Celosvětový průzkum hospodářské kriminality 2016

Zpráva za Českou republiku

www.pwc.com/cz

35%
společností prodělalo jeden nebo více případů hospodářské kriminality

36%
případů tvořila počítačová kriminalita

pwc

Obsah

Celosvětový průzkum hospodářské kriminality, který provádí společnost PwC, je největším průzkumem svého druhu na světě. V roce 2016 se jej zúčastnilo 6 337 respondentů ze 115 zemí, včetně 79 společností z České republiky.
Cílem průzkumu byla nejen analýza současného stavu hospodářské kriminality, ale také identifikace trendů a změn ve vnímání budoucích rizik.

Úvod

S potěšením Vám představuji výsledky Celosvětového průzkumu hospodářské kriminality 2016, který provedla poradenská společnost PwC. Jde o největší průzkum svého druhu na světě. Abychom získali co nejkomplexnější pohled na současný stav hospodářské kriminality, jejího vnímání a povědomí organizací o ní, shromáždili jsme odpovědi od 6337 organizací ze 115 zemí, včetně 79 významných společností z České republiky.

Letošní průzkum znovu upozorňuje na hrozbu počítačové kriminality, která začala být teprve před několika lety považována za zcela novou formu rizika. Nicméně, v poslední době se stala hlavním tématem každé diskuse týkající se podvodných jednání. Žádná firma není imunní - počítačová kriminalita ovlivňuje firmy bez ohledu na odvětví, ve kterém působí, či zemi, ve které sídlí. Kromě počítačové kriminality se tento průzkum zaměřuje také na oblast etiky a compliance. Dodržování právních a etických norem v podnikatelském prostředí, které se stále více globalizuje, je mnohem náročnější a stává se pro společnosti klíčovou otázkou.

Náš průzkum se zabývá také otázkou „příležitostí“. Nejde jen o příležitosti, které umožňují podvody páchat, ale hlavně o příležitosti, které mohou společnosti využít ve svůj prospěch při aktivním boji proti hospodářské kriminalitě, a které přitom nejsou nadměrnou zátěží pro jejich právní odpovědnost.

Budu velmi rád, pokud se seznámíte s výsledky našeho průzkumu a vyvodíte z nich závěry relevantní pro své podnikání. Společnostem, které působí na mezinárodní úrovni, poskytujeme jak celosvětové výsledky, tak i výstupy zaměřené na konkrétní země. Jsem přesvědčen, že vám naše analýzy umožní lépe pochopit, jak významný dopad může hospodářská kriminalita mít na vaše podnikání, pomůže posoudit riziko podvodu, kterému mohou čelit, a najít způsoby ke zmírnění těchto rizik.

Na závěr bych chtěl poděkovat účastníkům průzkumu, kteří byli tak laskavi a podělili se s námi o své zkušenosti s podvody. Zvláštní poděkování patří respondentům z České republiky. Jsem rád, že všichni z nich sdílí naše přesvědčení, že hospodářská kriminalita je příliš nákladná na to, abychom ji ignorovali.

Sirshar Qureshi,
Partner zodpovědný za Forenzní služby ve střední a východní Evropě, PwC

Hlavní zjištění

Současný stav hospodářské kriminality v České republice

Hospodářská kriminalita i nadále představuje závažný problém ovlivňující společnosti po celém světě, v zemích střední a východní Evropy i v České republice. Za posledních 24 měsíců se s jedním nebo více případy hospodářské kriminality setkala více než třetina (35 %) respondentů z České republiky, což je srovnatelné s průměrným výskytem ve střední a východní Evropě (33 %) i celosvětově (36 %).

Ve srovnání s předchozím průzkumem poklesl výskyt hospodářské kriminality o 13 procentních bodů. Při vyvozování závěrů bychom nicméně neměli být příliš optimističtí. V kontextu vývoje aktuálních rizik, mohou firmy čelit sofistikovaným podvodům, které mohou bez povšimnutí probíhat několik let. Tyto skryté a dlouho trvající podvody jsou pro společnosti větším nebezpečím, než jednorázové incidenty. Jsou obvykle také spojeny s vyššími náklady.

Jako již tradičně, nejčastějším typem hospodářské kriminality v České republice zůstává zpronevěra majetku (61 %). Majetková zpronevěra je obecně vnímána jako podvod, který je ve srovnání s jinými typy hospodářské kriminality jednodušší odhalit. Proto je její pravidelný výskyt na čele žebříčku podvodů předvídatelný.

Podle našeho průzkumu jsou dalšími čtyřmi nejčastějšími typy podvodů počítačová kriminalita (36 %), podvody v nákupním procesu (25 %), podplácení a korupce (21 %) a účetní podvody (21 %).

Většina podvodů v České republice je odhalena pomocí firemních kontrol (celkem 68 %). Nicméně stále téměř každý pátý případ podvodu je odhalen způsobem, na který nemá management společnosti žádný vliv, nejčastěji naprostou náhodou (14 %).

Podle průzkumu z roku 2016 počet podvodů spáchaných externím pachatelem (54 %) mírně převažuje nad podvody spáchanými interním pachatelem.

Za posledních 24 měsíců se s jedním nebo více případy hospodářské kriminality setkalo 35% společností z České republiky.

Počítačová kriminalita

Více než třetina respondentů v České republice, kteří se setkali s podvodem, zmínila v této souvislosti počítačovou kriminalitu. Což dokonce mírně převyšuje výsledky za střední a východní Evropu i celosvětový průměr. V případě, že bychom z tohoto průzkumu měli vybrat jen jeden klíčový poznatek, měla by to být změna vnímání počítačové kriminality. Již není považována za „pouhý" IT problémem, chápou ji jako zásadní hrozbu, která má dopad na podnikání a provoz firmy jako celku.

Podle výsledků našeho předchozího průzkumu, má výskyt počítačová kriminality rostoucí trend. Počet účastníků průzkumu, kteří se s ní setkali, se zvýšil mezi roky 2011 a 2016 z 13 % respondentů na 36 %. V měnícím se podnikatelském prostředí, kde drtivá většina dokumentů, komunikace a transakcí probíhá digitální formou, to však není žádným překvapením.

Účastníci průzkumu z České republiky považují počítačovou kriminalitu za největší hrozbu. Více než jedna třetina z nich očekává, že budou ohroženi počítačovým podvodem v příštích 24 měsících . Kromě toho si 57 % dotázaných myslí, že se riziko počítačové kriminality zvýšilo.

Díky rychlým technologickým změnám se tradiční vnímání počítačové kriminality rozšířilo. K systémům, které jsou ohrožené počítačovou kriminalitou, patří v současné době nejen počítače, ale také mobilní zařízení, zařízení připojená ke cloudu, a dokonce i automobily a zařízení v domácnosti připojená k internetu.

Z finančního hlediska je počítačová kriminalita velmi nákladná. Vice jak čtvrtina firem z celého světa uvedla, že za poslední dva roky utrpěla v jejím důsledku ztrátu přesahující 1 200 000 Kč.

36% respondentů z České republiky, kteří prodělali hospodářskou kriminalitu, uvedli, že se setkali s počítačovou kriminalitou.

Etika a compliance

V našem průzkumu se podplácení a korupce umístily na pomyslném čtvrtém místě žebříčku nejčastějších typů hospodářské kriminality v České republice.

Pozitivní zprávou je, že více než 86 % účastníků průzkumu má ve společnosti formálně nastavený etický a compliance program, což je lehce nad průměrem za střední a východní Evropu i celý svět (obojí shodně 82 %).

Celkem 80 % respondentů je přesvědčeno, že jejich etický kodex pokrývá klíčová rizika/oblasti a stanovuje hodnoty jejich firmy. Podle 79 % respondentů jsou firemní hodnoty jasně vymezeny a zaměstnanci jim rozumí. Více než polovina (55 %) společností pravidelně školí své zaměstnance v oblasti etického kodexu a podpůrných směrnic.

Tato relativně vysoká čísla naznačují, že české společnosti mají zavedený přiměřený etický kodex. Klíčovým faktorem účinného fungování compliance program je však to, zda zaměstnanci rozumí etickým principům firmy. Pravidelná školení zaměstnanců proto doporučujeme všem společnostem.

