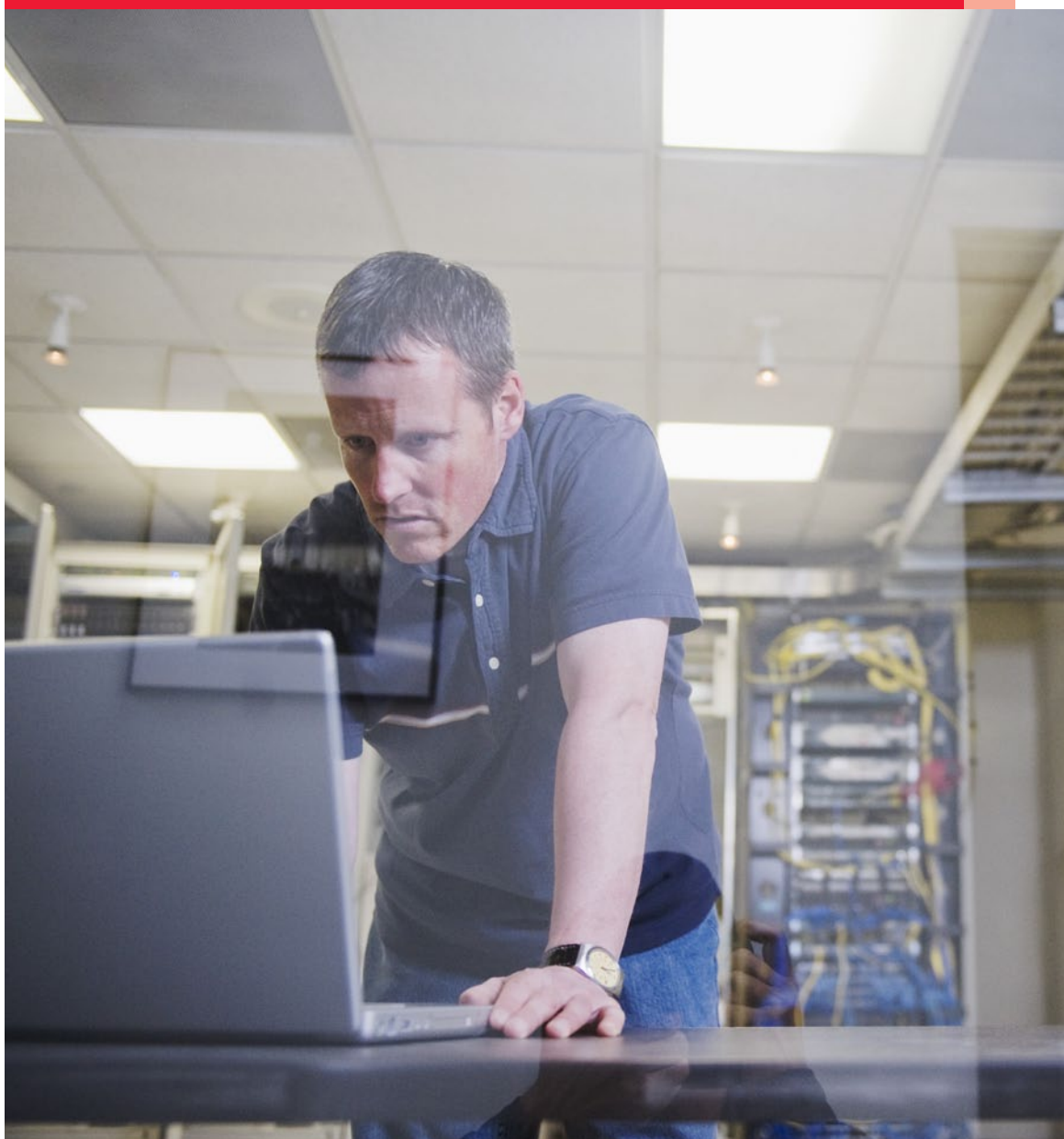


Počítačová kriminalita pod lupou

Celosvětový průzkum hospodářské
kriminality - Česká republika

*Téměř 4000 společností
v 78 zemích světa nám
pomohlo sestavit obrázek
o podvodech a ostatní
hospodářské kriminalitě*

prosinec 2011



Obsah

| | |
|---|-----------|
| Úvod | 5 |
| Hlavní zjištění | 6 |
| <i>Počítačová kriminalita</i> | 6 |
| <i>Současný stav hospodářské kriminality v České republice</i> | 7 |
| Počítačová kriminalita středem pozornosti | 8 |
| <i>Počítačová kriminalita na scéně</i> | 8 |
| <i>Je počítačová kriminalita skutečně jen vnější hrozbou?</i> | 9 |
| <i>Z čeho jsou společnosti opravdu znepokojeny?</i> | 10 |
| <i>Je vaše společnost v ohrožení?</i> | 11 |
| <i>Kdo je v organizaci zodpovědný za řízení rizik počítačové kriminality?</i> | 12 |
| Současný stav hospodářské kriminality v České republice | 13 |
| <i>Vědí společnosti, jakému riziku jsou vystaveny?</i> | 13 |
| <i>O jaké typy hospodářské kriminality se jedná?</i> | 13 |
| <i>Jaké jsou náklady hospodářské kriminality? A její nepřímá škoda?</i> | 14 |
| <i>Kdo je klasickým pachatelem podvodů?</i> | 14 |
| <i>Jak společnosti postupovaly vůči pachatelům podvodů?</i> | 15 |
| <i>Jak společnosti odhalují podvody?</i> | 16 |
| <i>Jak může hodnocení rizik podvodů pomoci společnostem?</i> | 17 |
| <i>Hospodářská kriminalita v budoucnu</i> | 18 |

*Zločin číhá
za každým monitorem*



Úvod

Velice nás těší, že vám můžeme představit výsledky **Celosvětového průzkumu hospodářské kriminality 2011** provedeného společností PwC, který je v současné době nejrozsáhlejším průzkumem svého druhu na světě. Podařilo se nám shromáždit zkušenosti a názory **3877 odborníků ze 78 zemí**, včetně zástupců 84 předních společností z České republiky. Věříme, že výsledky tohoto průzkumu přinesou podnikatelské sféře důležitá fakta o vnímání, očekávání a skutečném dopadu podvodných aktivit na její činnost.

Hospodářská kriminalita si nevybírá. Ovlivňuje organizace po celém světě a žádné ekonomické odvětví ani společnost vůči ní nejsou imunní. Dopady hospodářské kriminality nemají pouze finanční charakter. Mohou mít rovněž za následek poškození dobrého jména firmy či její značky, což v konečném důsledku může vést ke zhoršení její pozice na trhu. Současná společnost stále méně toleruje neetické chování. Organizace si proto musí být jisty, že permanentně budují a udržují veřejnou důvěru.

Náš šestý ročník Celosvětového průzkumu hospodářské kriminality **upozorňuje na rostoucí riziko počítačové kriminality**. Většina lidí a společností v dnešní době spoléhá na internet a další technologie. Tímto chováním se však vystavují potenciálnímu riziku útoku zločinců z celého světa. Úniky informací, krádeže citlivých dat, počítačové viry nebo hacking jsou relativně novým, ale o to nebezpečnějším druhem hospodářské kriminality. Naše studie se zaměřuje na závažnost jejich dopadů a jejich vliv na společnosti po celém světě.

