

Globálny prieskum hospodárskej kriminality 2016

Správa za Slovensko

www.pwc.com/sk

34%

spoločností na
Slovensku sa stretlo
s jedným alebo
viacerými prípadmi
hospodárskej
kriminality

13%

prípadov tvorila
počítačová kriminalita





Obsah

3	Predslov
4	Hlavné zistenia
4	Súčasný stav hospodárskej kriminality na Slovensku
5	Počítačová kriminalita
5	Etika a compliance
6	Hospodárska kriminalita na Slovensku
6	Hospodárska kriminalita ako nezadržateľná hrozba
7	Akým druhom hospodárskej kriminality čelia slovenské spoločnosti?
8	Počítačová kriminalita
9	Korupcia a úplatkárstvo
10	Koľko stojí podvod?
11	Technológia v hospodárskej kriminalite – požehnanie alebo prekliatie?
11	Počítačová kriminalita ohrozuje všetky aspekty biznisu
15	Detekčné metódy
18	Páchatelia ekonomickej kriminality
18	Aký je typický profil páchatela podvodu?
19	Čo je hlavným motivačným faktorom hospodárskej kriminality?
20	Etika & Compliance
23	Budúcnosť hospodárskej kriminality – realita hospodárskej kriminality verzus vnímanie rizika
24	Kontakty

Globálny prieskum hospodárskej kriminality, ktorý uskutočňuje spoločnosť PwC, je najväčší svojho druhu. V ročníku 2016 sa na ňom zúčastnilo 6 337 respondentov zo 115 krajín, vrátane 89 reprezentantov zo Slovenska.

Zámerom prieskumu nie je iba zistiť súčasný stav hospodárskej kriminality, ale aj identifikovať trendy a vývoj rizík v budúcnosti.

Predslov

Radi by sme prezentovali výsledky Globálneho prieskumu hospodárskej kriminality za rok 2016, ktorý vykonala spoločnosť PwC. Tak ako v minulých rokoch, aj tento rok je prieskum spoločnosti PwC najväčším a najkomplexnejším prehľadom údajov o hospodárskej kriminalite nielen vo svete, ale aj na Slovensku. Na to, aby sme dokázali čo najlepšie zmapovať súčasný stav hospodárskej kriminality, jej povahu a vnímanie zo strany spoločností, snažili sme sa skontaktovať čo najviac respondentov. V tomto roku sa zapojilo 6 337 organizácií zo 155 krajín, vrátane 89 spoločností zo Slovenska.

Hlavnou témou pre tento rok je počítačová kriminalita, ktorá bola v minulosti vnímaná ako úplne nová forma kriminality, no v dnešnom podnikateľskom prostredí sa stáva súčasťou stále väčšieho podielu prípadov a diskusií. V dnešnom svete nie je žiadna zo spoločností imúnna voči počítačovej kriminalite. Tento typ kriminality postihuje spoločnosti bez ohľadu na odvetvie, v ktorom podnikajú, ale aj miesto, kde sú registrované. Okrem témy počítačovej kriminality sa prieskum zameriava aj na princípy etického podnikania a dodržiavanie regulačných nariadení. Správne plnenie regulačných opatrení v podnikateľskom prostredí, ktoré sa čoraz viac globalizuje, je stále náročnejšie a stáva sa hlavnou otázkou mnohých spoločností.

Globálny prieskum hospodárskej kriminality sa tiež zaoberá témou „**príležitostí**“. Nie sú to len príležitosti, ktoré prispievajú k hospodárskej kriminalite, ale skôr také príležitosti, ktoré prinášajú proaktívnu prevenciu a pritom nekladú nadmernú záťaž na právnu zodpovednosť organizácie.

Naša správa si kladie za cieľ zlepšenie celkového povedomia o téme hospodárskej kriminality. Myslíme si, že výsledky prieskumu zlepšia povedomie ohľadom tohto fenoménu a prispedia k tomu, aby organizácie vedeli správne zhodnotiť riziko, ktoré im hrozí, aké môže mať materiálne dopady na ich pôsobenie a ako sa účinne brániť.

Globálny prieskum hospodárskej kriminality sa zameriava nielen na lokálne trhy, v tomto prípade Slovensko, ale predstavuje súhrnný dokument pokrývajúci globálne prostredie, ktorý je určený pre spoločnosti s celosvetovým pôsobením.

Na záver by sme sa chceli poďakovať všetkým respondentom za čas, ktorý nám venovali a za to, že boli ochotní s nami zdieľať svoje skúsenosti z praxe. Naše poďakovanie patrí najmä slovenským spoločnostiam za ich príspevky.

Sirshar Qureshi,

Partner zodpovedný za Forenzné služby v rámci Strednej a východnej Európy, PwC

Hlavné zistenia

Súčasný stav hospodárskej kriminality na Slovensku

Hospodárska kriminalita je stále vážny problém ovplyvňujúci spoločnosti na svete, v krajinách strednej a východnej Európy ("Stredná a východná Európa") a na Slovensku. Na Slovensku sa za posledných 24 mesiacov viac ako tretina (34%) respondentov stretla s jedným alebo viacerými prípadmi hospodárskej kriminality. Výskyt hospodárskej kriminality je porovnateľný s priemerom za Strednú a východnú Európu (33%) a s celosvetovým priemerom (36%).

