krize interní auditoři a Výbory pro audit pojímat nezávislost jako sekundární při poskytování maximální přidané hodnoty. V neposlední řadě musí CAE řešit otázku, zda vůbec pomoci vedení, jak jen to je možné, anebo odmítnout pomoc v zájmu udržení nezávislosti.

Jsme toho názoru, že situace kolem pandemie určitě zvýrazní roli interního auditu. Jeho unikátní pozice a profesionalita ho předurčuje k tomu, aby poskytoval organizaci kvalitní poradenské služby, a tím napomáhal k neustálému zdokonalování jejích vnitřních procesů, zejména řízení rizik a kontrolních mechanismů. Jako vnitřní poradce může interní audit působit dokonce k hledání optimálního řešení. Avšak to v žádném případě neznamená, že přebírá odpovědnost za rozhodnutí vedení či vlastnictví rizik.

Zatímco postavení poradenských služeb je odůvodněné v rámci moderního pojetí interního auditu, pandemie posunula interní auditory do rolí mimo jejich zaběhlou zónu. Některé auditní funkce doznaly změn vně jejich tradičního rozsahu působnosti, i když to může vést k ohrožení nezávislosti jejich funkce a oslabení jejich objektivity. Např. díky jejich znalosti rizik a kontroly se někteří auditoři přesunuli dočasně do útvarů druhé či první obranné linie. Jiné útvary IA analyzují procesy, které jsou nejvíce ovlivněny covid-19 a identifikují

potřebné změny v klíčových kontrolách, aby minimalizovaly riziko v hlavních procesech organizace.

CAE by měl být schopen v krizi předvídat, v kterých oblastech poskytne vedení a orgánům správy a řízení organizace co největší přidanou hodnotu z poradenských služeb. Např. interní auditoři mohou pomoci vedení koncipovat a realizovat náležité strategie ke zmírnění rizik nebo mohou identifikovat a upřednostňovat nová v souvislosti s pandemií vyvstalá rizika, která ohrožují nosné strategie organizace. Určitou pomoc jim mohou poskytnout studie, které se zabývají aktuálními i budoucími riziky a jsou publikovány jak na stránkách Mezinárodního (IIA), tak i Evropského institutu interních auditorů (CEIIA). V současnosti se jedná o „On Risk 2021 report" (IIA) a „Risk in Focus 2021 report" (ECIIA).

„Video-konference, teleworking jsou dobrým nástrojem na předání informací, ale špatným nástrojem na řešení problémů."

Zároveň je třeba konstatovat, že poskytování poradenských služeb by však nemělo ohrozit v žádném případě rutinní ujišťovací práci interních auditorů. Interní audit musí nadále aplikovat přístup založený na rizicích v plánování a uskutečňování auditních plánů. Pokud se mění rizikový profil organizace, musí se přehodnotit a upravit, resp. doplnit, i plán auditu. V době pandemie musí být interní audit ve stálém spojení s Výborem pro audit a ostatními třetími stranami, včetně těsného spojení s externím auditorem. Středem pozornosti se musí stát aktuálnost plánu auditu, vyřazování nepotřebných zakázek a zařazování nových, vyvolaných dopadem pandemie.

Nezávislost funkce interního auditu není samoúčelná, ale všemi auditory je vnímána jako prostředek, který zabezpečuje objektivitu, nestrannost, oprávnění a kredibilitu interních auditorů. Je-li funkční nezávislost či objektivita auditorů ohrožena kvůli těsným vztahům s managementem a kvůli jejich zapojení do neauditních činností, je vždy důležité včas vestavět náležitou obrannou brzdu a pojistky. Interní auditoři musí prostřednictvím aplikace profesionálních standardů trvat na objektivním posuzování a zdržet se předpokládaných manažerských odpovědností. Ve všech takových případech musí být CAE včas informován a schvalovat dodatečné úkoly, které byly vyžádány vedením a managementem. Pokud jsou tyto pojistky nedostatečné, pak by CAE měl doporučit použití skupinového či externího auditora. CAE tak musí mít stoprocentní jistotu, že fungují odůvodněné obranné pojistky v případech, kdy reaguje na naléhavé potřeby vedení.

„Pandemie posunula interní auditory do rolí mimo jejich zaběhlou zónu."