Hledali jsme odpovědi na otázky týkající se počítačové kriminality, hrozeb, které s sebou přináší, a toho, jak se společnosti brání kybernetickým útokům. Do našeho průzkumu jsme rovněž zahrnuli několik základních otázek z oblasti hospodářské kriminality, které nám pomohly sledovat dlouhodobé trendy v této oblasti a porovnat letošní data s předchozími ročníky.

Studie je rozdělena na dvě části:

- počítačová kriminalita – povědomí organizací o jejím nebezpečí, její dopad na společnosti a jak firmy bojují proti souvisejícím rizikům
- současný stav hospodářské kriminality v České republice – se zaměřením na typy podvodů, jejich odhalování, následky a pachatele těchto zločinů



Sirshar Qureshi
partner, oddělení
Forezních služeb,
PwC Česká republika



Michal Kohoutek
ředitel, oddělení
Forezních služeb,
PwC Česká republika

Hlavní zjištění

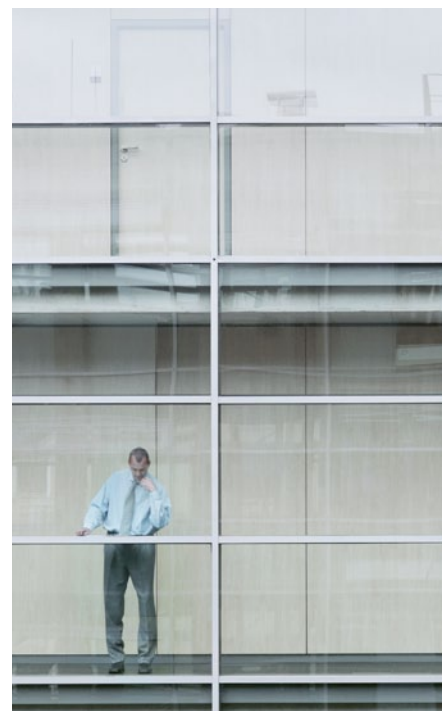


Počítačová kriminalita

- Zatímco v minulosti se počítačová kriminalita v našem průzkumu příliš neobjevovala, dnes patří mezi nejčastěji páchané hospodářské zločiny. V České republice zaujímá svou četností čtvrtou pozici (**13 %**). Přestože je tato hodnota pod průměrem regionu střední a východní Evropy (**18 %**) i celosvětově (**23 %**), předpokládáme, že se její podíl bude v následujících letech dále zvyšovat. **30 %** českých společností se domnívá, že v následujícím roce **bude s velkou pravděpodobností čelit počítačové kriminalitě**. To ji, společně s korupcí a uplácením a zneužitím informací v obchodním styku, řadí mezi nejvíce obávané hospodářské zločiny.
- České společnosti si stále více uvědomují nebezpečí počítačové kriminality. Celkem **98 % českých respondentů** uvedlo, že jejich vnímání rizik plynoucích z počítačové kriminality se ve srovnání s předchozím rokem nezměnilo, nebo dokonce vzrostlo. K tomuto růstu povědomí došlo i přesto, že **2 z 5** českých respondentů v uplynulém roce **neprošli žádným školením se zaměřením na počítačovou bezpečnost**.
- V případech ohrožení počítačovým zločinem se české společnosti nejvíce obávají **krádeže duševního vlastnictví** (včetně krádeže dat), **poškození dobrého jména** společnosti a **krádeže osobních údajů**.
- Společnosti již nevidí hrozbu počítačového zločinu přicházející z vnějšího prostředí: **21 %** českých respondentů považuje toto riziko spíše za **vnitřní hrozbu**, podle dalších **32 %** dotazovaných je stejně pravděpodobné, že útok přijde zevnitř stejně jako zevnu společnosti. V tom, že nejpravděpodobnějším původcem počítačového zločinu uvnitř organizace je **Oddělení informačních technologií (IT)**, se shodují respondenti v České republice, ve střední a východní Evropě i celosvětově.
- Celkem **71 %** dotazovaných uvedlo, že jejich společnosti disponují **vlastními prostředky pro prevenci a odhalování počítačové kriminality**. Téměř polovina respondentů rovněž věří, že jejich organizace je schopna počítačovou kriminalitu interně vyšetřit. Tyto schopnosti jsou většinou přisuzovány právě oddělení IT, které je však zároveň chápáno jako největší interní hrozba v případě počítačového zločinu. Je proto velmi znepokojivé, že **69 %** českých společností **nespolupracuje se specialisty z oblasti forenzních technologií nebo o této spolupráci neví**.
- **Jen 20 %** českých společností **přehodnocuje rizika počítačové kriminality častěji než jednou za rok**. Přes srovnatelné výsledky se společnostmi ve střední a východní Evropě i ve světě nemusí být tato frekvence dostatečná k tomu, aby udržela krok s rychlostí vývoje rizik informačních technologií.