V porovnaní s predchádzajúcim prieskumom je výskyt hospodárskej kriminality rovnaký. To však neznamená, že podnikateľské prostredie je stabilné. Prostredie, v ktorom organizácie pôsobia sa vyvíja, čo sa týka rizika a preto môžu niektoré prípady hospodárskej kriminality zostať neodhalené aj niekoľko rokov. Tieto skryté, avšak dlhodobé podvody, sú nebezpečnejšou a nákladnejšou hrozbou ako jednorázový podvod.

Už tradične najčastejším typom hospodárskej kriminality na Slovensku je sprenevera majetku (67%). Spreneveru majetku je jednoduchšie odhaliť v porovnaní s ostatnými druhmi hospodárskej kriminality. Preto je častý výskyt sprenevery v prieskume očakávaný.

Okrem sprenevery majetku ďalších päť najčastejších typov podvodov zahŕňa počítačovú kriminalitu (13%), podvod v nákupnom procese (20%), korupciu a úplatkárstvo (23%), insider trading a úverový podvod (každý po 10%).

Väčšina prípadov podvodov na Slovensku je odhalená pomocou rôznych typov firemných kontrol (spolu 61%). Zhruba jeden z piatich prípadov je odhalený spôsobom mimo pôsobnosti manažmentu spoločnosti. Z toho 11% je odhalených na základe tipu z vonkajšieho prostredia firmy.

Podľa prieskumu z roku 2016 má väčšinu spáchaných podvodov na svedomí interný páchatel' (52%) v porovnaní s prípadmi spáchanými osobami mimo firmy.



Na Slovensku sa za posledných 24 mesiacov viac ako tretina (34%) respondentov stretla s jedným alebo viacerými prípadmi hospodárskej kriminality.

Počítačová kriminalita

Približne 13% z tých respondentov, ktorí sa na Slovensku stretli s hospodárskou kriminalitou uviedlo, že išlo o počítačovú kriminalitu. Toto číslo je výrazne pod priemerom krajín strednej a východnej Európy ako aj globálnym priemerom. Ponaučenie, ktoré by sme si mali odniesť, je zmena vo vnímaní počítačovej kriminality nielen ako IT problému, ale ako základného problému podnikania.

Podľa našich predchádzajúcich prieskumov si počítačová kriminalita udržuje stabilný trend. Je to protichodný výsledok, ak vezmeme do úvahy meniace sa podnikateľské prostredie, kde je väčšina dokumentov, komunikácie a transakcií digitálna.

Slovenskí respondenti považujú počítačovú kriminalitu za druhú najväčšiu hrozbu (17% respondentov) po sprenevere majetku a jej výskyt

v priebehu najbližších 24 mesiacov považujú za pravdepodobný. Toto vnímanie rizika je nižšie v porovnaní so Strednou a východnou Európou (25%) aj so svetom (34%). Na druhej strane si 58% spoločností myslí, že riziko vzrástlo.

V dôsledku rýchlej zmeny technologického procesu sa tradičné vnímanie počítačovej kriminality rozšírilo. K systémom, ktoré sú ohrozené počítačovou kriminalitou, patria aj mobilné telefóny, prístroje pripojené na cloud, automobily a prístroje v domácnosti.

Z finančného hľadiska je počítačová kriminalita veľmi nákladná. Za posledné dva roky stratila jedna štvrtina oslovených spoločností vo svete viac než 44 tisíc EUR v dôsledku počítačovej kriminality.



Približne 13% z tých respondentov, ktorí sa na Slovensku stretli s hospodárskou kriminalitou uviedlo, že išlo o počítačovú kriminalitu.

Etika a compliance

V prieskume sa korupcia a úplatky umiestnili ako druhý najčastejší druh hospodárskej kriminality. Približne 8% spoločností uviedlo, že boli požiadané o zaplatenie úplatku za posledných 24 mesiacov. Výsledok je výrazne nižší v porovnaní so Strednou a východnou Európou (17%) a globálnym priemerom (13%).

Pozitívna správa je, že 80% z oslovených spoločností má formálne nastavený etický a compliance program, čo je tesne pod priemerom za krajiny strednej a východnej Európy a celosvetovým priemerom (obidva po 82%).



Približne 8% spoločností uviedlo, že boli požiadané o zaplatenie úplatku za posledných 24 mesiacov.

Až 90% z tých spoločností odpovedalo, že si myslia, že ich etický kódex pokrýva kľúčové riziká/smernice a udáva hodnoty spoločnosti. Pre 92% respondentov platí, že hodnoty sú nastavené jasne a sú pochopené zamestnancami. Viac ako polovica spoločností (57%) organizuje pravidelné školenia k obsahu etického kódexu.

Tieto relatívne vysoké výsledky naznačujú, že firmy na Slovensku majú zavedený primeraný Etický kódex. Porozumenie etických princípov zamestnancami a komunikácia naprieč firmou sú kľúčovými prvkami, ktoré prispievajú k efektívnej funkcii compliance. Všetci účastníci uviedli, že sú im odporúčané pravidelné školenia.