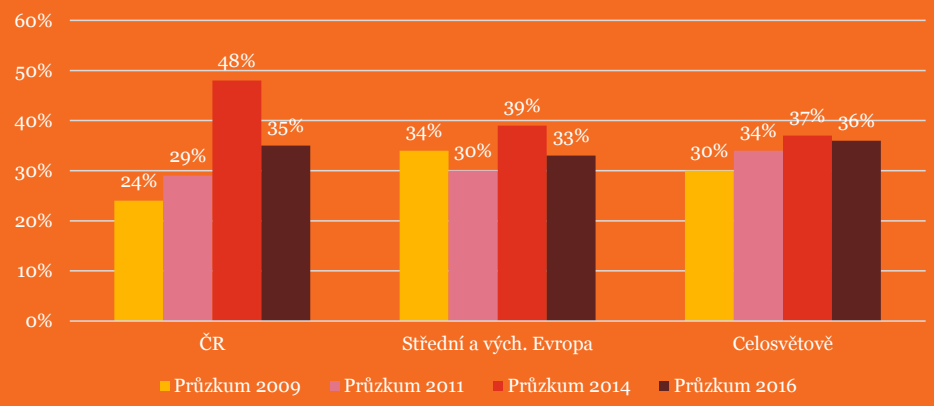
V posledních 24 měsících bylo 6% společností požádáno o zaplacení úplatku.

Hospodářská kriminalita v České republice

Hospodářská kriminalita je stálou hrozbou
Kolik společností se setkalo s podvodem během posledních dvou let?

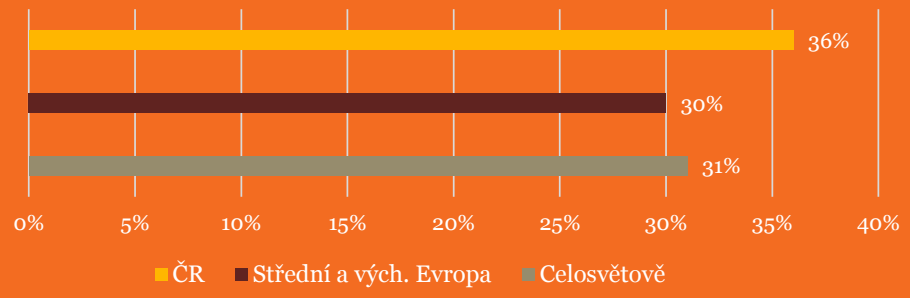
Hospodářská kriminalita je důvodem obav společností všech velikostí, průmyslových odvětví i různých vlastnických struktur. Za uplynulé dva roky se více než třetina (35 %) respondentů z České republiky setkala s hospodářskou kriminalitou. Ve srovnání se střední a východní Evropou (33 %) je výskyt hospodářské kriminality v České republice častější. Jediným pozitivem na tomto výsledku je pokles v porovnání s výsledky z předchozího průzkumu z roku 2014. I přesto má výskyt hospodářské kriminality od roku 2009 stále rostoucí tendenci.

Výskyt hospodářské kriminality



Více než třetina (36 %) firem, které se setkaly s hospodářskou kriminalitou, řešila za poslední dva roky více než deset případů. Tento výsledek překračuje průměr střední a východní Evropu (30 %) i celosvětový průměr (31 %). Z toho je možné vyvodit, že pokud se česká firma stane obětí podvodu, je pravděpodobné, že nepůjde ojedinělý případ a může se opakovat.

Více než 10 incidentů hospodářské kriminality za posledních 24 měsíců



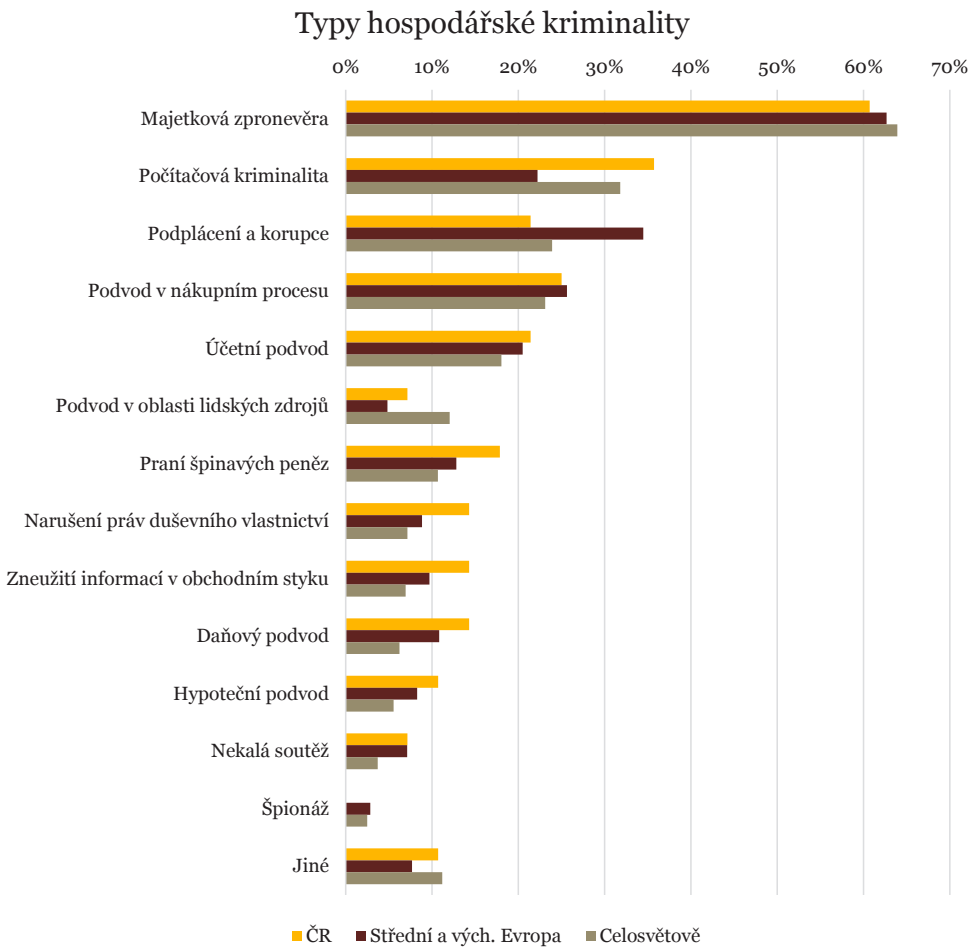
Jakým typům hospodářské kriminality české společnosti čelí?

Výskyt většiny typů hospodářské kriminality (s výjimkou počítačové kriminality a účetních podvodů) se ve srovnání s výsledky z předchozího průzkumu snížil.

Mezi nejčastější typy hospodářské kriminality patří zpronevěra majetku (zaznamenalo 61 % dotázaných, kteří se střetly s hospodářskou kriminalitou), dále stále četnější počítačová kriminalita (36 %), podvody v nákupním procesu (25 %), podplácení a korupce a v neposlední řadě účetní podvody (obojí 21 %).