Současný stav hospodářské kriminality v České republice

- Hospodářská kriminalita nadále představuje závažný problém ovlivňující společnosti po celém světě, včetně České republiky. Celkem **29 % společností v České republice se v uplynulém roce stalo obětí hospodářské kriminality**. Tento výsledek je mírně pod průměrem regionu střední a východní Evropy (**30 %**) i pod celosvětovým průměrem (**34 %**). Představuje však oproti minulému průzkumu **nárůst výskytu podvodů o 5 procentních bodů**.
- **Majetková zpronevěra** tradičně zůstává nejčastějším typem hospodářské kriminality v České republice (**75 %**). Stejná situace je ve střední a východní Evropě (**69 %**) i celosvětově (**72 %**). Tento výsledek však není překvapením vzhledem k tomu, že majetková zpronevěra je zpravidla lépe odhalitelná než jiné typy podvodů. **Společně s počítačovou kriminalitou** se rovněž nejvíce podílí na procentuálním nárůstu společností postižených hospodářskou kriminalitou.
- Dalším nejčastějším typem podvodu v České republice jsou **účetní podvody (21 %)** a **korupce a uplácení (21 %)**. Přestože podíl těchto typů hospodářské kriminality ve srovnání s rokem 2009 poklesl, měli bychom být při tvorbě konečných závěrů opatrní. Naše zkušenosti ukazují, že výskyt korupce či uplácení je pravděpodobně mnohem vyšší, neboť je velmi složité tyto delikty identifikovat a často zůstávají neodhaleny. V případě účetních podvodů mohl být pokles způsoben snížením nátlaku na vedení společností, aby manipulovaly s finančními výkazy, a „vylepšovaly“ si tak své výsledky. V době, kdy tento průzkum probíhal, totiž došlo k částečnému zlepšení ekonomické situace. Vzhledem k současnému vývoji světové ekonomiky, zejména Evropy, však může tento tlak opět velmi rychle zesílit a dosáhnout i vyšších úrovní.
- Náklady spojené s podvodem jsou vysoké. Téměř **38 %** respondentů z České republiky, kteří se v minulých dvanácti měsících setkali s podvodem, uvedlo, že celkové náklady **přesáhly 100 tisíc USD**, přitom **8 %** utrpělo škodu převyšující **5 milionů USD**. Důsledky podvodu však nejsou pouze přímé finanční náklady. Přestože je zpravidla velmi obtížné nepřímé náklady vyčíslit, jejich dopady mohou být stejně závažné. Celkem **67 %** společností, které se staly obětí hospodářského zločinu v uplynulých dvanácti měsících, uvedlo jako nejzávažnější nefinanční dopad **zhoršení morálky zaměstnanců**.
- Hlavní hrozba z pohledu hospodářské kriminality přišla zevnitř organizace, a to **ze strany zaměstnanců (67 %)**. Toto číslo ve srovnání s rokem 2009 (**50 %**) výrazně vzrostlo. Nejčastějšími **externími pachateli byli zákazníci (43 %)** a **dodavatelé (29 %)**.
- Náš průzkum naznačuje, že se české společnosti nebojí radikálního postupu vůči interním i externím pachatelům podvodů. Nejčastější reakcí v případě interních pachatelů bylo **propuštění (81 %)**. Obdobně v **71 %** byl ukončen obchodní vztah s externím pachatelem. Tento výsledek představuje výrazný nárůst oproti roku 2009 (**30 %**) a je vysoko nad průměrem střední a východní Evropy (**53 %**) i celosvětově (**39 %**). Malá tolerance vůči pachatelům podvodů je jistě pozitivní, přesto bychom společností rovněž doporučili, aby se více soustředily i na oblast prevence. Programy „poznej lépe své zaměstnance a obchodní partnery“, které by měly být aplikovány před začátkem spolupráce, jsou zajisté méně nákladné než následky podvodů.
- Je povzbuzující, že prostřednictvím detekčních mechanismů je odhaleno stále více podvodů. Již **38 %** napadených českých společností odhalilo podvod pomocí **systémů řízení rizik** nebo během **pravidelných interních auditů (2009: 35 %)**. Je tedy zřejmé, že se tuzemské firmy při detekci podvodu **chtějí stále méně spoléhat na náhodu**. Avšak v situaci, kdy **1 z 5 podvodů** byl odhalen prostředky mimo oblast vlivu managementu, vidíme v této oblasti stále prostor pro zlepšení:
 - **42 %** českých společností **neprovádí žádné hodnocení rizik podvodů** nebo o takovém hodnocení neví. Hlavním důvodem je **pocit nedostatečné přidané hodnoty tohoto nástroje (57 %)** nebo **neznalost obsahu** tohoto pojmu (**21 %**).
 - **71 %** českých společností **nevyužívá mechanismu anonymní informační linky**. Tento fakt je poměrně překvapivý, jelikož z naší zkušenosti fungující anonymní informační linka pomáhá k odhalení podvodů právě v situacích, kdy se jiné prostředky detekce ukazují jako neúčinné.



Počítačová kriminalita středem pozornosti

Co je počítačová kriminalita?

Celosvětový průzkum hospodářské kriminality 2011 se zaměřil na finanční kriminalitu a podvodné aspekty spojené s počítačovým zločinem. Tento zločin byl pro potřeby průzkumu definován takto:

„Počítačová kriminalita je hospodářský trestný čin spáchaný pomocí počítače či internetu. Typickými příklady počítačové kriminality jsou šíření virů, nelegální stahování médií, phishing a pharming a krádeže osobních informací, jako jsou např. údaje o bankovním účtu. Nespádají sem běžné podvody, kdy je počítač používán jako vedlejší nástroj s cílem spáchat podvod. Zahrnujeme zde pouze takové hospodářské zločiny, kde jsou počítač, internet nebo užití elektronických médií a zařízení hlavním, nikoliv náhodným, prvkem.“¹

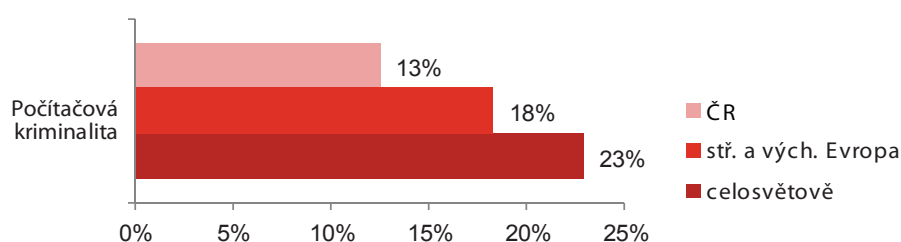
Výše zmíněná definice může být chápána jako obecný popis počítačové kriminality, nicméně mnoho lidí vnímá tuto oblast jako širší fenomén, který dává prostor k různým interpretacím. Jednotná celosvětová definice počítačové kriminality neexistuje, což může vést k tomu, že společnosti si nemusí plně uvědomovat všechna rizika, která s ní souvisí, ani jaké dopady může mít na jejich fungování. Následný boj proti počítačovému zločinu nebo jeho detekce jsou pak velmi složité.

¹ Definováno společností PwC ve spolupráci s akademickým partnerem průzkumu, profesorem Peterem Sommerem z London School of Economics.

Počítačová kriminalita na scéně

Zatímco v minulosti se počítačová kriminalita v našem průzkumu příliš neobjevovala, dnes patří mezi nejčastěji páchané hospodářské zločiny. V České republice zaujímá svou četností čtvrtou pozici (13 %), což je pod průměrem regionu střední a východní Evropy (18 %) i celosvětově (23 %). Předpokládáme však, že se její podíl bude v následujících letech dále zvyšovat.

Podíl počítačové kriminality na spáchaných podvodech



Jen 2 % respondentů z České republiky se domnívají, že riziko plynoucí z počítačové kriminality ve srovnání s minulým rokem klesá. Naopak celých 98% dotázaných uvedlo, že se jejich vnímání rizik buď zvýšilo (32%) nebo zůstalo na stejné úrovni (66%).

30 % českých společností očekává, že v následujícím roce bude s největší pravděpodobností čelit počítačové kriminalitě. To ji, společně s korupcí a uplácením a zneužitím informací v obchodním styku, řadí mezi nejvíce obávané hospodářské zločiny. Tato statistika jasně ukazuje, že hrozba počítačového zločinu neustále roste.

„V dnešním technologickém světě stále více společností používá internet, sociální sítě nebo mobilní aplikace ke zvýšení své výkonnosti a efektivnější obsluze zákazníků. Je zde však i stinná stránka věci. S tím, jak se rozšiřuje používání nových technologií, roste i počet a účinnost počítačových útoků. Jasně vidíme, že počítačová kriminalita je na vzestupu. Stále častěji se na nás společnosti obrací, abychom jim pomohli vyšetřit, jak došlo k únikům citlivých dat a kdo je za to zodpovědný.“

Pavel Jankech

senior manažer, Oddělení forenzních technologií,
PwC Česká republika



Počítačová kriminalita je „lákavá“

Podvodník se obvykle nenachází na místě zločinu, takže je nižší pravděpodobnost jeho dopadení.