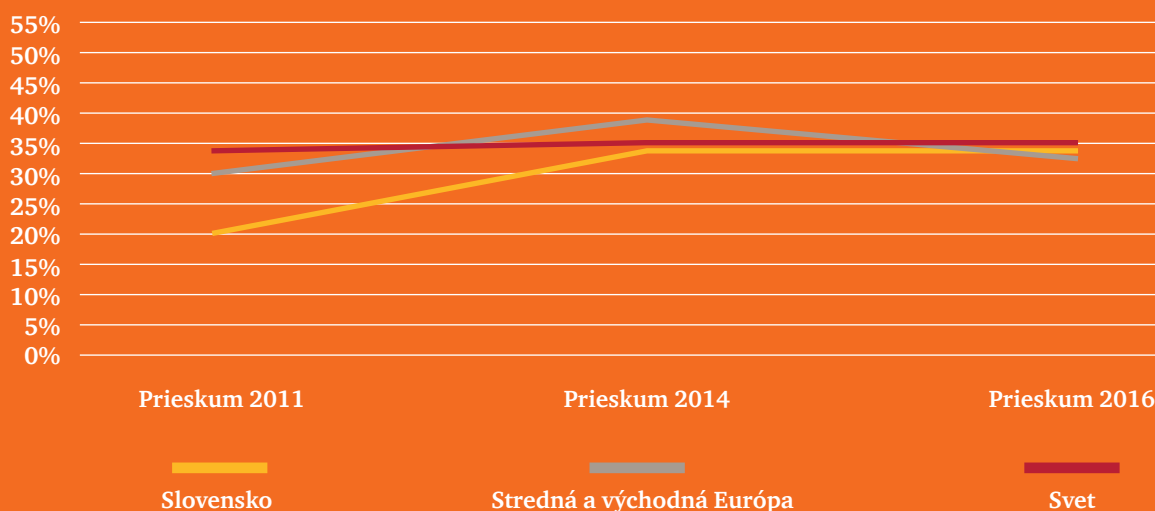
Hospodárska kriminalita na Slovensku

Hospodárska kriminalita ako nezadržateľná hrozba Koľko spoločností čelilo podvodom za posledné dva roky?

Hospodárska kriminalita je stále hlavným dôvodom na obavy pre organizácie bez ohľadu na ich veľkosť, oblasť podnikania, či vlastnícku štruktúru. Viac ako jedna tretina (34%) respondentov zo spoločností na Slovensku má za uplynulé dva roky skúsenosť s hospodárskou kriminalitou. V porovnaní s krajinami

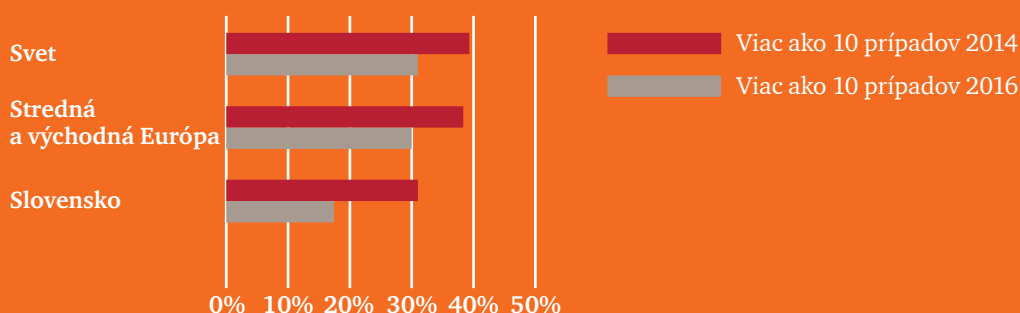
strednej a východnej Európy, z ktorých 33% vykazuje výskyt hospodárskej kriminality, na Slovensku dochádzalo k podvodom častejšie. Tento výsledok môžeme vnímať čiastočne ako pozitívny, keďže došlo k poklesu oproti výsledkom z roku 2014. Na druhej strane, od roku 2011 sme zaznamenali rastúci trend.

Výskyt podvodov



Viac ako 10 individuálnych prípadov uviedlo 17% spoločností, ktoré sa stretli s hospodárskou kriminalitou oproti 31% spoločností, ktoré mali takúto

skúsenosť v roku 2014. Výsledky sú výrazne nižšie v porovnaní so Strednou a východnou Európou (30%) aj s globálnymi výsledkami (31%).



Akým druhom hospodárskej kriminality čelia slovenské spoločnosti?

Najčastejším typom hospodárskej kriminality je sprenevera majetku, ktorú označilo až 67% spoločností. Po sprenevere majetku nasleduje úplatkárstvo a korupcia (23%), podvody v nákupnom procese (20%), počítačová kriminalita (13%), insider trading (zneužitie dôverných informácií) a úverové podvody (oboje po 10%).

Pri väčšine typov hospodárskej kriminality vidíme pokles v porovnaní s výsledkami predchádzajúceho prieskumu. Jedinou výnimkou sú kybernetická kriminalita a účtovné podvody.