61%

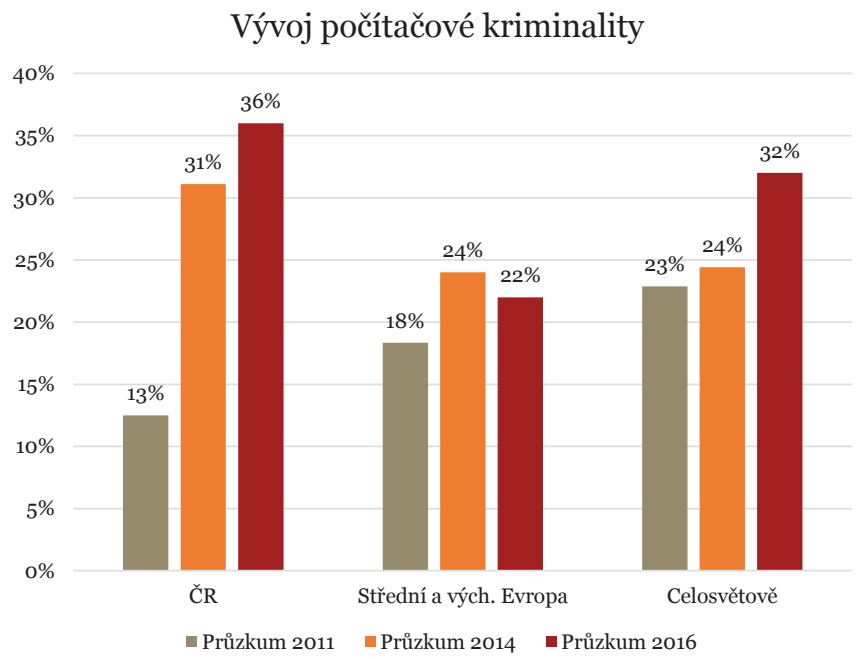
Majetková zpronevěra je na prvním místě žebříčku v každém našem průzkumu. Vzhledem k tomu, že je považována za nejjednodušeji odhalitelný podvod, je její umístění v čele žebříčku předvídatelné.



Obecně řečeno, výsledky za Českou republiku jsou víceméně totožné s výskytem hospodářské kriminality v regionu střední a východní Evropy i celosvětově. Přesto dotazované firmy z České republiky uvedly větší výskyt počítačové kriminality než je průměr ve střední a východní Evropě i celosvětově. Naopak podplácení a korupce se zdá být větším problémem ve střední a východní Evropě než v České republice.

Počítačová kriminalita

Výskyt počítačová kriminality vykazuje od roku 2011, kdy byla nově zařazena do našeho průzkumu, rostoucí trend, a to jak globálně, tak regionálně. V České republice (36 %) je dokonce ještě vyšší než ve střední a východní Evropě (22 %) i celosvětově (32 %). Ze všech typů hospodářské kriminality je ta počítačová vnímána respondenty z České republiky také jako největší hrozba.

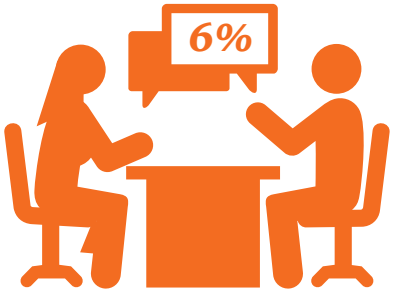


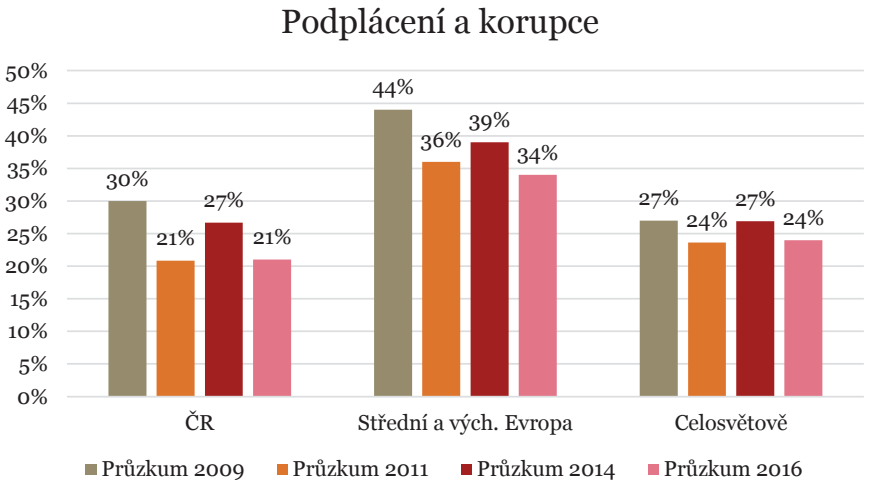
Podplácení a korupce

Navzdory poklesu míry korupce a podplácení v České republice z 27 % na 21 %, a stejně tak ve střední a východní Evropě i celosvětově, patří tento typ hospodářské kriminality od roku 2009 mezi nejzávažnější. Podle Českého průzkumu názorů generálních ředitelů 2016 vnímají téměř tři čtvrtiny českých firem podplácení a korupci jako hrozbu pro své podnikání.

Dotazované společnosti také uvedly, že v posledních 24 měsících byly požádány o zaplacení úplatku (6 % v ČR) nebo, že ztratily příležitost oproti konkurenci, která úplatek zaplatila (12 % v ČR). Letošních výsledek (6 %) pak představuje pokles o více než polovinu ve srovnání s výsledky předchozího průzkumu z roku 2014 (16 %).

Tento klesající trend se zdá být optimistický. Měli bychom však být opatrní při vyvozování závěrů. Realita může být mnohem horší. Na základě našich zkušeností je podplácení a korupce typem podvodu, který je poměrně obtížné odhalit. Navíc vnímání toho, co je již podplácení a korupce, může být subjektivní napříč trhem. Chování, které některé společnosti vnímají jako součást obvyklé obchodní praxe, jiné považují za podplácení a korupci.





Dopady hospodářské kriminality

Když zvážíme finanční ztráty v důsledku hospodářské kriminality, průzkum ukazuje, že 40 % českých firem, které se setkaly s hospodářskou kriminalitou, přišlo nejméně o 1 200 000 Kč.

Naši respondenti shodně uvádějí mnohem širší škody než jen přímé finanční dopady podvodu. Jedná se například o škody vyplývající z přerušení provozu, náklady na nápravná opatření, vyšetřování a preventivních kroky, pokuty od regulátorů nebo vyplacené honoráře za právní řešení daného problému. Kritický je ale hlavně negativní dopad na morálku zaměstnanců a ztráta dobré pověsti společnosti, které mají významný vliv na její dlouhodobou výkonnost. Tyto druhy škod, samozřejmě ne vždy kvantifikovatelné, mohou časem převýšit relativně krátkodobé finanční ztráty z daného podvodu.

Důsledky hospodářské kriminality nespočívají pouze ve finančních ztrátách, ale často bývají mnohem širší. Skutečné náklady hospodářské kriminality je obtížné odhadnout, a to zejména pokud si uvědomíme, že čistě finanční ztráta je často jen malou složkou celkových následků. Ze společností, které utrpěly škodu v důsledku podvodu, 25 % uvedlo jako nejvýznamnější dopad na pověst a sílu značky a 30 % zaznamenalo negativní dopad na morálku zaměstnanců.

Technologie v hospodářské kriminalitě – požehnání nebo prokletí?

Rozhovor

Marek Novotný
Senior manažér, Poradenství

Jaké jsou aktuální trendy v oblasti počítačových podvodů?
V současné době celý svět funguje prostřednictvím informačních a komunikačních technologií. Komplexnost řešení, množství dat a výkon hardwaru se každoročně zvyšuje. Stejným tempem se vyvíjí i počítačové podvody. Například díky snížení cen výpočetní techniky, jsou v současnosti běžné přístupy, které dříve nebyly možné. Proto se objevují složitější scénáře podvodů. Je důležité si uvědomit, že pachatelé podvodů mohou používat úplně stejné technologie jako vy a v mnoha případech je ovládají lépe než vy. Je docela běžné, že používají pokročilé analytické nástroje, jako jsou algoritmy strojového učení například pro simulaci chování běžného zákazníka.

Co jsou nejčastější cíle kybernetických útočníků?
Nejvíce počítačových podvodů souvisí s krádeží peněz. Nejkritičtější oblastí jsou služby spojené s jejich převody. Způsob, jakým je jejich krádež provedena, se liší podle typu podnikatelské činnosti. Může jít o manko ve skladu prostřednictvím manipulace se skladovou evidencí, změny bankovních účtů v dodavatelských nebo zaměstnaneckých kmenových datech podnikových systémů, vrstvení transakcí (layering), krádeže identit za účelem získání přístupu k bankovním účtům atd. Druhou klíčovou oblastí je průmyslová špionáž a poškození pověsti firmy prostřednictvím specializovaných skupin najatých konkurencí. Firemní špionáž se v dnešní době do značné míry opírá o tzv. kybernetickou inteligenci.