Podvodník může útočit z jiné země/jurisdikce. Orgány činné v trestním řízení pak mohou mít omezené možnosti pachatele identifikovat a potrestat.

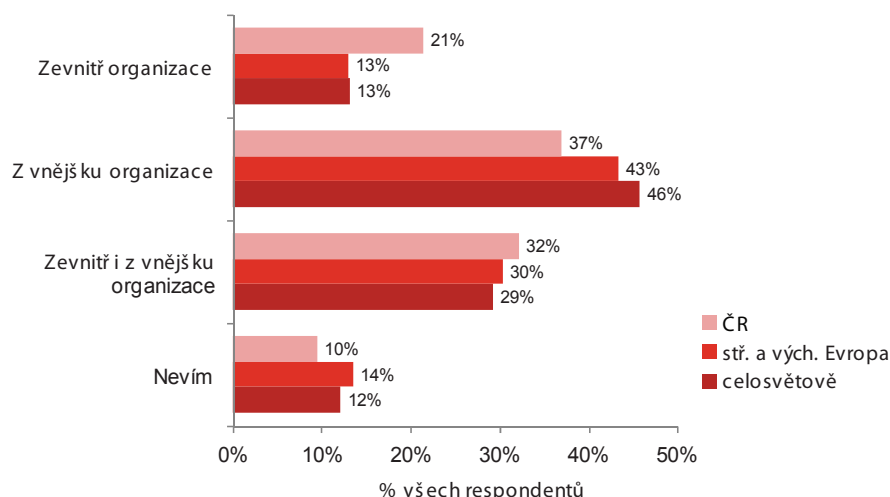
Z důvodu zeměpisných, právních či politických překážek se pachatel může vrátit zpět „na místo činu“ bez větší hrozby odhalení.

Rychlý vývoj informačních technologií společně komplikuje snahu držet krok v prevenci počítačové kriminality.

Je počítačová kriminalita skutečně jen vnější hrozbou?

Počítačový zločin byl tradičně vnímán jako nebezpečí přicházející z vnějšího prostředí. Náš průzkum však naznačuje změnu v tomto chápání: 21 % českých respondentů vidí toto riziko spíše jako **vnitřní hrozbu**, dalších 32 % dotazovaných považuje za stejně pravděpodobné, že útok přijde zevnitř nebo zvenku. Tento posun můžeme sledovat u respondentů po celém světě.

Odkud hrozí vaší organizaci největší riziko?



Oddělení IT je vnímáno jako nejpravděpodobnější pachatel počítačové kriminality uvnitř společnosti jak v České republice (51 %), tak i ve střední a východní Evropě (53 %) a ve světě (53 %). Tento výsledek není překvapením vzhledem k tomu, že zaměstnanci oddělení IT jsou vnímáni jako ti, kteří mají nezbytné znalosti, ale i příležitosti, ke spáchání takového činu. Konkrétně se jedná například o administrátorská práva pro přístup do systémů, a tím i možnost měnit nebo mazat data v systémech, jakož i schopnost zahazovat za sebou stopy, které by mohly vést k odhalení pachatele.

Zajímavé ovšem je, že čeští respondenti vidí riziko vnitřního útoku přicházejt rovněž z oddělení obchodu a marketingu (31 %), financí (22 %) či z oddělení provozu (20 %).

Naproti tomu za nejméně pravděpodobné považují dotázaní možnost, že by počítačový zločin provedl někdo z právního oddělení (4 %) nebo z oddělení lidských zdrojů (7 %). Společnosti by však neměly opomíjet ani tato oddělení, protože počítačový zločin může přijít odkudkoliv.



„Cesta, jak přimět společnosti přemýšlet o počítačové kriminalitě, vede přes diskuzi nad riziky, ne přes technické debaty o šifrování, penetračním testování nebo o nastavení firewallů. Nechme společnosti zamyslet se nad tím, co se může stát s jejich dobrým jménem, pokud ke ztrátě důležitých dat dojde.“

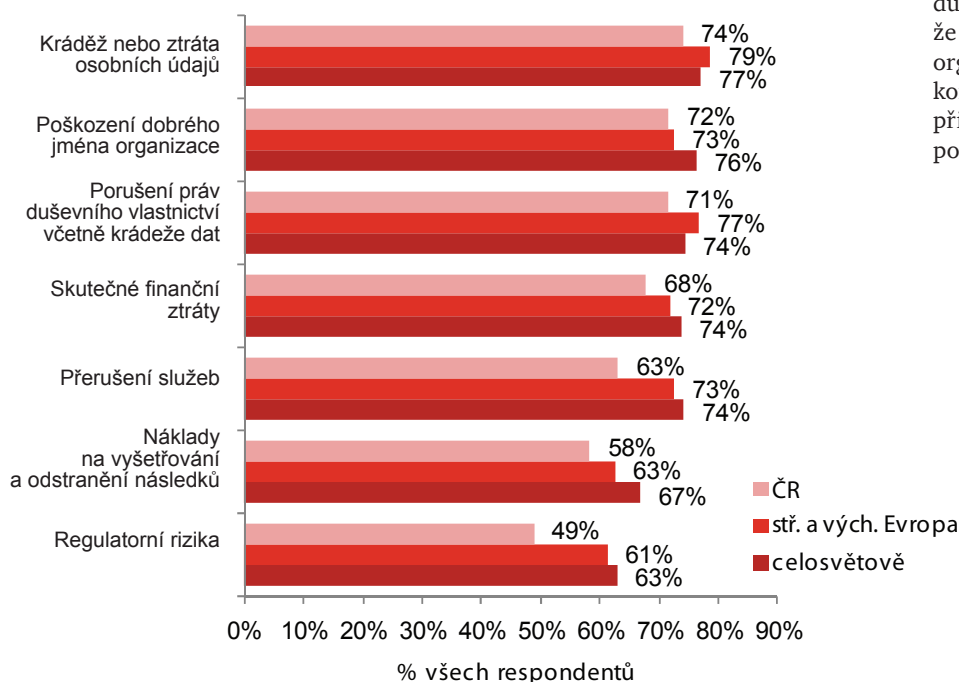
Filip Volavka

senior manažer, Oddělení forenzních technologií,
PwC Česká republika

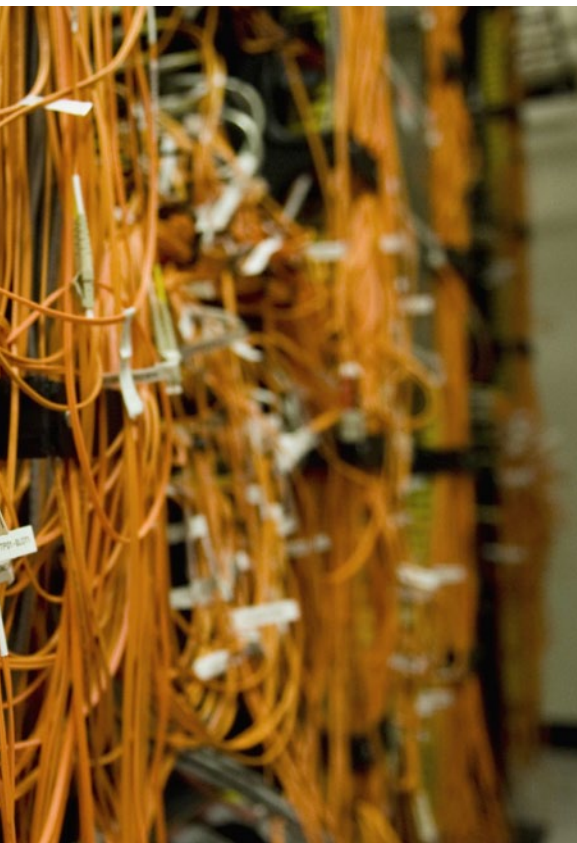
Z čeho jsou společnosti opravdu znepokojeny?