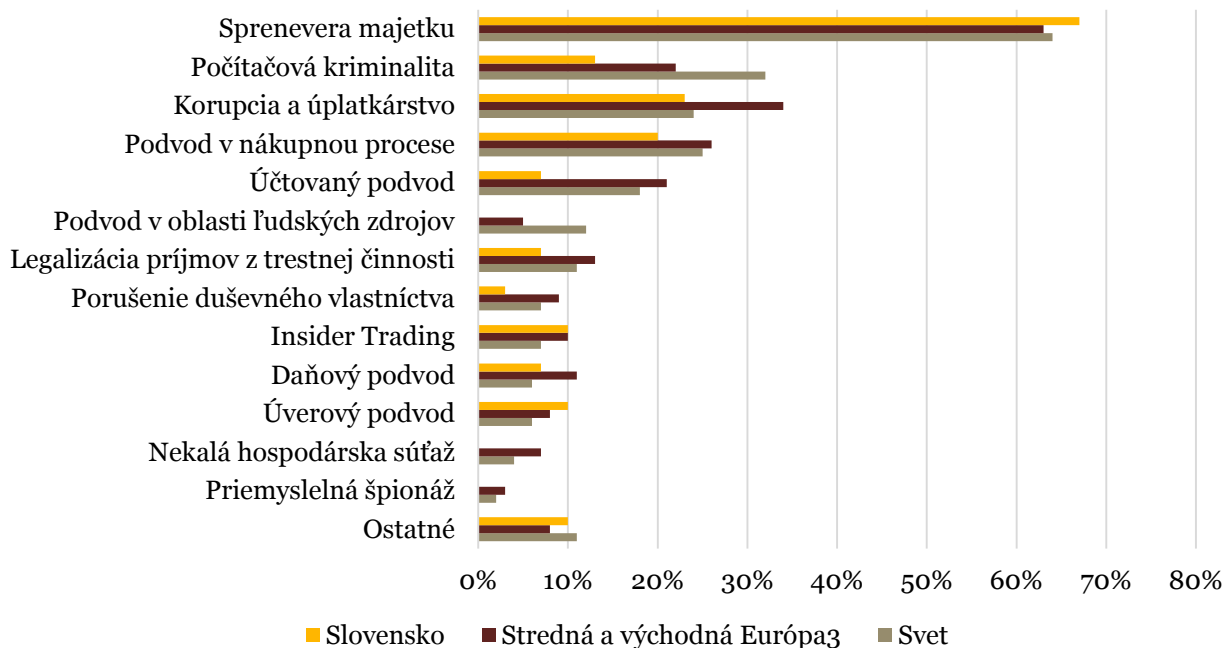
67%

Každoročne sa na prvom mieste umiestňuje sprenevera majetku. Takéto umiestnenie je ľahko predvídateľné vzhľadom na fakt, že sprenevera majetku je najjednoduchšie odhaliteľná.

Výsledky slovenského prieskumu ukazujú viac-menej rovnakú úroveň hospodárskej kriminality ako je priemer v krajinách strednej a východnej Európy a svetový priemer. Počítačová kriminalita je na Slovensku nižšia v porovnaní s krajinami strednej

a východnej Európy a globálnymi výsledkami. Korupcia a úplatkárstvo sa ukazujú ako závažnejší problém, keď porovnáme Slovensko s priemerným výskytom v rámci Strednej a východnej Európy.

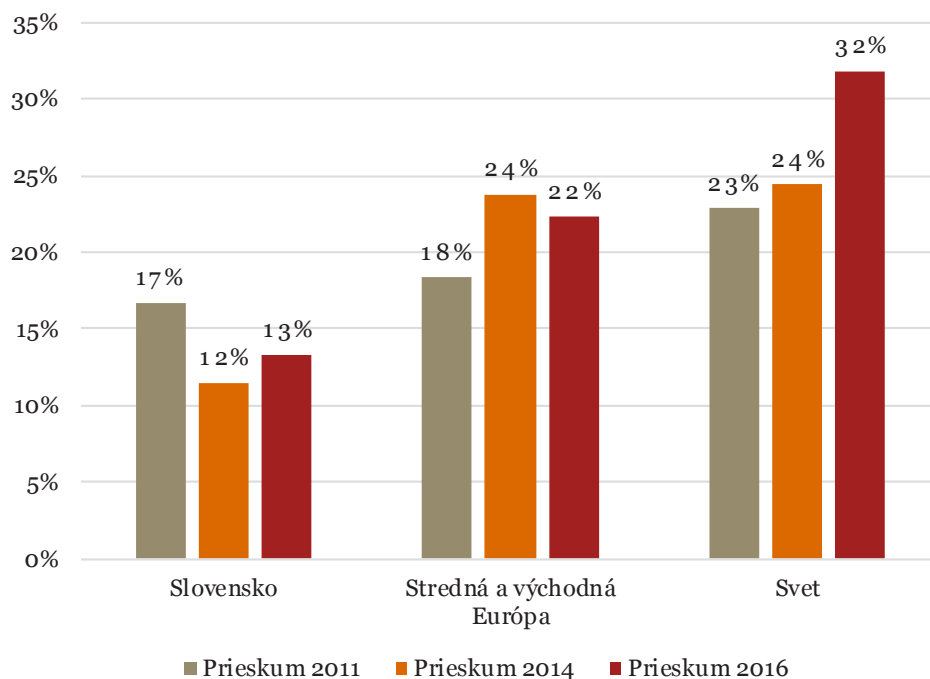
Typ podvodu



Počítačová kriminalita

Počítačová kriminalita na Slovensku vzrástla v porovnaní s rokom 2014, stále sa však drží pod hodnotami Strednej a východnej Európy aj pod svetovými hodnotami.