Vzniká otázka, zda má interní audit sáhnout po kompromisu mezi tím, že bude nezávislý, a tím, že bude nápomocný zvláště v době krize. Odpověď je důrazné ne. Při dodržování profesionálních standardů, pojistek a dohledu ze strany Výboru pro audit tak musí interní audit poskytovat organizaci přidanou hodnotu ve formě konkrétních, nezávislých a objektivních analýz, ujištění a poradenských služeb.

Závěr

Zkušenosti ukazují, že generální manažeři – vizionáři přistoupili k tvorbě strategických rozhodnutí z hlediska nastolení normální, i když nové situace daleko před tím, než došlo k uvolnění regulačních opatření, resp. postupnému zvládání pandemie. Avšak všichni musíme mít na paměti, že nová situace bude hodně odlišná od té, co jsme znali.

Nicméně aby interní auditoři mohli stanovit strategická opatření, musí nezávisle zhodnotit, jak zvládli současnou krizi. Zastáváme názor, že hlavním úkolem interních auditorů je zabránit, aby se organizace za čas neocitly před další, a ještě horší globální hrozbou a nebyly zaskočeny a nepřipraveny. Interní auditoři musí ocenit nejen pandemickou připravenost organizace, ale i jejich vlastní připravenost k poskytnutí větší přidané hodnoty svým klientům. Dobrá zpráva pro interní auditory je, že ani v budoucnosti nebudou nahrazeni robotickou kontrolou, protože lidský faktor je v této oblasti přes veškerou jeho omylnost nenahraditelný. ■

S využitím zahraniční literatury

TIPY PRO AUDIT VYDÁVÁNÍ PLATEBNÍCH KARET

Ing. Jana Šorfová, FCCA

Interní auditorka, mentorka v mentoringových programech ČIIA a Equilibrium (Britská obchodní komora), lektorka finanční gramotnosti dětí a dospělých, zahradní designérka.

Kontakt: jsorfova@centrum.cz

Milí kolegové,
téměř celý svůj profesní život se zabývám auditem, jak externím, tak interním. Napadlo mne, že by se vám, kteří dnes a denně hodnotíte stav vnitřního kontrolního prostředí ve finančních institucích, a nejen v nich, mohl hodit seriál tipů, na co ve vybraných oblastech nezapomenout. Budu velmi ráda, pokud mi zašlete jakékoliv případné podněty a připomínky ze své praxe k uvedeným tématům.

Seriál jsem rozdělila na následující okruhy:

- Proces vydávání platebních karet
- Přijímání platebních karet, vč. provozu bankomatové sítě
- Finance a daně
- Data, marketing a externí komunikace

Dnes tedy několik tipů k vydávání platebních karet. Jak vlastně ale procesy vypadají a existuje někdo ve vaší organizaci, kdo je má celé popsané – od zelené louky až například do reportingu do ČNB? Velmi pravděpodobně ne. Budou existovat útržky popisu procesů v několika odděleních, jako auditor ho budete asi pravděpodobně skládat poprvé. Já to dělám tak, že si celý proces představím jako vývoj v čase a kladu auditovaným například níže uvedené typy dotazů. Vždy hledám někoho (tj. ne systém), kdo danou oblast kontroluje. Pokud tam není žádná osoba, která by oblast vyhodnocovala, popř. sledovala a vyhodnocovala chybové hlášky ze systémů, nedává moc smysl trávit auditorský čas dalším zkoumáním.

V karetním průmyslu u vydávání karet nezapomeňte na uzavírání smluv např. se SIA, VISA a Mastercard, všimněte si, jak obšírné jsou jejich poplatkové politiky a jak obrovské různorodé soubory se vám budou denně automaticky načítat do systémů.

Ze své praxe jsem pro vás vybrala následující tipy na zamyšlení a otázky pro auditované:

- Víte jistě, že se včas načtou všechny soubory, a nejsou v nich duplicity a obsahují jen částky, které tam mají být?
- Máte dobře vymyšlenou účetní metodiku, na jaké účty se mají spousty údajů účtovat?
- Je za každým účtem hlavní knihy odpovědná účetní nebo někdo jiný, který ví, zda ta spousta údajů dává smysl, nic tam není dvakrát a nic nechybí?
- Existují kontroly, které vás ujistí, že například číslo karty nemáte tam, kde být nesmí?
- Trochu na odlehčenou – máte zajištěny dostatečné dlouhodobé dodávky plastů na výrobu karet a dobré a pravidelně vyhodnocované smlouvy s těmi, kdo do nich dávají čipy?
- Co se stane, když některý z dodavatelů bude mít problémy – budete je mít také, nebo máte náhradní plán?