V případě ohrožení počítačovým zločinem se české společnosti nejvíce obávají **krádeže duševního vlastnictví (71 %)**, včetně krádeže dat, **poškození dobrého jména společnosti (72 %)** a **krádeže osobních údajů (74 %)**.

Obavy týkající se počítačové kriminality



Vzhledem k těmto rostoucím obavám z počítačové kriminality je velmi důležité, aby společnosti prokázaly, že právě ony jsou tou nejbezpečnější organizací na trhu, a tím dosáhly nejen konkurenční výhody, ale současně tak přispěly k budování bezpečného podnikatelského prostředí.



Je vaše společnost v ohrožení?

Jak jsme již zmínili, **32 %** respondentů si uvědomuje, že riziko počítačového zločinu je na vzestupu. Počítačová kriminalita se zařadila mezi čtyři nejvýznamnější druhy podvodu. Mnoho respondentů rovněž uvedlo, že jsou silně znepokojeni z možných dopadů počítačového zločinu na dobré jméno jejich organizace. Navzdory všem těmto obavám však společnosti v této oblasti nepodnikají dostatečné kroky a zaměřují se spíše na reakci, než na prevenci.

Náš průzkum ukázal, že v České republice:

- Celkem **71 %** dotazovaných uvedlo, že jejich společnosti disponují **vlastními prostředky pro prevenci a odhalování počítačové kriminality**, na druhé straně však
- **69 %** dotazovaných neví nebo si není vědomo, zda jejich společnost využívá specialistů v oblasti forenzních technologií
- **2 z 5** respondentů v uplynulém roce **neprošli žádným školením se zaměřením na počítačovou bezpečnost**
- **39 %** organizací nemá připraven postup případného krizového vypnutí počítačových sítí nebo o takovém postupu respondenti neví.

Hlídní sociálních sítí

Více než polovina (**56 %**) českých respondentů uvedla, že jejich organizace nesleduje používání sociálních sítí, nebo si toho nejsou vědomi. Toto číslo je poměrně překvapivé, neboť tyto stránky mohou představovat velké bezpečnostní riziko, pokud je zaměstnanec zneužije.

Přestože sociální sítě jako **Facebook** nebo **LinkedIn** nemusí samy o sobě představovat skutečného původce počítačové kriminality, mohou sloužit jako velmi cenný zdroj pro počítačový zločin typu sociálního inženýrství a následné efektivní útoky, např. phishing. Příkladem může být schéma, kdy jsou na sociálních sítích sbírány veškeré informace o cílové osobě, aby mohlo dojít k přesně zaměřenému počítačovému útoku na tuto osobu nebo k nainstalování škodlivého kódu do jejího počítače.

V případě, kdy společnosti přijaly preventivní opatření proti počítačovému zločinu, celkem **92 %** respondentů uvedlo, že monitorují vnitřní i vnější elektronickou komunikaci, včetně aktivity na webových stránkách. Zaměstnanecké smlouvy **62 %** dotazovaných společností obsahují pravidla správného užívání interní dokumentace a informací. Interních vzdělávacích programů se účastnilo **35 %** respondentů. To dokazuje, že společnosti, které přijaly preventivní opatření, podnikají správné kroky. Ostatní organizace jsou ovšem vystaveny hrozbě poškození dobrého jména nebo ztrátě citlivých informací tím, že nemají nastaveny adekvátní kontroly.

„Sociální sítě představují revoluci v mezilidské komunikaci. Dokonce i společnosti využívají jejich služby, a to z důvodu marketingu, lepší komunikace se zákazníkem nebo za účelem získávání informací. Pobyt na sociálních sítích však s sebou přináší celou řadu bezpečnostních rizik. Nejde pouze o neefektivně strávený čas zaměstnanců u počítače. Sociální sítě mohou být rovněž branou pro únik citlivých dat nebo pro vniknutí škodlivého počítačového kódu do systémů společnosti.“

Pavel Jankech

senior manažer, Oddělení
forenzních technologií,
PwC Česká republika

„Výkonní ředitelé a představenstva společností stále považují informační bezpečnost jen za technický problém. Toto je nesprávná představa, která se musí změnit. Rozsah finančních rizik a hrozba poškození dobrého jména společnosti jasně ukazují, že informační bezpečnost by měla být jednou z hlavních oblastí, které vedení společnosti řeší.“

Tomáš Kuča

vedoucí oddělení Risk Assurance,
PwC Česká republika a Slovensko

Kdo je v organizaci zodpovědný za řízení rizik počítačové kriminality?

Našich respondentů jsme se rovněž zeptali, kdo by měl být zodpovědný za řízení rizik týkajících se počítačové kriminality. Více než polovina (52 %) dotázaných v České republice přisuzuje hlavní zodpovědnost ředitelům oddělení IT. Dalších 29 % si myslí, že je to odpovědnost výkonných ředitelů a představenstva společnosti. Tato čísla nasvědčují tomu, že bez ohledu na to, zda je ředitel IT členem představenstva, není odpovědnost sdílena s výkonným ředitelem a představenstvem společnosti. Je zřejmé, že riziko bezpečnosti informačních technologií je obvykle odpovědností ředitele IT.

Je však zároveň nezbytné, aby výkonný ředitel a představenstvo společnosti porozuměli počítačové kriminalitě a pravidelně vyhodnocovali její rizika.

Není proto příliš překvapující, že dle našeho průzkumu výkonní ředitelé a představenstva pravidelně hodnotí rizika spojená s počítačovou kriminalitou: **pouze 20 %** organizací **hodnotí hrozby počítačového zločinu častěji než jednou za rok** a u **6 %** společností se tímto rizikem výkonní ředitelé a představenstva dokonce nezabývají vůbec.

Tato čísla ukazují, že vedení společností nekladou dostatečný důraz na řízení rizik, která počítačová kriminalita představuje pro jejich organizaci. Věříme, že v budoucnu bude jednou z rozhodujících charakteristik společností, které efektivně řídí rizika a uvědomují si výhody s tím spojené, právě výkonný ředitel, který skutečně rozumí rizikům a příležitostem počítačového světa.

Jaké kroky by měly společnosti podniknout, aby se ubránily počítačovým útokům?