Vývoj počítačovej kriminality

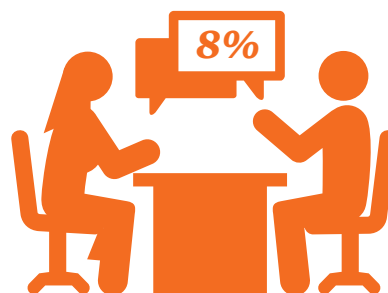


Korupcia a úplatkárstvo

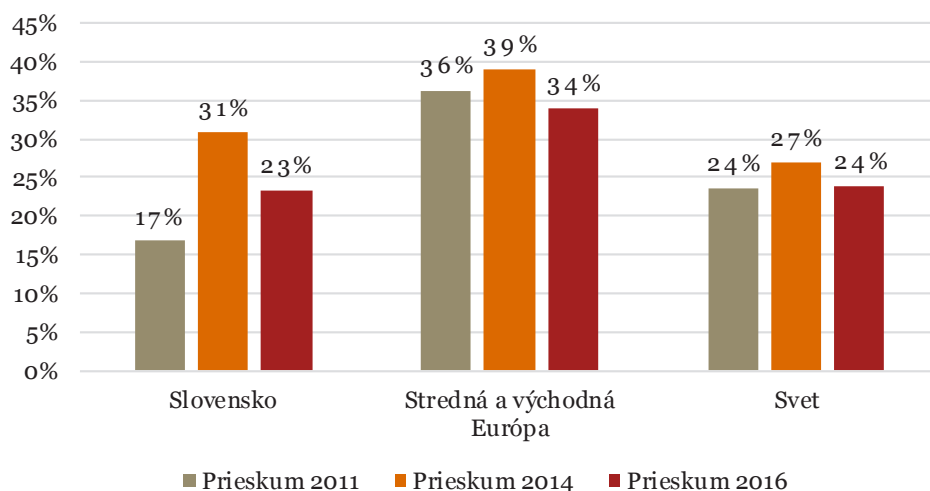
Napriek tomu, že prieskum ukazuje na pokles korupcie a úplatkov na Slovensku (z 31% v 2014 na 23% v 2016), v Strednej a východnej Európe a celosvetovo, korupcia stále zostáva závažným problémom od sledovaní v roku 2011.

Účastníci prieskumu na Slovensku uviedli, že v uplynulých 24 mesiacoch boli požiadaní, aby zaplatili úplatok (8%) a sú toho názoru, že stratili príležitosť oproti konkurencii, ktorá úplatok bola ochotná zaplatiť (22%). Tohtoročné výsledky poukazujú na výrazný pokles v porovnaní s predchádzajúcim vydaním prieskumu (o 12 a 19 percentných bodov v porovnaní s minulými prieskumami).

Klesajúci trend sa zdá byť optimistický. Musíme však byť opatrní pri vyvodzovaní záverov, keďže aktuálny stav korupcie a úplatkárstva môže byť oveľa horší. Na základe našich skúseností je korupcia a úplatkárstvo ťažko odhaliteľný typ hospodárskej kriminality. Vnímanie toho, čo je korupcia a úplatkárstvo môže byť veľmi individuálne naprieč spektrom spoločností. Správanie, ktoré jedna spoločnosť považuje za bežné obchodné praktiky môže iná spoločnosť považovať už za prekročenie hranice korupcie a úplatkárstva.



Korupcia a úplatkárstvo



Koľko stojí podvod?

Počítačová kriminalita na Slovensku vzrástla v porovnaní s rokom 2014, stále sa však drží pod hodnotami Strednej a východnej Európy aj pod svetovými hodnotami.



Respondenti z nášho prieskumu zaznamenali širšie škody ako straty z prerušenia činnosti, náklady spojené so zavádzaním nápravných opatrení, vyšetrovaním podvodov a preventívnymi opatreniami, pokutami od regulátorov, či právnymi poplatkami. Kritické sú náklady spojené s poškodením morálky a reputácie, keďže majú vplyv na dlhodobé obchodné výsledky. Tieto straty nie sú vždy vyčísliteľné a môžu v priebehu času prevýšiť priamu krátkodobú stratu spôsobenú podvodom.

Dôsledky hospodárskej kriminality neznamenia pre spoločnosti len finančné straty. Polovica z oslovených spoločností uviedla dopad na morálku zamestnancov a v 31% prípadov došlo k poškodeniu obchodných vzťahov v dôsledku výskytu podvodu v organizácii.



Technológia v hospodárskej kriminalite – požehnanie alebo prekliatie?

Počítačová kriminalita ohrozuje všetky aspekty biznisu

Nie je prekvapením, že v digitálnom prostredí, aké je v súčasnosti bežné, je výskyt počítačovej kriminality rastúci. Od roku 2011, kedy bola počítačová kriminalita v našom prieskume po prvýkrát uvedená ako samostatná kategória, sa frekvencia jej výskytu mení (17% v roku 2011 v porovnaní s 12% v 2014 a 13% v 2016). 17% spoločností tvrdí, že boli nejakým spôsobom ovplyvnené počítačovou kriminalitou. Výsledok je tesne pod výsledkami za Strednú a východnú Európu a globálnym priemerom (22% a 26%).

Nárast počítačovej kriminality popísaný v predchádzajúcom odseku je takisto podporený vnímaním rizika. Niečo viac než polovica slovenských spoločností (58%) uvádza, že podľa ich názoru riziko počítačovej kriminality vzrástlo.