Pokud v organizaci naleznete uspokojivé efektivní kontroly na výše uvedené, můžeme přejít na distribuci karet klientům:

- Jak je distribuce ke klientovi ochráněna od možného zneužití například pracovníkem pobočky nebo někým jiným?
- Jak se řeší a vyhodnocují reklamace, a jak vlastně klient ví, že jeho karta je připravená k vyzvednutí nebo že přijde poštou?
- Jaké druhy karet vydáváte a dává to ekonomický smysl – opravdu potřebujete desítky druhů? Kdo toto vyhodnocuje a jak?

Pro oblast reportingu a řízení jsem vybrala následující okruhy otázek:

- Jak vlastně vypadá manažerský reporting – obsahuje všechny typy výnosů a nákladů a kdy a jak se počítají průměry – neměly by být vážené?
- Jak vypadá reporting do ČNB – není možné, že se některé typy karet do reportu vůbec nedostanou?
- Kdo a jak reporting pravidelně kontroluje na vaše sub-systémy a jsou v nich data správná, úplná a včas?
- Využíváte dostatečně datové analýzy, a popř. umíte je správně interpretovat?
- Kdy a jak poznáte, že v systémech jsou neúplná, duplicitní, zastaralá nebo jinak chybná data?

V každém procesu, který auditujete, nezapomeňte na test efektivnosti kontrol přístupových oprávnění, kapacity a stálosti relevantních systémů a jejich IT podpory, transferových cen, KPIs klíčových pracovníků a jejich zastupitelnosti. Ptejte se jich také na množství práce a celkovou spokojenost. A nezapomeňte, kdo se nezeptá, ten to neví a ani by neměl hodnotit.

Všem vám i vašim auditovaným přeji hodně štěstí a spokojenosti! ■

NOVINKA

Komentář k zákonu o finanční kontrole ve veřejné správě

Jana Czudek Kranecová, Damian Czudek,
Tereza Koucká Hőfferová, Andrea Vuongová

Zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, byl vytvořen v rámci přípravy na vstup České republiky do Evropské unie. Navzdory tomu, že měl být jen přechodným řešením, zůstal zákon o finanční kontrole doposud v prakticky nezměněné podobě. Okruh jeho adresátů zahrnuje orgány státní správy i samosprávy a dále například i příspěvkové organizace, které nejsou správním orgánem. Z tohoto důvodu je právní úprava v něm obsažena obecná a pro zavedení do praxe vyžaduje značnou dávku znalostí a zkušeností.

Komentář, který je čtenářům předkládán, má být praktickým pomocníkem pro všechny orgány veřejné správy při nastavování finanční kontroly. Jedná se o jedinečnou publikaci, která kromě toho, že obsahuje právní výklad jednotlivých ustanovení, přináší i konkrétní příklady a doporučení, které pomohou posílit systém ochrany veřejných prostředků.

450 Kč

www.alescenek.cz

18. setkání interních auditorů z finanční oblasti

23. února proběhlo už 18. setkání interních auditorů z finanční oblasti, které Český institut interních auditorů tradičně pořádal ve spolupráci s Českou bankovní asociací a KPMG Česká republika. Podruhé se toto setkání konalo formou webináře a sledovalo ho více než 200 účastníků. Setkání zahájil Michal Čup z KPMG společně s výkonnou ředitelkou ČBA Monikou Zahálkovou, prezidentem ČIIA Tomášem Pivoňkou a guvernérem ČNB Jiřím Rusnokem.

Úvodního slova se ujal vzácný host, guvernér České národní banky Jiří Rusnok, který dodatečně popřál ČIIA k 25. narozeninám. Vyzdvihl užitečnost interního auditu ve finančním sektoru jako nezávislého hlasu, který přispívá k posilování řídicího a kontrolního systému a pomáhá zkvalitňovat organizaci. Podle guvernéra se v souvislosti s pandemií dostávají do popředí zájmu manažerů i interních auditorů nová rizika: *„Veškerý finanční svět funguje z mnoha procent ve virtuálním světě, ale to nijak nezmenšuje rizika, se kterými se potýká. Dokonce přibyla rizika další, zejména spojená s technologií: kybernetická rizika, záležitosti business continuity managementu a krizového řízení.“* Tyto změny s sebou podle guvernéra nesou zvyšující se požadavky na rozvoj dovedností interních auditorů.