Které technologie jsou v současnosti nejčastěji používány při počítačových podvodech?
Počítačoví podvodníci mohou využívat jakoukoliv technologii, která je v současnosti dostupná. Otázkou je jen záměr pachatele. Může jít o široké spektrum možností a technologií od speciální fráze ve veřejných vyhledávačích až po vysoce sofistikované hackerské techniky, které obvykle zahrnují i prvky sociálního inženýrství. Důležitým faktem je, rostoucí množství technologií, komplexnost a množství funkcí dostupných v zařízeních, jež se rok od roku zvyšuje. Proto se počítačový podvod netýká pouze počítačů. Téměř každý má dnes chytrý telefon s přístupem k internetovému bankovnictví. Podobně přenosné technologie, jako chytré hodinky nebo fitness náramky, umožňují komunikaci s jinými zařízeními. Operační systémy jsou součástí televizorů a domácích kin. Jsou dokonce v herních konzolích nebo autech. Stále více se blíží doba inteligentních domácností a v nich množství přístrojů, které mohou být použity k počítačovému podvodu a trestné činnosti, se zvyšuje.

Co dělat, když se něco takového přihodí v mé firmě?
To záleží na vyspělosti interních postupů, kontrol, systémů a celkové připravenosti podniku na takovou událost. Na základě našich zkušeností zanechává každý podvod specifickou stopu, která může být odhalena v podnikových datech bez ohledu na to, zda se jedná o opakující se podvod nebo ojedinělý incident. Jsme schopni analyzovat jak strukturovaná i nestrukturovaná data, najít specifické stopy podvodů a vyšetřit je. Pomáháme klientům s prevencí, poskytujeme jim plnou podporu během řešení nepříjemných incidentů i při následných navazujících krocích.

Je možné dělat něco lépe tak, abychom se vyhnuli počítačovým podvodům nebo na ně byli alespoň připraveni?
Většina podvodů vzniká už při chybném nastavení procesů, nedostatečnou disciplínou uživatelů a ignorováním rizik. Nutností je pravidelné používání informačních systémů a dodržování interních a externích směrnic a postupů. Pokud ve vaší firmě funguje systém pravidelného hodnocení rizik, měli byste být schopni odhalit slabá místa a soustředit se na ně. U mezinárodních společností je dokonce patrné, jak se rizika a hrozby přesouvají z kontinentu na kontinent a z jedné země do další. Díky tomu byste měli být schopni reagovat dříve, než k podvodu dojde i u vás. Navíc můžete zavést pokročilé systémy, které dokáží rozeznat vzory chování v datech, odhalit podezřelé aktivity a předpovídat podvody. Tyto systémy jsou schopny využít a zpracovat veškerá data z vašich podnikových systémů a zlepšit úroveň vaší obrany a připravenosti na počítačový podvod.

Počítačová kriminalita ohrožuje všechny aspekty podnikání

Není žádným překvapením, že v současném digitálním prostředí má výskyt počítačové kriminality rostoucí tendenci. Od roku 2011, kdy byla počítačová kriminalita v našem průzkumu poprvé uvedena jako samostatná kategorie podvodu, její četnost vzrostla téměř třikrát (13 % společností, které se setkaly s hospodářskou kriminalitou, v roce 2011 ve srovnání s 36 % společností v roce 2016). Kromě toho dalších 28 % respondentů z České republiky uvedlo, že byli nějakým způsobem ohroženi počítačovou kriminalitou.

Tento výsledek je mírně nad průměrem za střední a východní Evropu (22 %) i celý svět (26 %). Nárůst případů počítačové kriminality je také podporován vnímáním s ní souvisejících rizik. Více než polovina českých firem (57 %) se domnívá, že se riziko počítačové kriminality zvýšilo a podle Českého průzkumu názorů generálních ředitelů 2016 téměř polovina českých společností vnímá jako hrozbu i tempo, kterým se technologie vyvíjí.

Vnímání vzrůstu rizika počítačové kriminality

57%
Česká republika

44%
Střední a východní Evropa

53%
Svět

Poškození dobrého jména společnosti, krádež, ztráta osobních údajů nebo přerušení provozu společnosti jsou celosvětově nejobávanější důsledky počítačové kriminality. Počítačová kriminalita je také finančně nákladná. Čtvrtina dotázaných firem z celého světa utrpěla v jejím důsledku za poslední dva roky ztrátu převyšující 1 200 000 Kč.

Průzkum také ukázal, že 46 % českých firem vidí největší hrozbu v počítačové kriminalitě páchané externími pachateli, 33 % z nich si myslí, že hrozba může pocházet jak od interních, tak i externích pachatelů, a pouze 9 % věří, že hrozba pochází pouze od interních pachatelů. Zbytek respondentů nemá na původce počítačové kriminality jednoznačný názor. Podobně je hrozba počítačové kriminality vnímána jak ve střední a východní Evropě, tak celosvětově.

Členové představenstva téměř poloviny firem v České republice nevyžadují interní hodnocení týkající se připravenosti jejich firmy vypořádat se s počítačovou kriminalitou.

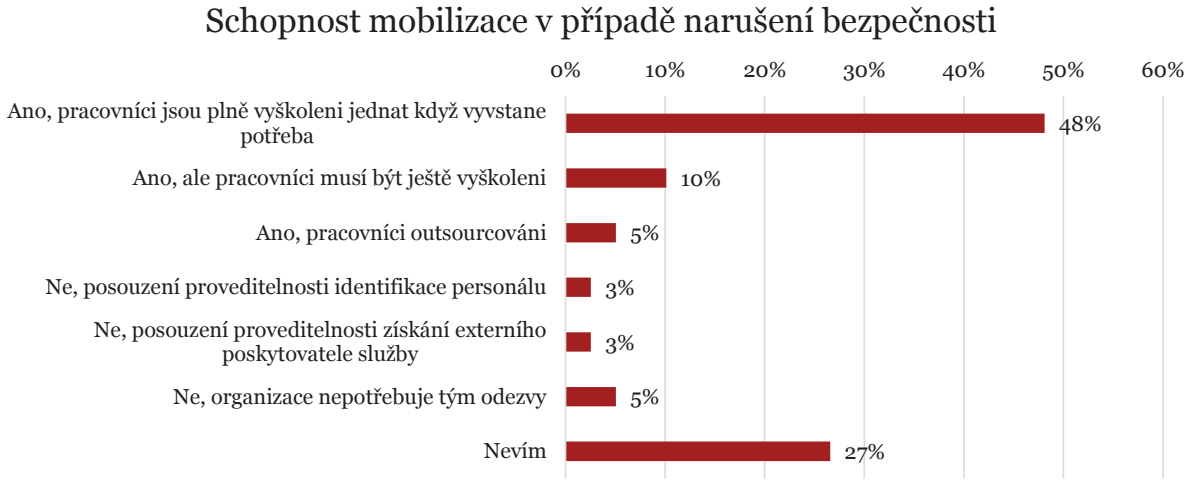
17% **společností dokonce nepřipravuje žádné takové interní hodnocení a**

28% **ani o požadavku na jejich přípravu neví.**

V souvislosti s rostoucím výskytem počítačové kriminality je skutečnost, že téměř polovina společností nemá informace o své připravenosti čelit těmto incidentům, alarmující.

Obdobné je to s plánem reakce na vypořádání se s počítačovými útoky. Pouze 33 % dotazovaných má tento plán plně funkční.

Téměř polovina firem v České republice (48 %) má plně vyškolený tým odezvy, který je schopen v případě potřeby zasáhnout a vypořádat se s narušením IT prostředí. Toto číslo by se mohlo zdát poměrně vysoké. S ohledem na neustále se měnící digitální prostředí a skutečnost, že žádná společnost není imunní vůči těmto útokům, mají však společnosti stále co zlepšovat, aby zmírnily riziko negativního dopadu případných útoků.