Poškodenie reputácie spoločnosti, krádež alebo strata osobných údajov a prerušenie činnosti sú globálne najobávanejšími dôsledkami počítačovej kriminality. Počítačová kriminalita je finančne nákladná. Celosvetovo jedna štvrtina spoločností stratila za posledných 24 mesiacov viac ako 44 tisíc EUR v dôsledku počítačovej kriminality.

V najbližších 24 mesiacoch očakávajú slovenské spoločnosti hrozbu počítačovej kriminality z externého prostredia (47%). Napriek tomu, že spoločnosti považujú počítačovú kriminalitu za hrozbu:

23% respondentov uvádza, že ich spoločnosti nepripravujú žiadne správy ohľadom pripravenosti na možný kybernetický útok.

22% respondentov uvádza, že nevie, či sú v ich spoločnosti takéto informácie požadované a pripravované.

Je alarmujúce, že takmer polovica spoločností nemá správy o pripravenosti na útok, ak berieme do úvahy rastúcu tendenciu výskytu počítačovej kriminality.

Výsledky prieskumu ukazujú, že 51% slovenských spoločností má pripravený plán pre prípad kybernetického útoku. Toto číslo je vysoko nad pripravenosťou spoločností v Strednej a východnej

Európe (36%) aj vo svete (37%). Na druhej strane, niektoré spoločnosti stále nie sú na možný útok adekvátne pripravené. 17% spoločností na Slovensku nemá pripravený žiadny plán a ani ho neplánuje pripraviť. V porovnaní s 13% slovenských spoločností, ktoré boli obeťou počítačovej kriminality, je ďalšia štvrtina spoločností bez funkčného plánu.

Vnímanie rastu rizika počítačovej kriminality

58%
Slovensko

44%
*Stredná
a východná
Európa*

53%
Svet



Viac ako polovica zúčastnených spoločností na Slovensku (60%) má celkovo vyškolený tím, ktorý je schopný v prípade potreby zasiahnuť a riešiť narušenie IT prostredia. Číslo sa síce môže zdať vysoké, ale ak vezmeme do úvahy neustále zmeny v digitálnom

prostredí a skutočnosť, že žiadna spoločnosť nie je imúnna voči kybernetickým útokom, spoločnosti stále majú na čom pracovať, aby obmedzili riziko negatívneho dopadu prípadných útokov.

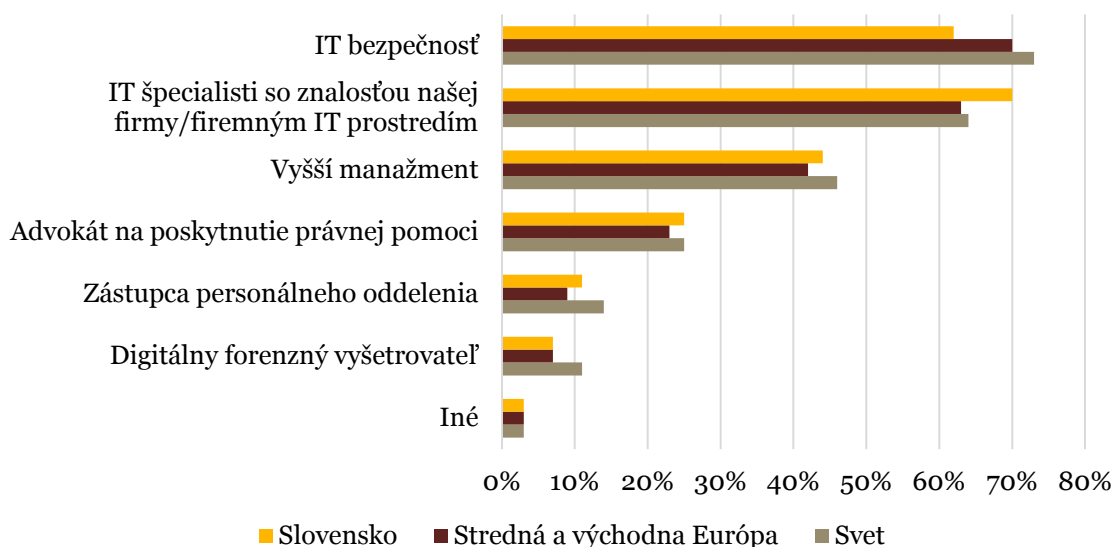
Schopnosť mobilizácie v prípade narušenia IT prostredia



Vyškolený tím, ktorý je schopný v prípade potreby zasiahnuť, je väčšinou zložený z ľudí so špecializáciou v IT bezpečnosti, informatikov, vyššieho manažmentu a právnika. Zo slovenských, regionálnych a celosvetových výsledkov vyplýva, že iba malý počet všetkých tímov má člena, ktorý je špecializovaný digitálny forenzný vyšetrovateľ (po 7% na Slovensku a v Strednej a východnej Európe a 10% celosvetovo).

Neadekvátne zloženie tímov a pochopiteľná snaha o rýchle vyriešenie problému môže viesť k vyššiemu riziku, že tím prehliadne niektorý potenciálne zásadný dôkaz. Toto môže viesť k zhoršenej schopnosti spoločnosti porozumieť, kde došlo k pochybeniu a jej schopnosti žalovať páchatelov.

Zloženie zásahového tímu



Rozhovor

Pavol Adamec

Direktor, Riadenie rizík a informačné technológie



Ako sa kybernetické podvody vyvíjali v poslednej dobe?