ČNB se podělila o zkušenosti s provozem Centrální evidence účtů

Dalším hostem byl Petr Staněk, ředitel sekce statistiky a datové podpory v České národní bance, který prezentoval *„První zkušenosti při provozování Centrální evidence účtů (CEÚ)“* a představil vývoj legislativního rámce a regulace CEÚ. S účastníky setkání také sdílel hlavní problematické body kontrolních návštěv ČNB u bankovních institucí: *„Například spousta spořitelen si myslela,*

že smlouvou o zřízení stavebního spoření vzniká také účet do evidence CEÚ, což vůbec není pravda.“ ČNB také banky často upozorňovala na důležitost ochrany osobních údajů a diakritiky: *„Nutíme instituce k opravám, pokud najdeme rozdíly v diakritice mezi smluvní dokumentací a tím, co je vykázáno v centrální evidenci účtu.“* Staněk dodal, že od roku 2018 národní banka navštívila 42 úvěrových institucí. Kontroly uzavřela u 22 z nich.

Makro okénko Mojmíra Hampla

Na pana Staňka navázal Mojmír Hampl, který v KPMG vede poradenské služby pro finanční sektor. Vyjádřil se k očekávanému vývoji hlavních „makro“ ukazatelů v roce 2021: k hospodářskému růstu, veřejnému dluhu a inflaci. *„Covid-19 je jako ‚menší válka‘. Nárůst veřejného dluhu ve vyspělém světě, ale i v rozvíjejících se ekonomikách, dosáhne vrcholu, jaký jsme viděli naposled během druhé světové války,“* okomentoval makroekonomické vyhlídky Hampl. *„Když vezmu faktory, které mluví pro vyšší a nižší inflaci, a pominu faktor nejistoty ohledně možné velké spotřebitelské euforie po pandemii, tak bych řekl, že pro udržení inflace bude klíčová jediná věc: nezávislé centrální banky s mandátem udržovat inflaci nízko,“* shrnul názor na budoucí vývoj inflace Hampl. Všechny ostatní ukazatele se podle experta z KPMG mohou vyvíjet libovolně vzhledem k velké míře nejistoty spojené s vývojem pandemie a jejím zvládáním.

ESG a jeho vliv na české banky

Nosné téma setkání *„Jak se mění tradiční bankovnictví v souvislosti s ESG a udržitelným financováním?“* uvedli Martin Křivánek a Lukáš Bajgar z KPMG. Martin Křivánek na úvod vysvětlil, co se skrývá za tou, pro řadu posluchačů neznámou, zkratkou ESG. Poté nastínil klíčové oblasti dopadu na banky, jejich funkci, řídicí a kontrolní systém, tržní transparentnost a procesy řízení rizik. *„Zajímavé je, že v oblasti řízení rizik, která tou regulací bude postižena nejvíce, je zatím výrazný prostor pro růst,“* okomentoval výsledky průzkumu na téma ESG u českých bank Křivánek. Na závěr svého vystoupení shrnul, že více než 65 % současných auditních témat v sobě zahrnuje také aspekty ESG a interní audit na ně bude muset být odborně i kapacitně vybaven: *„ESG bude v těch prvních letech zejména o kvalitativních informacích a až v dalších letech se překlopíme do klasických skórovacích modelů.“*

Panelovou diskusi si vzal na starost Lukáš Bajgar. Velmi zajímavé postřehy o aktuálnosti tématu ESG a udržitelném financování přinesli ředitelé útvarů interního auditu významných institucí: Sylva Floríková (Česká spořitelna), Lenka Landa Schejbalová (Komerční banka), Markéta Hruboňová (Generali Česká pojišťovna) a Tomáš Pivoňka (skupina ČEZ). Panelisté se shodli, že ačkoliv se regulace v ESG oblasti teprve chystá, tak ve všech těchto institucích téma ESG již několik měsíců velmi rezonuje. Ovlivňuje jak jejich strategii a obchodní model, tak i mění zavedené procesy a přístupy k vyhodnocování rizik. Týmy interního auditu v těchto institucích již ESG zohledňují ve svém auditním plánu.