Společnosti, které se umí rychle vypořádat s narušením IT prostředí, mají svůj tým odezvy obvykle složený z pracovníků s dobrou znalostí IT prostředí své firmy (78 %), specialistů na IT bezpečnost (64 %), členů vrcholového vedení (56 %) a právníků (26 %). Naproti tomu podle respondentů z České republiky pouze jeden z dvaceti týmů odezvy zahrnuje forenzní vyšetřovatele specializované na digitální technologie. Celosvětový průměr je přitom jeden z deseti.

Složení týmu odezvy

Neadekvátní složení týmu a pochopitelná snaha o rychlé vyřešení problému může vést k vyššímu riziku přehlédnutí některých potenciálně zásadních důkazů. To může omezit schopnost společnosti správně vyhodnotit všechny dopady narušení, možnost stíhat pachatele a hlavně schopnost pochopit, jak k danému narušení došlo.

Aktivity a úsilí týmu odezvy by měly být vždy koordinovány a odezva by měla být sladěna s cíli vyšetřování.

Detekční metody

Pozitivním zjištěním našeho průzkumu je to, že stále větší množství podvodů je odhalováno pomocí systémových mechanismů (54 % v roce 2011, 61 % v roce 2014 ve srovnání s 68 % v roce 2016). Celkem 68 % českých respondentů také uvedlo, že podvod byl odhalen zavedenými firemními kontrolami (ve srovnání s 54 % ve střední a východní Evropě a 47 % celosvětově).

Vedle „tradičních" detekčních metod, jako jsou řízení rizik podvodů (18 %) a interní audit (14 %), bychom chtěli upozornit na rostoucí podíl datové analýzy (zvýšení z 5 % v roce 2014 na 14 % v roce 2016) a monitorování podezřelých transakcí (zvýšení z 8 % na 14 %). V měnícím se podnikatelském prostředí, kdy různé podvodné aktivity zanechávají v datech specifické stopy, mohou být tyto automatizované detekční mechanismy velmi účinným nástrojem. Navíc, pokud jsou tyto nástroje plně zautomatizované, mohou probíhat v reálném čase bez nebo s velmi omezeným lidským zásahem.

Společnosti by však neměly usnout na vavřínech. Podle respondentů z České republiky bylo stále ještě 18 % podvodů odhaleno způsobem, na který neměl management žádný vliv, nejčastěji naprostou náhodou (14 %). Z výsledků je také vidět evidentní prostor pro zlepšení detekčních metod, které mohou být klasifikovány jako „firemní kultura". Ve srovnání s předchozím průzkumem jsme zjistili, že žádný podvod nebyl hlášen přes anonymní informační linku nebo interním varováním (ve srovnání s 18 % v roce 2014) . A to navzdory skutečnosti, že téměř polovina společností monitoruje podněty z anonymní informační linky.

Tento výsledek může naznačovat, že počet upozornění přijatých přes tento kanál nemusí být pravdivý, nebo že anonymní informační linka prostě nefunguje efektivně. Efektivní anonymní informační systém je nejen výkonným nástrojem v boji s hospodářskou kriminalitou, ale je také součástí zdravého a etického podnikatelského prostředí.

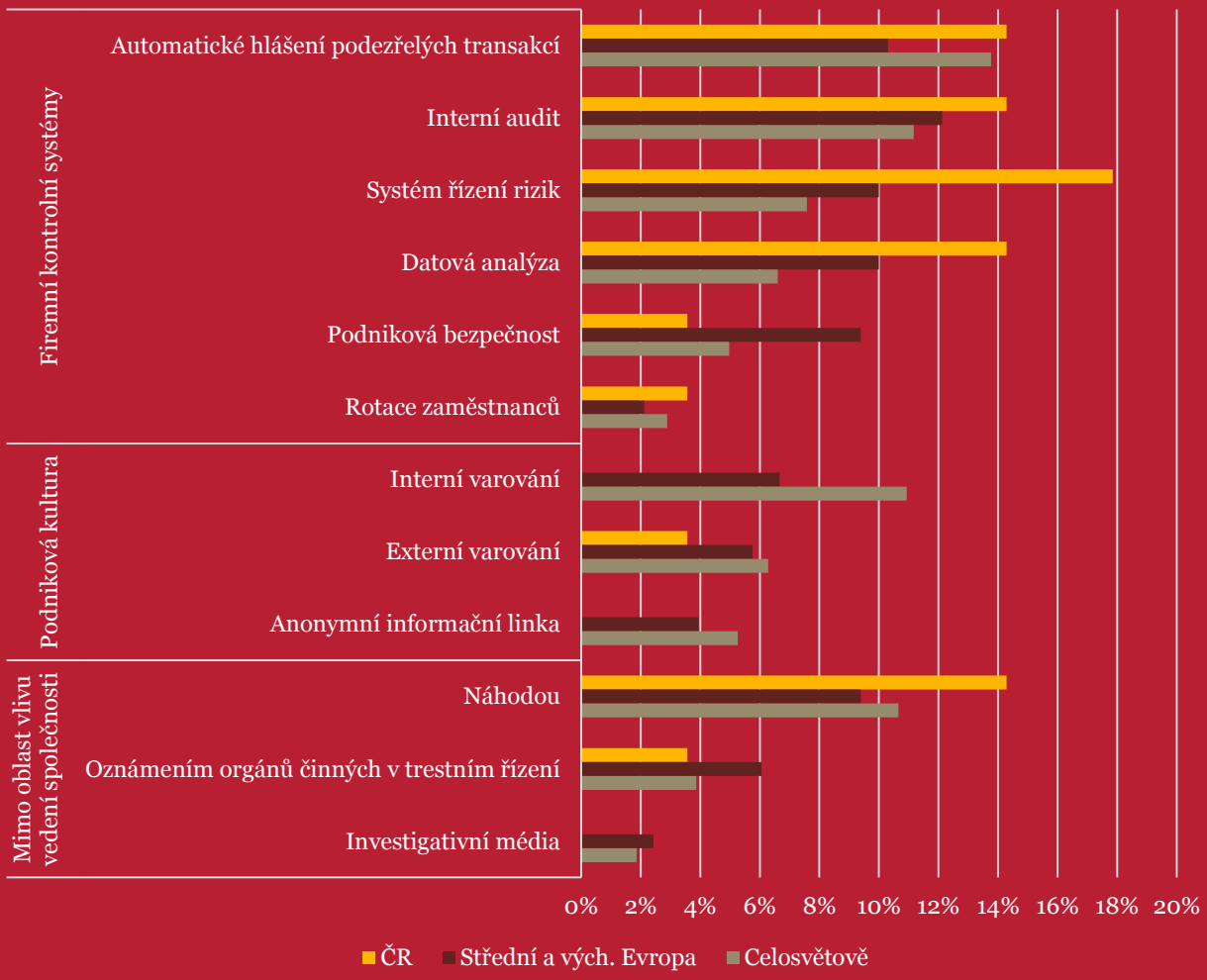
Znaky efektivně fungující anonymní informační linky

- Nedílná součást etického a compliance programu
- Několik komunikačních kanálů (například zvláštní telefonní linka, e-mailová schránka, kontaktní místo), aby byl mechanismus přístupný a snadno použitelný pro všechny zaměstnance a informátory i z prostředí mimo firmu
- Anonymita a důvěrnost
- Ochrana oznamovatelů před odvetou
- Komunikace a vzdělávání
- Pozitivní přístup vedení
- Analýza podnětů získaných prostřednictvím tohoto kanálu a vytváření statistik
- Zveřejnění vyřešených podnětů
- Možnost externího poskytovatele

Analýza podnětů z anonymní informační linky může narazit na několik problémů. Při vyšetřování zpráv je třeba rozlišit, zda byl podnět pravdivý, nebo falešný. Avšak šetření falešných podnětů zatěžuje vyšetřovatele a odpoutává pozornost od „skutečných“ případů.