- 1. Zapojení výkonného ředitele** – generální ředitel a představenstvo společnosti si musí uvědomit počítačové hrozby. Je důležité, aby rozuměli všem rizikům a novým možnostem počítačové kriminality.
- 2. Přehodnocení bezpečnostních funkcí a připravenost** organizace pro případ počítačového zločinu – na rozdíl od tradiční hospodářské kriminality je počítačová kriminalita mnohem rychlejší ve vytváření nových druhů útoků. Společnosti proto potřebují neustále přizpůsobovat své postupy a procesy.
- 3. Povědomí** – organizace by měla znát současné i nově vznikající počítačové prostředí. Pokud je splněna tato podmínka, pak mohou být přijata důležitá rozhodnutí následovaná jasně definovanými kroky.
- 4. Vytvoření reakčního týmu pro případ ohrožení počítačové bezpečnosti** – tento tým by měl jednat velmi pružně a rychle. Pokud je takový tým vytvořen, pak je každý případ zaznamenán, rizikově vyhodnocen a řešen.
- 5. Školení všech zaměstnanců** – organizace by měly rozšiřovat povědomí o hrozbách počítačové kriminality, a to například i pomocí najímání zkušených odborníků v této oblasti, jejichž znalost je pak sdílena s dalšími zaměstnanci. Vytvoření takového prostředí je ideálním preventivním opatřením.
- 6. Aktivní a jasný postoj vůči počítačové kriminalitě** – společnosti by měly veřejně komunikovat, jaké preventivní a reaktivní opatření provedly v oblasti počítačového zločinu, a učinit jasné právní kroky proti pachatelům počítačové kriminality.

Současný stav hospodářské kriminality v České republice

Vědí společnosti, jakému riziku jsou vystaveny?

Hospodářská kriminalita nadále představuje závažný problém ovlivňující společnosti po celém světě, včetně České republiky. Celkem **29 % tuzemských společností se v uplynulém roce stalo obětí hospodářské kriminality**. Tento výsledek je mírně pod průměrem regionu střední a východní Evropy (**30 %**) i pod celosvětovým průměrem (**34 %**), představuje tak oproti minulému průzkumu **nárůst výskytu podvodů o 5 procentních bodů**.

O jaké typy hospodářské kriminality se jedná?

Podíl jednotlivých typů hospodářské kriminality v ČR



Majetková zpronevěra tradičně zůstává nejčastějším typem hospodářské kriminality v České republice (**75 %**). Stejná situace je rovněž ve střední a východní Evropě (**69 %**) i celosvětově (**72 %**). Tento výsledek však není překvapením vzhledem k tomu, že zpronevěra je zpravidla lépe odhalitelná než jiné typy podvodů. Zdá se, že zpronevěra se **společně s počítačovou kriminalitou** nejvíce podílí na nárůstu počtu společností postižených hospodářskou kriminalitou.

Dalším nejčastějším typem podvodu v České republice jsou **účetní podvody (21 %)** a **korupce a uplácení (21 %)**. Přestože podíl těchto typů hospodářské kriminality ve srovnání s rokem 2009 poklesl, měli bychom být při tvorbě našich závěrů opatrní:

- Naše zkušenosti ukazují, že **výskyt uplácení a korupce je pravděpodobně mnohem vyšší**, neboť tyto podvody je velmi složité identifikovat a často zůstávají neodhaleny. Porovnání s průměrem střední a východní Evropy dosaženém v roce 2011 (**36 %**) také naznačuje, že i výsledek za Českou republiku bude pravděpodobně dosahovat reálně vyšších hodnot.

- V případě účetních podvodů náš průzkum ukazuje na celosvětový pokles výskytu tohoto typu hospodářské kriminality. Avšak ve srovnání s ostatními zeměmi byl pokles v České republice ještě výraznější.

Důvody poklesu podílu účetních podvodů mohou být různé:

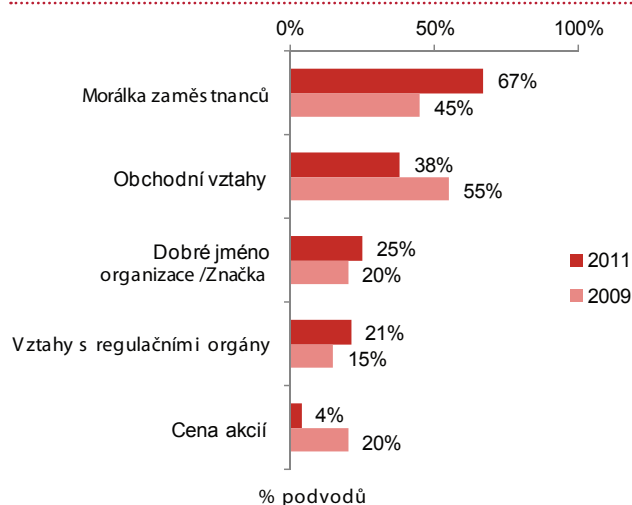
- společnosti mohly zavést přísnější kontroly, které případné pachatele odrazují
- vedení společností již nečelí takovým tlakům na manipulaci finančních výsledků jako před dvěma lety, kdy řada společností bojovala o přežití
- podvody již nemohou být tak důsledně odhalovány, neboť v posledních letech docházelo celosvětově ke snižování počtu zaměstnanců, kteří se právě prevencí a odhalováním hospodářské kriminality zabývali
- vzhledem k tomu, že letošní průzkum byl zaměřen na oblast počítačové kriminality, mohli někteří respondenti, kteří dříve do kategorie účetních podvodů zařadili i ty podvody, kde došlo k použití počítačů, elektronických zařízení a internetu, letos tyto podvody zařadit do kategorie počítačové kriminality.

Jaké jsou náklady hospodářské kriminality? A její nepřímá škoda?

Téměř **38 %** respondentů z České republiky, kteří se v minulých 12 měsících setkali s podvodem, uvedlo, že celkové náklady **přesáhly 100 tisíc USD**. Celkem **8 %** postižených utrpělo dokonce škodu převyšující **5 milionů USD**.

Celkem **67 %** společností, které se staly obětí hospodářského zločinu v uplynulých 12 měsících, uvedlo jako nejzávažnější nefinanční dopad **zhoršení morálky zaměstnanců**. Jako další zmiňovaly poškození obchodních vztahů (**38 %**), popřípadě poškození reputace nebo obchodní značky (**25 %**).

Nepřímé náklady podvodů v České republice



Kdo je klasickým pachatelem podvodů?

Z našich zkušeností vyplývá, že většina případů hospodářské kriminality je páchána zevnitř společnosti (**67 %**), tj. interními pachateli, což ve srovnání s rokem 2009 znamená výrazný nárůst (2009: **50 %**). Tato skutečnost pravděpodobně souvisí s tím, že zaměstnanci jsou zapojeni do běžného provozu a znají lépe situaci uvnitř společnosti. Mají tak lepší příležitost ke spáchání podvodu.