Pokud jste se nemohli zúčastnit a rádi byste se dozvěděli více, pusťte si záznam na YouTube.

Na závěr bych ještě jednou rád poděkoval všem vystupujícím za jejich příspěvky a také mým kolegům z KPMG týmu Markets and Marketing za přípravu a realizaci online přenosu. ■

Michal Čup

ČESKÝ INSTITUT INTERNÍCH AUDITORŮ

ČESKÁ BANKOVNÍ ASOCIACE / CZECH BANKING ASSOCIATION

KPMG

Noví členové

- Ing. Petr Bimka, ČEPS, a.s.
- Ing. Tereza Blažková, Plzeňská teplárenská, a.s.
- Ing. Jan Brabec, MBA, Správa služeb hlavního města Prahy
- Bc. Věra Daňková, Česká spořitelna, a.s.
- Mgr. Linda Doan, PricewaterhouseCoopers Audit, s.r.o.
- JUDr. Kristína Duraj Chochlíková, Ministerstvo financií SR
- Ing. Bc. Jana Haidlová, DiS., Statutární město Liberec
- Ing. Petra Holešová, Statutární město Ostrava
- Ing. Markéta Houšková, Český telekomunikační úřad
- Ing. Tomáš Hubal, Správa železnic, státní organizace
- Mgr. Pavlína Jandová, Fakultní nemocnice Bulovka
- Ing. Barbora Jarošová, Výzkumný ústav lesního hospodářství a myslivosti, v.v.i.
- Mgr. Miroslava Jasenčáková, Individuální členka
- Ing. Pavel Kašpar, České dráhy, a.s.
- Ing. Jitka Kazimírová, CIA, Individuální členka
- Bc. Milan Klas, Individuální člen
- Ing. Jan Kubíček, AGEL a.s.
- Mgr. Jan Kubů, Fakultní nemocnice Bulovka
- Ing. Kateřina Mandíková, Dopravní podnik hl. m. Prahy, akciová společnost
- Ing. Bc. Marek Medve, Jihočeská univerzita v Českých Budějovicích
- Ing. Hana Murphy, ČSOB Pojišťovna, a. s., člen holdingu ČSOB
- Ing. Marek Pazdera, Západoslovenská energetika, a.s.
- Ing. Tomáš Petrák, Komerční banka, a.s.
- Ing. Petr Ptáček, MONETA Money Bank, a.s.
- Ing. Gabriela Raková, Správa železnic, státní organizace
- Ing. Michal Rajtora, Česká spořitelna, a.s.
- JUDr. Roman Růžička, Česká národní banka
- Ing. Anna Schreiberová, Deloitte Audit s.r.o.
- Miroslav Soukup, Ministerstvo životního prostředí ČR
- Dominika Smiková, Deloitte Audit s.r.o.
- Mgr. Ing. Lucien Strnad, UniCredit Bank Czech Republic and Slovakia, a.s.
- Ing. Marcel Sufčák, Generali CEE Holding B.V., organizační složka
- Ing. Radmila Sukupová, Statutární město Ostrava
- Ing. Simona Šabartová, Generali CEE Holding B.V., organizační složka
- Iva Škrabalová, MA, Individuální členka
- Petr Štěpánek, Individuální člen
- Ing. Erika Štěpánková, DiS., Zařízení služeb pro Ministerstvo vnitra
- Mgr. Stanislav Švára, Státní zemědělský intervenční fond
- Ing. Lenka Švecová, Státní pozemkový úřad
- Mgr. Monika Tengler, AGEL a.s.
- Bc. David Toman, Innogy Česká republika a.s.
- Petr Tuka, Individiuální člen
- Ing. Libuše Uherková, Uherskohradišťská nemocnice a.s.
- Terezie Urmaničová, MSc., BOHEMIA ENERGY entity s.r.o.
- Ing. Pavla van Dam Marková, Generali Česká pojišťovna a.s.
- Ing. Alexandra Vašašová, Ministerstvo financií SR
- Ing. Petr Vokáč, Krajský úřad Ústeckého kraje
- Ing. Vladislav Volenec, Centrum pro regionální rozvoj ČR
- Ing. Iveta Výtisková, MONETA Money Bank, a.s.
- Ing. Hana Wilferová, Plzeňský Prazdroj, a. s.
- Ing. Vladimíra Zacharidesová, Ministerstvo financií SR
- Ing. Lukáš Ziegler, Česká spořitelna, a.s.
- JUDr. Ing. David Zimandl, PST CLC, a.s.