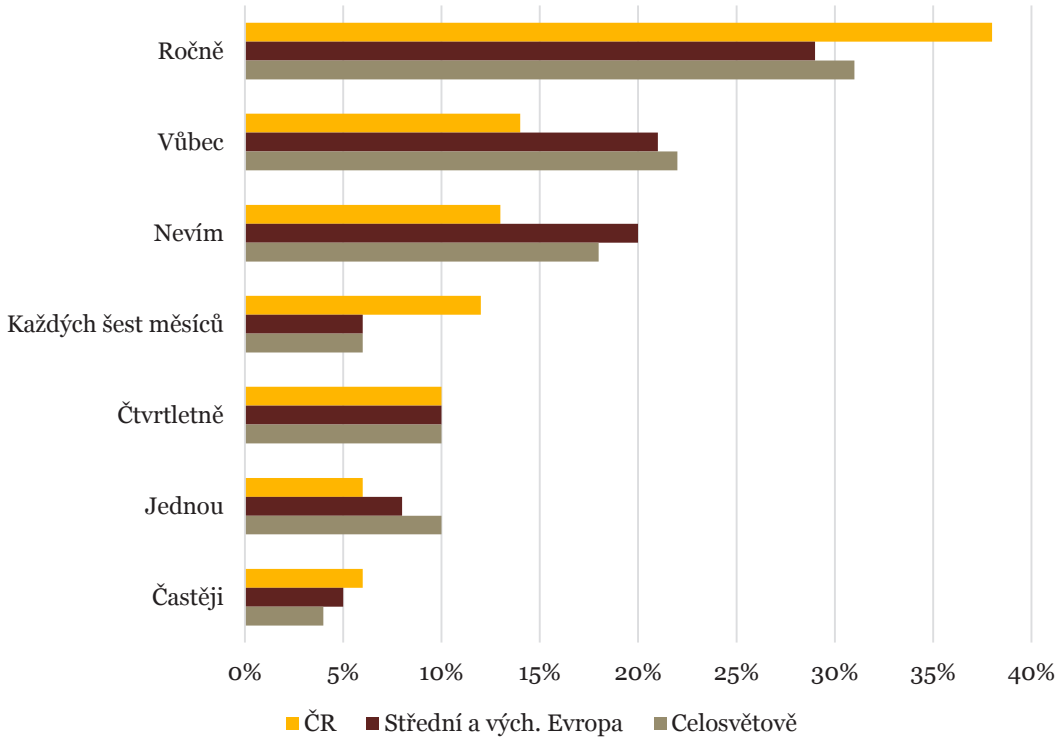
Aby předešly zneužívání tohoto důležitého detekčního nástroje, měly by společnosti nastavit takovou firemní kulturu, která bude zavádějící hlášení a předkládání falešných podnětů považovat za porušení základních firemních hodnot.

Odhalení podvodů



České firmy využívají systém řízení rizik pro odhalování podvodů častěji než je průměr pro střední a východní Evropu (10 %) nebo celosvětově (8 %). Tři čtvrtiny dotazovaných českých společností (72 %) mají tento systém zavedený a za poslední dva roky minimálně jednou rizika podvodů přehodnotily. Celosvětově to bylo 61 % firem a ve střední a východní Evropě dokonce pouze 58 % . Tento údaj koresponduje s poměrně vysokým počtem případů, kdy byla hospodářská kriminalita odhalena pomocí firemních kontrol.

Posouzení rizik podovodů bylo provedeno



Pachatelé hospodářské kriminality

Jaký je typický profil podvodníka?

Historicky je podíl interních a externích podvodníků na hospodářské kriminalitě téměř stejný. Letošní průzkum ukazuje, že v České republice mají mírnou převahu externí pachatelé (54 %) nad interními (43 %). U zbytku podvodů, respondenti nevěděli, zda byla společnost napadena zevnitř či zvenku.

Pokud se jedná o externího pachatele, celosvětové výsledky průzkumu ukazují, že se s největší pravděpodobností jedná o zákazníka (25 %). Zákazník se podle průzkumu podílí na hospodářské kriminalitě častěji než zástupci / zprostředkovatelé (17 %), kteří byli na první příčce žebříčku v posledním průzkumu z roku 2014, nebo prodejci (10 %).

A jak se mohou firmy bránit před útoky externích pachatelů? Zásadní je, aby společnost věděla, s kým obchoduje. Před vstupem do obchodního vztahu, ale i během něj by měly využívat „corporate intelligence" a prověrky „due diligence". Tyto postupy pomáhají firmám identifikovat jejich obchodní partnery, ověřit jejich morálku a poctivost. Jakýkoliv negativní záznam z minulosti by měl být varovným signálem. Navíc v současnosti, ve světle mnoha sankcí a rostoucích požadavků regulátorů, se tyto metody transparentnosti stávají čím dál důležitější.

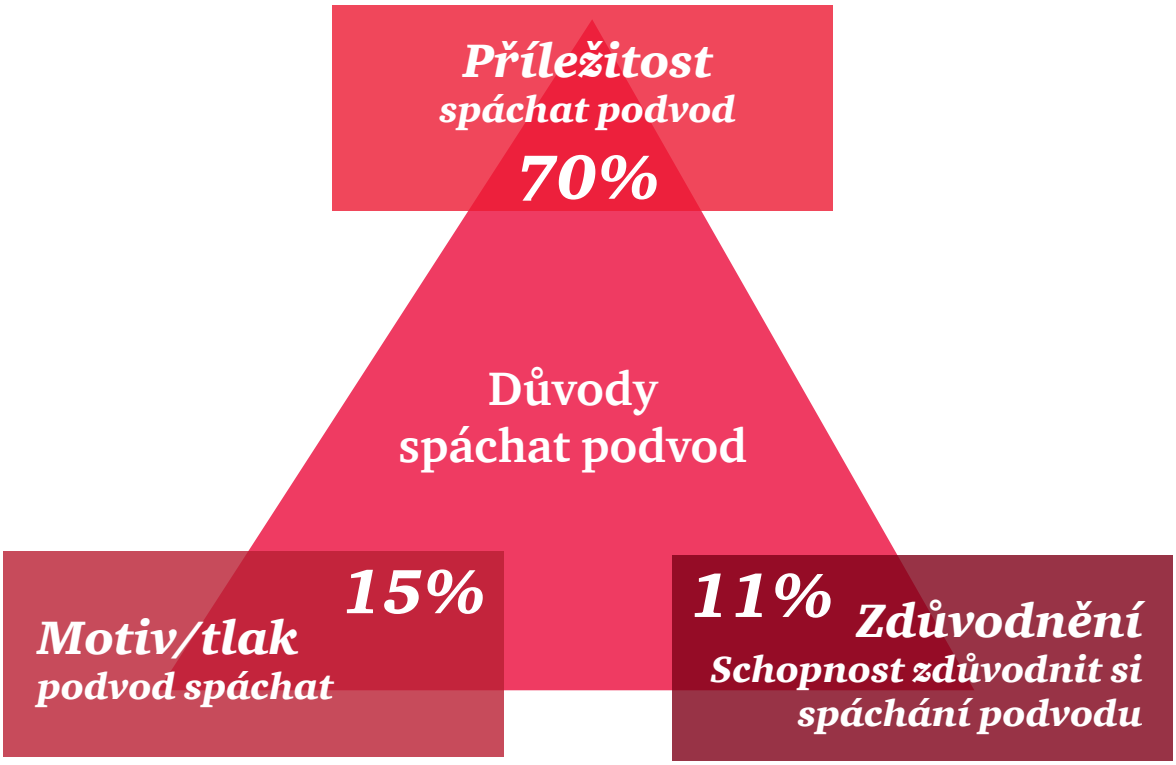
Profil interního podvodníka

Profil externího podvodníka

Co je hnací silou hospodářské kriminality?

Když jsme se zeptali našich respondentů, jaký faktor podle nich nejvíce přispěl k hospodářské kriminalitě spáchané interními subjekty, většina dle očekávání odpověděla, že příležitost (celosvětově 69 %) nebo schopnost podvod spáchat. Proto je nejlepším způsobem, jak předejít podvodu, zamezení vzniku těchto příležitostí posílením kontrol.

Nicméně, pouhá příležitost ke spáchání podvodu nestačí. Pachatel musí mít motiv nebo být pod tlakem, aby podvod spáchal. A také musí být schopen si svůj čin zdůvodnit. Odpovědi na tuto otázku naznačují, že podle společností je příležitost ke spáchání podvodu to nejdůležitější, přičemž zapomínají na význam ostatních dvou faktorů.