Hlavními externími pachateli podvodů byli ve **43 %** případů **zákazníci** a ve **29 %** **dodavatelé**. Počet podvodů, které byly spáchány obchodními zástupci nebo zprostředkovateli ve srovnání s rokem 2009 významně poklesl, a to o více než **40 procentních bodů**.

Základem prevence je znát svého obchodního partnera. Proverky typu „poznej svého zákazníka či dodavatele“ se tak staly důležitou součástí programů sloužících ke snižování rizik. Tyto programy transparentnosti jsou v současné době jedním z neúčinnějších preventivních prostředků, které mají společnosti k dispozici.

„Správná rozhodnutí mohou být činěna pouze na základě dostatečných a spolehlivých informací. Při navazování spolupráce s obchodními partnery doporučujeme společně zavést kontrolu konfliktu zájmů jako součást běžných obchodních postupů. Prověřování může společně pomoci nejen ve vyhodnocení potenciálních rizik souvisejících s třetími stranami, jako například dodavateli a zprostředkovateli. Lze ho využít i k vyhodnocení rizik, která souvisí s vnitřním prostředím firmy. Kontrola konfliktu zájmů může být totiž začleněna i do procesu náborem nových pracovníků, a tím poskytnout hodnotné informace před uzavřením zaměstnanecké smlouvy. Nicméně kontrolu konfliktu zájmů doporučujeme provádět pravidelně i při vyhodnocování stávajících zaměstnanců.“

Eva Křištofová
manažerka, Forenzní služby, PwC Česká republika



Jak společnosti postupovaly vůči pachatelům podvodů?

V České republice bylo v případě interních pachatelů nejčastější reakcí **propuštění (81 %)** a o každém druhém případě byla informována policie. Zde stojí za zmínku fakt, že počet případů, kdy **došlo k propuštění zaměstnance v reakci na zjištěný interní podvod, celkově v České republice vzrostl (2009: 65 %)**. Stejný trend byl také zaznamenán v regionu střední a východní Evropy i celosvětově. Jedná se o velmi pozitivní výsledek, jelikož se ukazuje, že společnosti jsou méně ochotny zaznamenat incident „zamést pod koberec“.

V podobném duchu jako u interních pachatelů vykazují české společnosti rovněž malou toleranci vůči externím pachatelům. V případě podvodu spáchaného externím pachatelem **86 %** českých respondentů odpovědělo, že jejich společnost informovala policii a **71 %** českých společností následně ukončilo obchodní vztah s pachatelem. Toto představuje pro Českou republiku dramatický nárůst oproti roku 2009 (**30 %**) a výsledek je dokonce vysoko nad hodnotami regionu střední a východní Evropy (**53 %**) i celosvětovým průměrem (**39 %**).

Celkově tyto výsledky jasně indikují, že většina českých společností se při postupu proti pachatelům podvodů ubírá správným směrem, a vysílají tak jasnou zprávu ohledně vnímání podvodů jak v rámci své společnosti, tak i externě. Přesto bychom rovněž doporučili, aby se více soustředily na oblast prevence. Programy „poznej lépe své zaměstnance a obchodní partnery“, které by měly být aplikovány před začátkem spolupráce, jsou zajisté méně nákladné než důsledky podvodů.

„Pro zvýšení efektivity anonymního informačního systému je potřeba provést několik důležitých kroků před jeho samotným zavedením. Patří mezi ně zejména porozumění firemní kultuře a její správné zhodnocení, nastavení cílů a jejich prezentace či volba správných prostředků, které budou použity. Firma by také měla mít jasný plán, jak bude ohlášené případy řešit a jak o nich bude informovat ostatní zaměstnance.“

„Efektivní anonymní informační systém pomáhá nejen předcházet pochybením a podvodnému jednání, ale dává také pozitivní signál směrem k obchodním partnerům a veřejnosti, a snižuje tak riziko negativního vnímání společnosti.“

Jiří Urban

senior manažer, Forenzní služby, PwC Česká republika

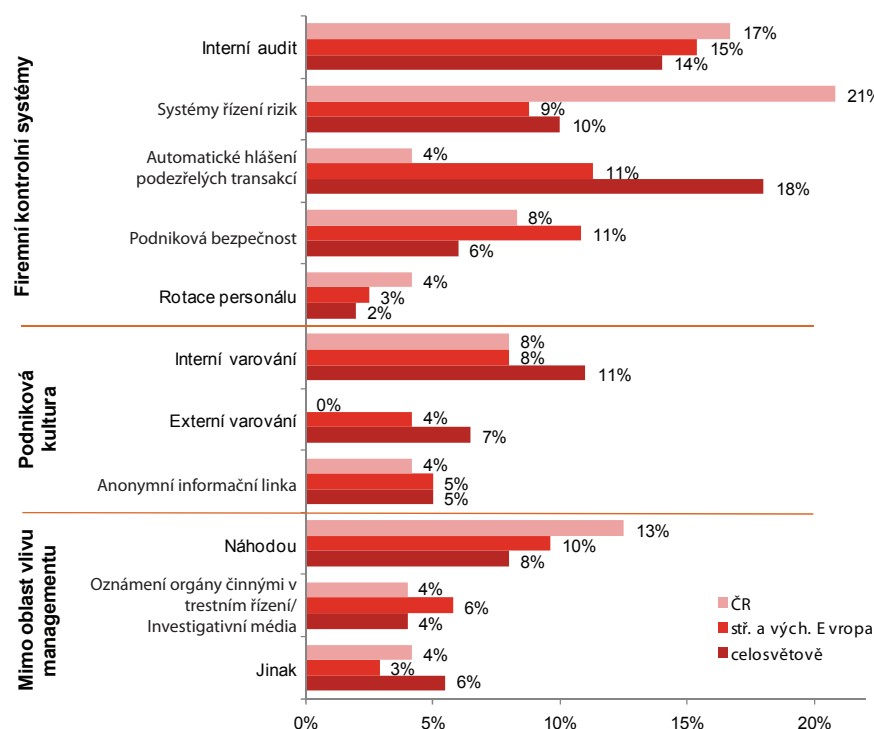
Jak společnosti odhalují podvody?

Je povzbuzující, že prostřednictvím detekčních mechanismů je odhaleno stále více podvodů. Celkem **38 %** českých společností odhalilo podvod pomocí **systémů řízení rizik** nebo během **pravidelných interních auditů** (2009: 35 %). Konkrétně **21 %** případů podvodného jednání bylo odhaleno prostřednictvím systémů řízení rizik, což je výrazně více ve srovnání se střední a východní Evropou (**9 %**) i celosvětovým průměrem (**10 %**).