RODINNÉ A VZDĚLÁVACÍ CENTRUM HOLOUBEK

Milena Vohralíková,
koordinátorka Rodinného a vzdělávacího centra Holoubek

Oblastní charita Pardubice má své sídlo v Holicích, ve městě známém jako rodiště afrického cestovatele Dr. Emila Holuba.

Centrum vzniklo v roce 2011 z dobrovolné aktivity maminek, dále za nesmírné podpory Oblastní charity Pardubice a paní ředitelky Mgr. Marie Hubálkové.

Záměrem bylo vytvořit prostředí, kde by se mohly celé rodiny scházet, vzdělávat se a kde dětem bude umožněno získávat poznatky a vědomosti ve všech oblastech výchovně vzdělávacích.

Na Holicku žije 17,5 tisíce občanů. V samotných Holicích, kam je většina maminek zvyklá dojíždět za pediatry, žije téměř 7000 obyvatel. V okruhu 20 km není žádné obdobné zařízení pro setkávání rodin s dětmi, které by nabízelo komplexní služby, jak v oblasti poradenství, tak i při praktických činnostech. Postupně od založení centra se nabídka vzdělávacích programů pro děti, dospělé i seniory stále rozšiřuje a reaguje na jejich aktuální potřeby. Provoz centra je každý pracovní den a je otevřené všem bez rozdílu sociálního postavení a bydliště. Vždy rádi přivítáme rodiny vyžadující pomoc. Rodinné centrum spolupracuje se Sociálním odborem města Holic, takže jsme tu i pro rodiny s dětmi ze znevýhodněného prostředí. Našimi návštěvníky jsou především rodiny s dětmi od narození až po školní věk, těhotné ženy a také senioři. Pro všechny máme připravené pravidelné programy i jednorázové akce. Rodiny v nabídce centra najdou hudebně pohybové aktivity, cvičení pro děti od 4 měsíců do 3 let ve skupinách respektující věk, aktivity s prvky Montessori, keramiku pro děti i dospělé, chvilky pro šikovné ručičky, cvičení pro těhotné a speciální kurzy pro seniory např. Trénink paměti a práce s počítačem.

Již desátým rokem mohou v Holoubku, zejména matky na rodičovské dovolené, absolvovat bezplatné vzdělávací kurzy osobního rozvoje, počítačových a jazykových dovedností.

Naše centrum navštíví průměrně 5600 klientů, v době pandemie v důsledku dodržování vládních nařízení se počet návštěv snížil. V době, kdy centrum muselo být pro veřejnost zcela uzavřeno, jsme poskytovali služby dětem rodičů záchranných složek s celodenním zaopatřením.

Vzhledem k tomu, že žádné aktivity centra nejsou realizovány komerčně, musíme řešit otázky finančního zajištění provozu i kvalitních lektorů prostřednictvím dotací MPSV z programu Rodina, dotací z prorodinného programu od Pardubického kraje a poskytnutím podpory města Holice za projekt Holoubku leť. Účastníme se i Burzy filantropie a nesmírně vítáme přízeň sponzorů, protože každá získaná finanční částka umožní zavést novou aktivitu pro klienty našeho centra.