Celý svet aktuálne pôsobí a vykonáva takmer všetky svoje aktivity prostredníctvom informačných a komunikačných technológií („ICT“). Komplexnosť riešení a množstvo dát a výkon hardwaru sa každým rokom zvyšujú. Kybernetické podvody sa vyvíjajú rovnakým tempom. Napríklad kvôli klesajúcim cenám výpočtovej techniky sú v súčasnosti bežné postupy, ktoré pred časom neboli možné. Z tohto dôvodu môžu nastať komplexnejšie scenáre. Je dôležité uvedomiť si, že páchatelia podvodov môžu používať tie isté technológie ako vy a vo väčšine prípadov aj tak robia, a sú v ich používaní veľmi dobrí. Je pomerne bežné, že použijú pokročilú analytiku, ako napríklad učiaci sa algoritmus na simulovanie správania sa bežného zákazníka.

Ktoré sú najkritickejšie oblasti kybernetických podvodov?

Najkritickejšou oblasťou sú prevody peňazí. Najčastejšie kybernetické podvody sa týkajú krádeže peňazí. Spôsob podvodu sa odlišuje aj z podnikateľského hľadiska (môže ísť o mankú v sklade kvôli manipulácii so záznamami v sklade, zmeny bankových účtov v nákupnom alebo mzdovom systéme, rozvrstvenie transakcií (layering), ukradnutie totožnosti kvôli získaniu prístupu k bankovým účtom, atď.). Druhou kritickou oblasťou je priemyselná špionáž a poškodenie reputácie. Existujú skupiny, ktorých cieľom je poškodiť vašu povesť pretože ich na to najala vašou konkurenciou. Všeobecne je ich cieľom zlepšiť si pozíciu na trhu, ktorá bude viesť k nárastu zisku. Priemyselná špionáž sa v súčasnosti vo veľkom spolieha na takzvaný cyber intelligence.

Aké technológie sa v súčasnosti najčastejšie používajú v kybernetických podvodoch?

Kybernetické podvody aktuálne môžu v sebe zahŕňať akúkoľvek dostupnú technológiu. Je to otázka použitia a zámeru páchatela, ako danú technológiu použije. Môže ísť o široké spektrum možností, od špeciálnej frázy vo verejne dostupnom vyhľadávacom až po vysoko sofistikované hackovacie techniky, ktoré zvyčajne obsahujú prvky social engineeringu. Dôležitým faktom je, že množstvo technológií rastie a ako je uvedené vyššie, aj komplexnosť a množstvo funkcií

v zariadeniach sa z roka na rok zvyšuje. Preto sa kybernetický podvod netýka len počítačov. Takmer každý mobilný telefón má prístup do internetového bankovníctva. Podobne aj prenosné technológie umožňujú komunikáciu s inými zariadeniami. Operačné systémy sú súčasťou televízií a domácich kín. Máte operačný systém v herných konzolách aj autách a ako sa približujeme k ére smart domácností, počet zariadení, ktoré môžu byť použité na kybernetický podvod a počítačovou kriminalitu, rastie.

Ako postupovať, keď sa niečo stane v mojej organizácii?

Záleží na vyspelosti procesov vo vnútri firmy, kontrolách, systémoch a pripravenosti na takýto incident. Na základe našich skúseností, každý podvod zanechá špecifickú stopu, ktorá môže byť odhalená v systémových dátach bez ohľadu na to, či išlo o jednorazový, alebo opakujúci sa podvod. Sme schopní analyzovať dáta (tak štruktúrované, ako aj neštruktúrované), nájsť tieto stopy a vyšetriť ich. Pomáhame zákazníkovi s prevenciou a poskytujeme celkovú podporu počas riešenia nepríjemnej situácie a v období po incidente.

Je možné robiť niečo lepšie, aby sa zabránilo kybernetickému podvodu alebo aspoň byť pripravený, keď dôjde k incidentu?

Stále je šanca robiť veci lepšie, záleží predovšetkým na type vášho biznisu. Za bežných okolností, podvodné konanie vzniká z nesprávneho nastavenia procesov v spoločnosti, zlou disciplínou zamestnancov a ignorovaním rizika podvodu. Pravidelné používanie systémov a dodržiavanie interných a externých smerníc a procedúr je nutnosťou. Ak vo firme funguje pravidelný systém hodnotenia rizík, potom ste schopní odhaliť slabé miesta a zamerať sa na ne. Ak ste z medzinárodnej firmy, môžete vidieť presúvanie sa rizika z jedného na druhý kontinent, z krajiny do krajiny a preto môžete reagovať skôr, než situácia nastane u vás. Navyše, môžete použiť pokročilé systémy na rozpoznanie vzorov správania, podozrivých aktivít, predpovedať incident. Tieto systémy dokážu spracovať a využiť dáta, ktoré už v systéme máte, (štruktúrované i neštruktúrované) a tým zvýšiť úroveň ochrany a pripravenosť. U nás, v PwC, poskytujeme podporu na základe dlhoročných skúseností a overenej kvality.