Je velmi pozitivní, že ve srovnání s rokem 2009 v České republice počet případů podvodného jednání odhalených náhodně nebo pomocí jiných faktorů, které jsou mimo oblast vlivu společnosti (**21 %**), poklesl (2009: **30 %**). Tato skutečnost svědčí o tom, že se české společnosti při detekci podvodu **nechtějí spoléhat na náhodu**. Avšak v situaci, kdy **1 z 5 podvodů** byl odhalen prostředky mimo oblast vlivu managementu, vidíme v této oblasti stále určitý prostor pro zlepšení:

- V České republice hraje odhalení podvodného jednání **pomocí elektronického a automatizovaného hlášení podezřelých transakcí** zanedbatelnou roli (**4 %**). Avšak v celosvětovém měřítku počet takto odhalených případů vzrostl z **5 %** v roce 2009 na **18 %** v roce 2011. Z našeho pohledu se jedná o velmi účinný nástroj, jelikož je identifikování podvodu založeno na elektronickém automatizovaném systému a detekce je zahájena vždy při každé podezřelé transakci, a to nezávisle na lidském faktoru.
- **71 %** českých společností **nevyužívá mechanismu anonymní informační linky**. Tento fakt je poměrně překvapivý, jelikož z našich zkušeností fungující anonymní informační linka pomáhá k odhalení podvodů právě v situacích, kdy se jiné prostředky detekce ukazují jako neúčinné.

Způsob odhalení podvodu



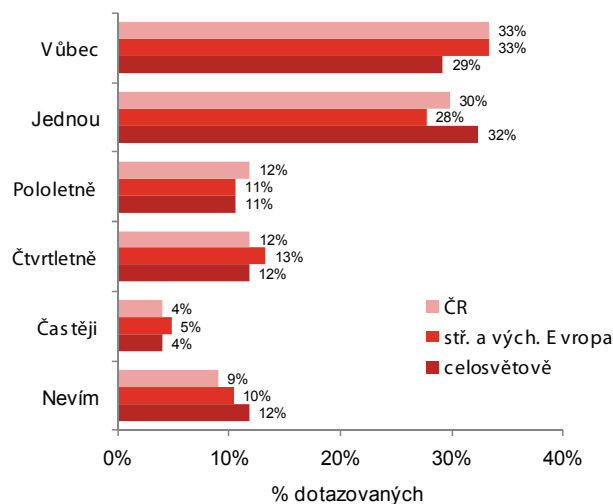
Jak může hodnocení rizik podvodů pomoci společností?

V rámci prevence podvodu je důležité, aby společnosti hodnotily rizika a identifikovaly možné mezery v systému. Pravidelné hodnocení rizik podvodů pomáhá společnostem určit, nakolik jsou případnému riziku podvodu vystaveny. Výsledky našeho průzkumu ukazují jasný vztah mezi frekvencí hodnocení rizik a případy odhalení podvodu.

Je proto znepokojivé, že **42 %** českých společností, které se zúčastnily průzkumu, **neprovedlo žádné hodnocení rizik podvodů (33%)** nebo o takovém hodnocení neví (**9%**). Další **30 %** provedlo toto hodnocení pouze jednou.

Hlavními důvody, proč české společnosti neprovedly hodnocení rizik podvodů, byl pocit **nedostatečné přidané hodnoty tohoto nástroje (57 %)** nebo neznalost obsahu tohoto pojmu (**21 %**). Tento výsledek ukazuje, že české společnosti mají pouze malé povědomí o této problematice.

Četnost hodnocení rizik podvodů



„Je nutné, aby společnosti pochopily výhody pravidelného provádění hodnocení rizik podvodů a jejich důležitost v boji proti hospodářské kriminalitě. Vzhledem k tomu, že podvod je vždy páchan se špatným úmyslem, je zřejmé, že musí být konstruován tak, aby ho nebylo možné odhalit. Přestože manažeři řešící celou řadu jiných a „důležitějších“ problémů mohou považovat hodnocení rizik podvodu za nevýznamnou záležitost, dobře navržený a efektivní postup může pomoci identifikovat oblasti více náchylné k podvodu a rovněž předpovědět chování potenciálního pachatele.“

Kateřina Halásek Dosedělová

senior manažerka, Forenzní služby, PwC Česká republika

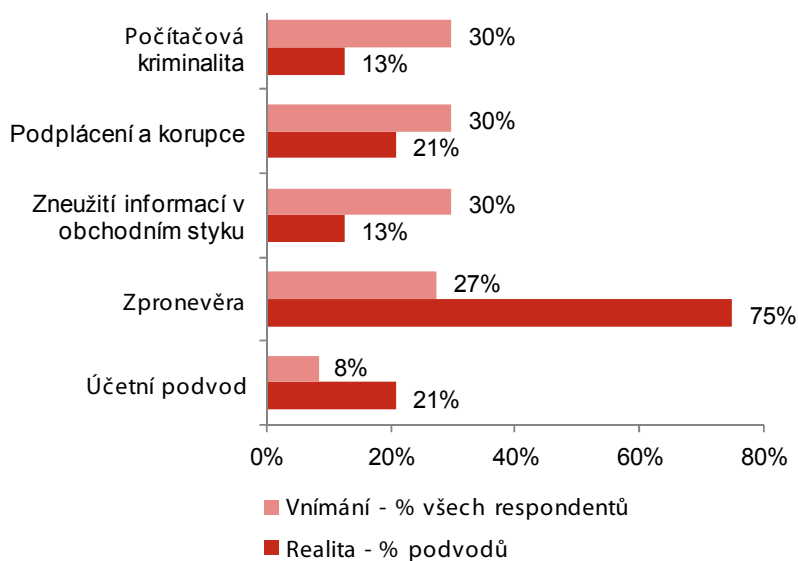


Hospodářská kriminalita v budoucnu

30 % českých společností považuje korupci, počítačovou kriminalitu a zneužívání informací v obchodním styku za typy podvodů, jimž by mohly čelit v následujících 12 měsících. Dalších 27 % respondentů se obává majetkové zpronevěry.

Zcela nepochopitelné je přesvědčení většiny společností v České republice, že se s hospodářskou kriminalitou v následujících 12 měsících nesetkají vůbec. Například pouze 8% českých respondentů se obává, že bude v blízké budoucnosti čelit účetnímu podvodu. Společnosti by však neměly podlehnout falešnému pocitu bezpečí. Vezmeme-li v úvahu současný vývoj světové ekonomiky, mohla by se tato iluze velmi snadno rozplynout.

Vnímání a skutečnost v České republice



Poznámky

Forenzní služby

Kontakty v České republice



Sirshar Qureshi

partner, Forenzní služby, PwC Česká republika

telefon: +420 251 151 235

e-mail: sirshar.qureshi@cz.pwc.com



Michal Kohoutek

ředitel, Forenzní služby, PwC Česká republika

telefon: +420 251 151 231

e-mail: michal.kohoutek@cz.pwc.com



Kateřina Halásek Dosedělová

senior manažerka, Forenzní služby, PwC Česká republika

telefon: +420 251 151 293

e-mail: katerina.halasek-dosedelova@cz.pwc.com



Jiří Urban

senior manažer, Forenzní služby, PwC Česká republika

telefon: +420 251 151 627

e-mail: jiri.urban@cz.pwc.com



Pavel Jankech

senior manažer, Forenzní technologie, PwC Česká republika

telefon: +420 251 151 336

e-mail: pavel.jankech@cz.pwc.com



Filip Volavka

senior manažer, Forenzní technologie, PwC Česká republika

telefon: +420 251 151 269

e-mail: filip.volavka@cz.pwc.com