Další služby pardubické Oblastní charity na Holicku spočívají zejména v podpoře rodin například při péči o blízké osoby prostřednictvím holického střediska Pečovatelské služby. Pomoc poskytujeme terénní i ambulantní formou. Další středisko v Holicích zajišťuje terénní Domácí zdravotní péči a komplexní podporu umírajícím a jejich rodinám v rámci Domácího hospice Andělů strážných. Na Holicku dále působí charitní sociální pracovnice Sociálně aktivizačních služeb pro rodiny s dětmi a Služeb pro pěstouny. Pro pečující a jejich blízké jsou určeny služby dvou pobytových a jednoho ambulantního střediska Odlehčovacích služeb Červánky, pro tyto klienty je zajišťována i doprava do středisek speciálně upravenými automobily pro přepravu osob se sníženou pohyblivostí. Obyvatelům regionu dále nabízíme služby Půjčovny kompenzačních pomůcek, Dopravu a doprovod osob a Domácí práce všeho druhu. Ve spolupráci se sociálními pracovníky neziskových i veřejnoprávních institucí zajišťujeme pomoc pro potřebné ze Sociálního šatníku a skladu nábytku a ze skladu Potravinové pomoci. V samotných Holicích byla nedávno také zprovozněna Paliativní ambulance určená pacientům s pokročilým vážným onemocněním. Služby ambulance jsou terénní, poskytované v domácnosti pacienta, od března bude možné také ambulantní vyšetření přímo na středisku.

Všechny naše kurzy, programy a služby jsou velkým dílem zajišťovány i dobrovolnickou činností. Nabízíme tedy nejen důležité aktivity pro děti, maminky, seniory i celé rodiny, ale můžeme nabídnout i zajímavou práci mladým, anebo těm, kterým stojí za to pomáhat lidem kolem sebe. ■

English Annotation

Michal Štička: Risk Management before and after the Pandemic: from the Repeated to the Continuous Management?

The author deals in his article with risks and risk management during the pandemic. He goes back in time before the beginning of the pandemic and the risk management at that time. The author emphasises the need of continuous risk assessment and creation of the conditions for this action.

Filip Zelingr, Pavel Javůrek: Active Fraud Prevention vs. Bare Improvisation on the Background of Current Changes

The authors in their article discuss the attitude to risk prevention and detection. They analyse the traditional approaches and approaches based on improvisation.

Jan Bukovský: Cybersecurity Risk Prevention

The author shows the list of basic cybersecurity risk including risk mitigation and concrete example.

Michal Merta: Why and How the Hacker Attacks?

The author describes form the general point of view the motivation and approach of the hacking attacks.

Kateřina Schovánková Nejedlá, Martin Dohnal: Fraud alias Auditor´s Nightmare

The authors describe how the internal auditor should behave if he/she faces the potential fraud in the company.

Radek Ščotka: Always Ready?

The author discusses generally how tho prepare for the crisis situations in the relation to current pandemic.

Šárka Nováková: We Are Ready to Protect Ourselves against the Threats in One of the Biggest Hospitals in the Czech Republic

The Chief Audit Executive Ing. Šárka Nováková, MBA shares her experiences from one of the biggest hospitals in the Czech Republic. The article is focused on description how the hospital systematically faces the threats.

Martin Kubš, Milan Puszkailer: Fraud, Fradulent Behavior, Audit Findings – Lessons Learnt, Curiosities...

The task of the Audit Body of the Ministry of Finance of the Czech Republic in the current period 2014–2020 is among others fraud risk assessment, fraud prevention and detection.

Ondřej Novák: Frauds in the Area of Harming the Interests of the European Union

The frauds I would like to describe are frauds where the intersests of the European Union were harmed during the implementation of projects co-financed from the European funds in the Czech Republic and where the actors were convicted.

Zdeňka Liv Prokšová: Fulfillment of the notification obligation in relation to breaches of budgetary discipline and criminal liability

The article deals with the cooperation of the Supreme Audit Office with the tax administrator and law enforcement authority, notification obligation which closely relates with this obligation, especially in relation to the breach of the budgetary discipline or the criminal liability.

Tereza Pavlíčková: Smart Quarantine and eRouška from the Perspective of GDPR

DPO of the Ministry of Health describes the project of Smart Quarantine with the focus on one of its tools – mobile application eRouška a its impact on the area of personal data protection.

Jiří Dvořáček, Josef Tyll: Will the Internal Audit Survive the Current Pandemic?

The Auditors ask the question, if the internal audit will survive the current pandemic. They assess, how the pandemic manifests, what is its impact on the internal audit activity and what lessons learnt and challenges it provides for the present and future.

Setkali jste se s podvodným jednáním obchodníků s energií?

Můžete se obrátit na naši bezplatnou zákaznickou linku

800 810 820

nebo zanechte svůj kontakt ve formuláři na speciální webové stránce **www.cez.cz/nedejtese**.

JSME S VÁMI. SKUPINA ČEZ