Příklady příležitostí:

- Vnitřní kontroly nejsou přizpůsobeny současnému rychle se měnícímu podnikatelskému prostředí a „novým“ typům hrozeb, včetně počítačové kriminality
- Omezená schopnost detekce, nedostatečný počet vyšetřovacích týmů s neodpovídajícími schopnostmi a dovednostmi
- Reaktivní, spíše než proaktivní, přístup
- Firemní kultura, míra tolerance k podvodům, špatný příklad vedení
- Zneužití důvěry

Etika a compliance:
Sladění rizik a odpovědností s hodnotami a strategií společnosti

Interview

Kateřina Halásek Dosedělová
Senior manager, Forenzní služby

Jaké jsou nejčastější regulatorní hrozby, kterým firmy v současnosti čelí?
Regulatorní prostředí, zejména v odvětví finančních služeb, je kvůli novým regulatorním požadavkům čím dál složitější. Korporace tudíž podléhají téměř neustálým změnám, například v oblasti sankcí. V případě, že společnosti nemají správně nastavený program compliance, jsou kvůli zvýšeným rizikům plynoucím z měnícího se prostředí zranitelnější vůči porušení regulatorních požadavků.

Jak se změnila funkce compliance v reakci na vyvíjející se rizika?
V dnešní době můžeme najít pracovníky compliance nejen ve finančních institucích a pobočkách zahraničních společností, ale také v ryze českých a slovenských společnostech nebo u státních organizací. To je opravdu dobré znamení. Bohužel stále existuje řada společností, které považují funkci compliance pouze za dodatečné náklady a zbytečnou zátěž a snaží se ji proto omezit na minimum. Nestačí jen zřídit funkci compliance proto, abychom splnili povinnost. Důležité je, aby měla dostatečné pravomoci a byla rovnocenným partnerem vrcholového vedení, který by jí měl poskytovat plnou podporu. Funkce compliance musí fungovat efektivně. A co přesně si pod tím představit? Reagovat na vyvíjející se rizika pomocí přístupu, který je založený na jejich posouzení, nastavení programu compliance napříč organizací s cílem snížit riziko porušení předpisů a mít vytvořený mechanismus pro podávání a eskalaci hlášení pro případy, kdy je identifikováno nedodržení předpisů.

Jak by měl efektivní compliance program fungovat?
Efektivní compliance program by měl být zaměřený na rizika podvodu v rámci celé společnosti identifikovaná na základě důkladné znalosti jejích slabin. Na jedné straně je potřeba snížit relevantní rizika, na straně druhé umožnit společnosti dosáhnout jejích cílů. Klíčovým předpokladem efektivního programu compliance je adekvátní komunikace napříč společností a její propojení se všemi každodenními činnostmi. Pracovník compliance by měl zajistit, aby byl program praktický a aby mělo oddělení compliance otevřené dveře pro všechny zaměstnance bez ohledu na jejich pozici, aby jim objasňovalo nejasnosti a odpovídalo na případné dotazy. Vy, jako pracovník compliance byste si měl být vědom, že zaměstnanci jsou přetíženi informacemi a v některých odvětvích je jejich fluktuace velmi vysoká. Zvažte proto zahrnutí témat compliance do pravidelné komunikace se zaměstnanci napříč celou firmou, či v relevantních odděleních. Podpora vrcholového vedení je klíčová. Nicméně v komunikaci je nejdůležitější, aby si compliance program vzal za své hlavně střední management. Ten je v každodenním kontaktu se zaměstnanci, a proto je poslem zpráv a vzorem. Pokud zaměstnanci uvidí svého manažera, který žije compliance programem, zapojí se a budou ho následovat.

Na závěr, můžete uvést typické důvody, proč compliance, respektive etické funkce selhávají?
Compliance není pouze o odškrtání seznamu. I přes to, že jde o funkci, která přímo nevytváří zisk, neměla by kvůli tomu mít nižší prioritu. Spíše naopak. I v případě, že vaše společnost musí snížit náklady, včetně nákladů na zaměstnance a školení, nemělo by být oddělení compliance automaticky tím, které se zruší. To by bylo strategicky špatným rozhodnutím. Zatímco se rizika a hrozby neustále mění, podstatou úspěšného compliance programu je jeho schopnost předvídat a odpovídat na změny prostředí. Dalším důvodem může být odcizení oddělení compliance od běžného života společnosti. Mějte na paměti, že vaši zaměstnanci, kteří jsou v kontaktu se zákazníky, stejně jako zaměstnanci z podpůrných oddělení, jsou vaší první linií obrany proti hospodářské kriminalitě. Snažte se je proto zapojit do compliance programu již v přípravné fázi. Pravidelně s nimi komunikujte a dejte jim pocit, že se na vás mohou kdykoliv obrátit se svými obavami nebo dotazy.

Etický a compliance program ve společnosti

Pět kroků k efektivnímu compliance programu

1. **Zajistěte, aby váš program compliance byl v souladu s firemní strategií a jasně o tom informujte zaměstnance.**
2. **Zhodnoťte a případně upravte pozici funkce compliance tak, aby se dokázala přizpůsobit prostředí, ve kterém se rizika a hrozby neustále mění.**
3. **Zajistěte, aby všichni, kteří mají zodpovědnost za program compliance, plně chápali jeho smysl ve firmě a svoji úlohu v něm.**
4. **Nezapomeňte na to, že vnitřní předpisy a školení o hodnotách společnosti nestačí. Je nezbytné soustavné a důsledné zapojení celé firmy.**
5. **Nesnižujte stav zaměstnanců compliance, když rizika rostou.**

Čtyři základní oblasti, na které se zaměřit, aby se zvýšila efektivnost compliance programu

Lidé a kultura
Jasné postupy a principy, kultura, kde je compliance pevně spojena s hodnotami, hodnocení a odměňování žádaného chování.

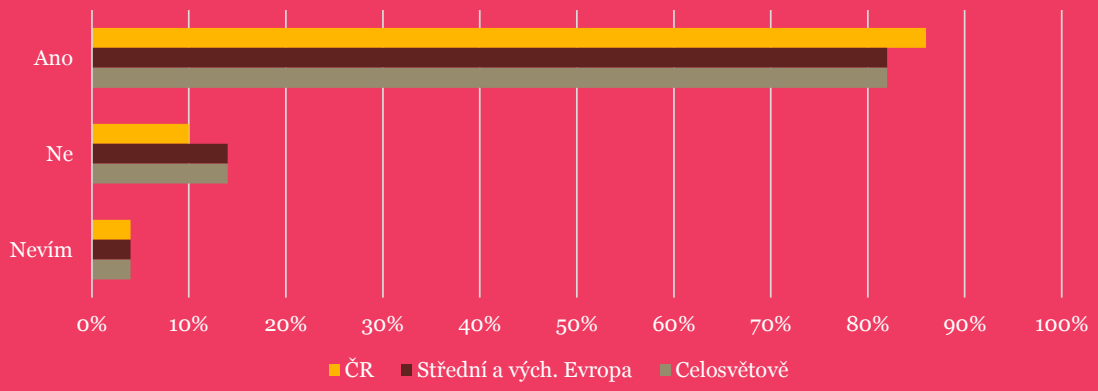
Role a odpovědnost
Formální struktura compliance. Zajištění jejího nastavení s ohledem na aktuální rizika.

Vysoce rizikové oblasti
Lepší implementace a testování na vysoce rizikových trzích a divizí.

Technologie
Lepší využití detekčních a preventivních nástrojů, včetně velkých datových analýz.

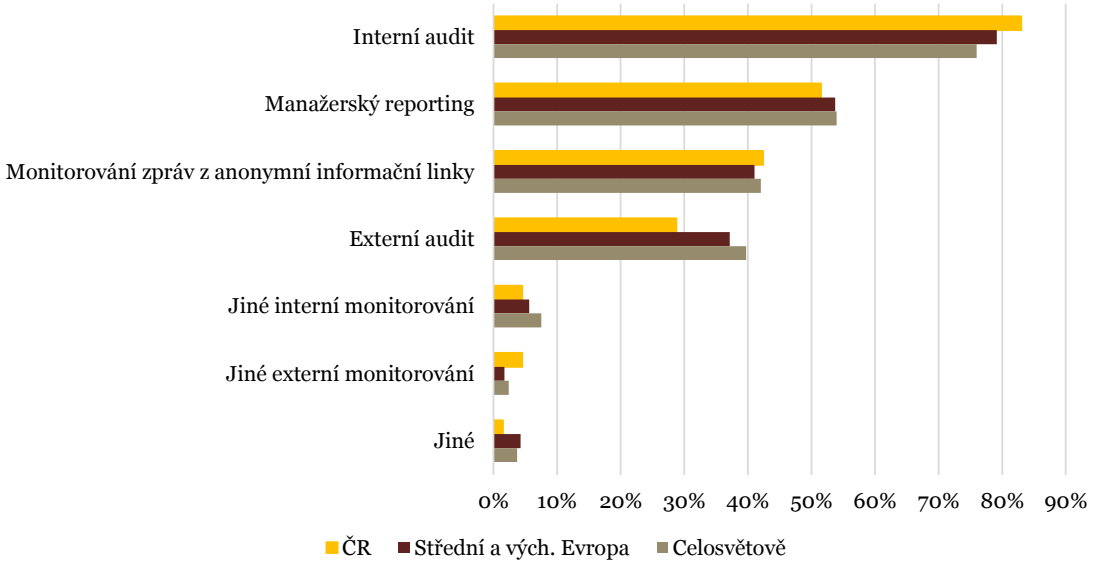
Náš průzkum ukazuje, že 86 % českých firem má formálně nastavený etický a compliance program. I přesto, že je toto číslo poměrně vysoké, stále zde existuje prostor pro zlepšení. Stejně jako ve střední a východní Evropě i celosvětově (oboje 38 %), mají české společnosti nejčastěji pracovníka compliance (46 %), který je zodpovědný za etický a compliance program ve společnosti.

Formální podniková etika a compliance program v organizaci



Aby bylo zajištěno, že compliance a etické programy společnosti jsou účinné, 83 % českých společností má interní audit, 52 % používá manažerský reporting a 42 % monitoruje podněty získané z anonymní informační linky. Podněty se týkají nejen podezření na podvody, ale také upozornění na nedodržování etických a právních požadavků managementem a ostatními zaměstnanci.

Jak zajisťujete, že je váš compliance program a etika podnikání efektivní?



Podíváme-li se blíže na to, jak je etický a compliance program zabudovaný ve firemním prostředí, 79 % dotazovaných společností odpovědělo, že jejich etický kodex pokrývá klíčová rizika/oblasti a stanovuje firemní hodnoty.

Pochopení potřeb zaměstnanců a komunikace napříč celou firmou jsou základními faktory přispívajícími k efektivnímu compliance programu. Výsledky našeho průzkumu jsou v tomto ohledu velmi pozitivní. Podle 79 % respondentů, jsou firemní hodnoty jasně stanoveny a sděleny a 55 % společností pořádá pravidelná školení na etický kodex a podpůrné vnitřní předpisy.

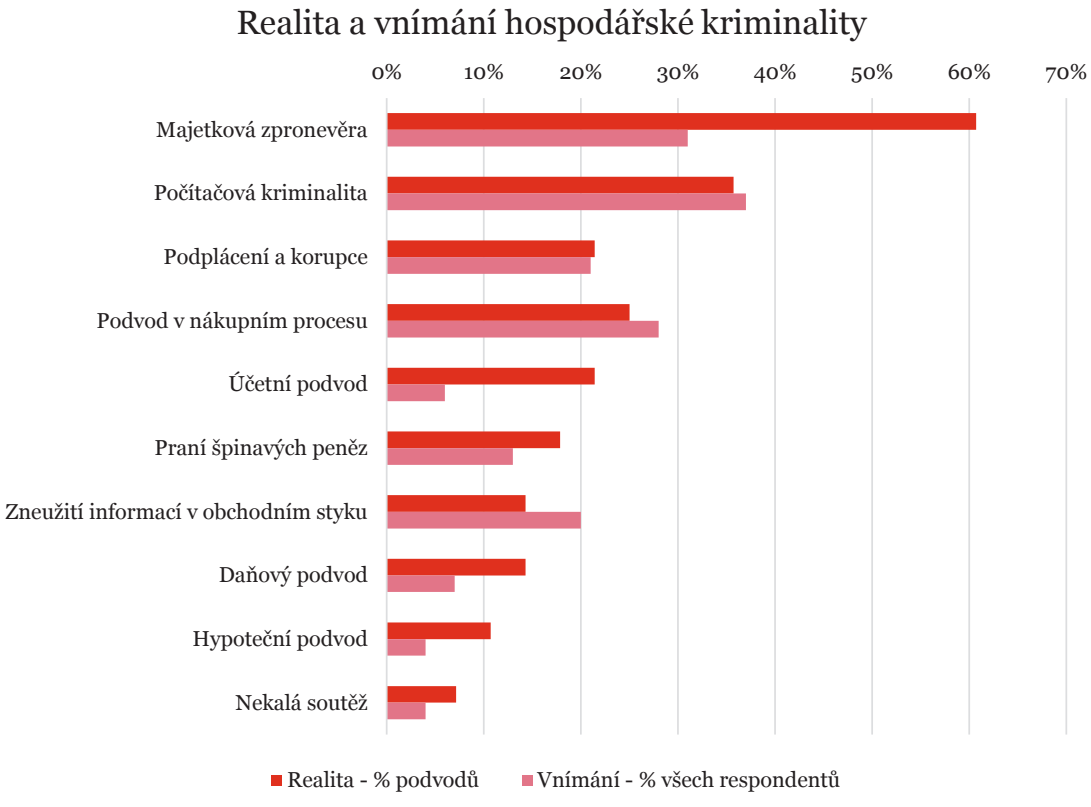
Podle 67 % respondentů považuje vedení jejich firmy etické podnikání za důležité a jde ostatním příkladem. Určuje tak etické klima společnosti a je důležitým prvkem účinné vnitřní kontroly.

I přes rostoucí důraz na etické hodnoty ve firemní komunikaci a rozšíření etických a compliance programů mohou být společnosti svědky nesouladu mezi přístupem vedení a realitou ve firmě. Ať už v chování, tak při přípravě rozpočtu, což zanechává společnosti zranitelné vůči selhání v oblasti compliance.

Budoucnost hospodářské kriminality - realita versus vnímání rizik

V rámci našeho průzkumu jsme se našich respondentů ptali, jakým druhům hospodářské kriminality očekávají, že by mohli čelit v příštích 24 měsících.

Poměrně zajímavé je porovnání vnímání rizik s reálným výskytem hospodářské kriminality. Zdá se, že i přes značný výskyt zpronevěry majetku, společnosti toto riziko podceňují. Naopak, vnímání počítačové kriminality jako hrozby pro společnost je vyšší, než jaký byl její skutečný výskyt. Firmy se vzhledem k rostoucímu trendu počítačové kriminality, který potvrzuje i náš průzkum, zcela správně obávají, že by počítačové kriminalitě mohly v budoucnu čelit.



Contacts

Sirshar Qureshi
partner, vedoucí Forenzních služeb pro střední a východní Evropu
+420 251 151 235
sirshar.qureshi@cz.pwc.com

Pavel Jankech
ředitel, Forenzní technologie
+420 251 151 336
pavel.jankech@cz.pwc.com

Kateřina Halásek Dosedělová
senior manažerka, Forenzní služby
+420 251 151 293
katerina.halasek-dosedelova@cz.pwc.com

www.pwc.com/cz

Praha
Hvězdova 1367/2c, 140 00 Praha 4
Tel.: +420 251 151 111
Fax: + 420 251 156 111

Brno
nám. Svobody 20, 602 00 Brno
Tel.: +420 542 520 111
Fax: +420 542 214 796

Ostrava
Zámecká 20, 702 00 Ostrava
Tel.: +420 595 137 111
Fax: +420 595 137 611

pwc