Detekčné metódy

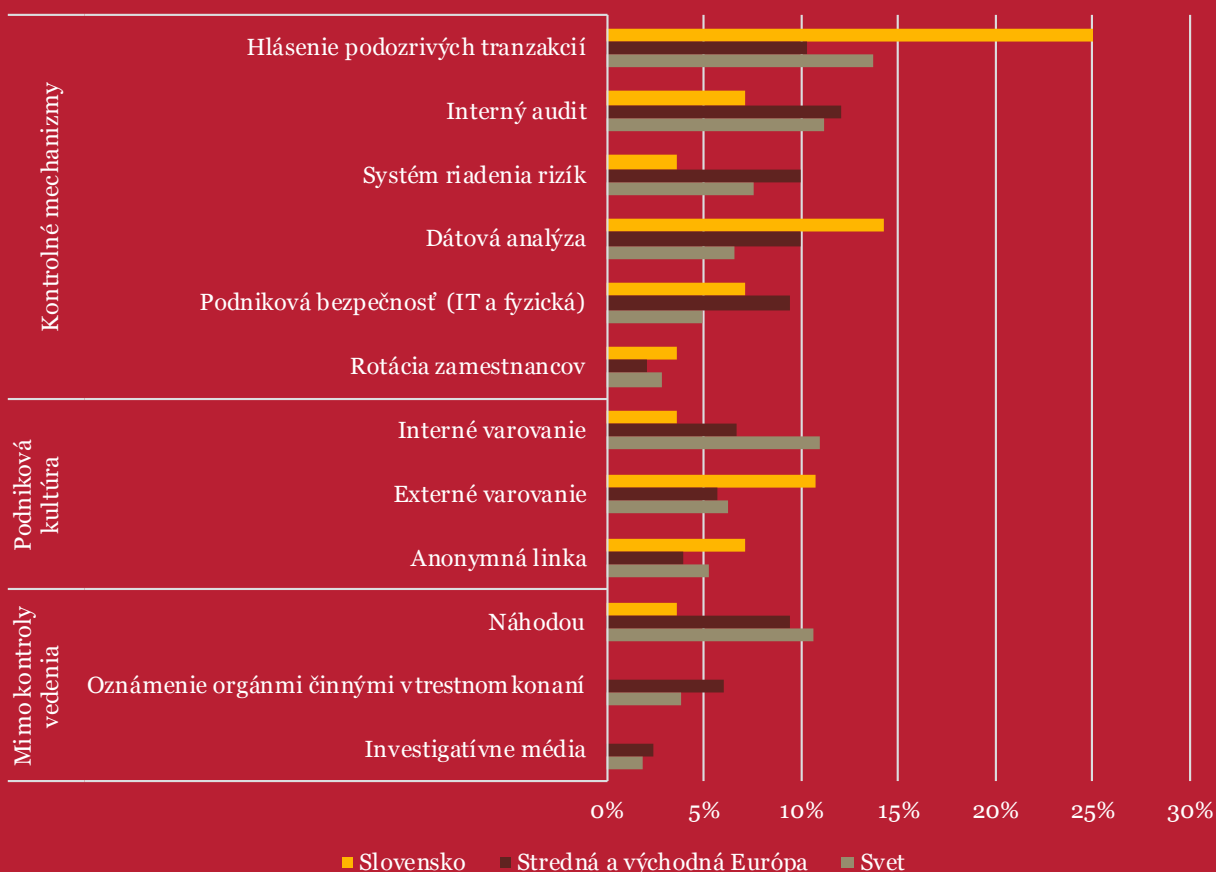
Pozitívnym zistením je, že stále väčšie množstvo podvodov sa odhalí cez systémové mechanizmy (55% prípadov v roku 2014 v porovnaní s 61% v 2016). Viac ako polovica, 61% slovenských respondentov odpovedalo, že bol u nich odhalený podvod pomocou firemných kontrol (v porovnaní s 54% v Strednej a východnej Európe a 47% celosvetovo).

Predovšetkým by sme radi zdôraznili rastúci podiel dátových analýz (nárast z 5% v roku 2014 na 14% v roku 2016) a monitoringu podozrivých transakcií (nárast z 8% na 25%). V meniacom sa podnikateľskom prostredí a prípadoch, keď rôzne podvody zanechávajú rozličné elektronické stopy, môžu byť tieto detekčné metódy veľmi užitočným nástrojom. Navyše, keď sú tieto procesy zautomatizované, môžu bežať v reálnom čase bez ľudských zásahov alebo s veľmi limitovanou nutnosťou na zásah. Na druhej strane, použitie „tradičných“ detekčných metód, ako je riadenie rizika podvodu (4%) a interný audit (7%), je podľa výsledkov na Slovensku nižšie v porovnaní so Strednou a východnou Európou (10% a 12%) a svetom (8% a 11%).

Napriek povzbudivému výsledku by sme nemali zaspáť na vavrínoch. Podľa účastníkov prieskumu je na Slovensku stále 18% spoločností, kde bola hospodárska kriminalita odhalená mimo poľa pôsobnosti manažmentu. Najčastejšie v tejto kategórii dostal manažment externé varovanie (11%). Vidíme priestor na zlepšenie detekčných metód v oblasti firemnej kultúry.

Anonymná informačná linka bola detekčnou metódou v 7% prípadov. Len 34% slovenských firiem pripravuje správy z podaní na anonymnej linke. Efektívny systém podaní na anonymné linky môže byť účinným nástrojom v boji s hospodárskou kriminalitou, ale takisto je aj súčasťou zdravého etického podnikateľského prostredia.

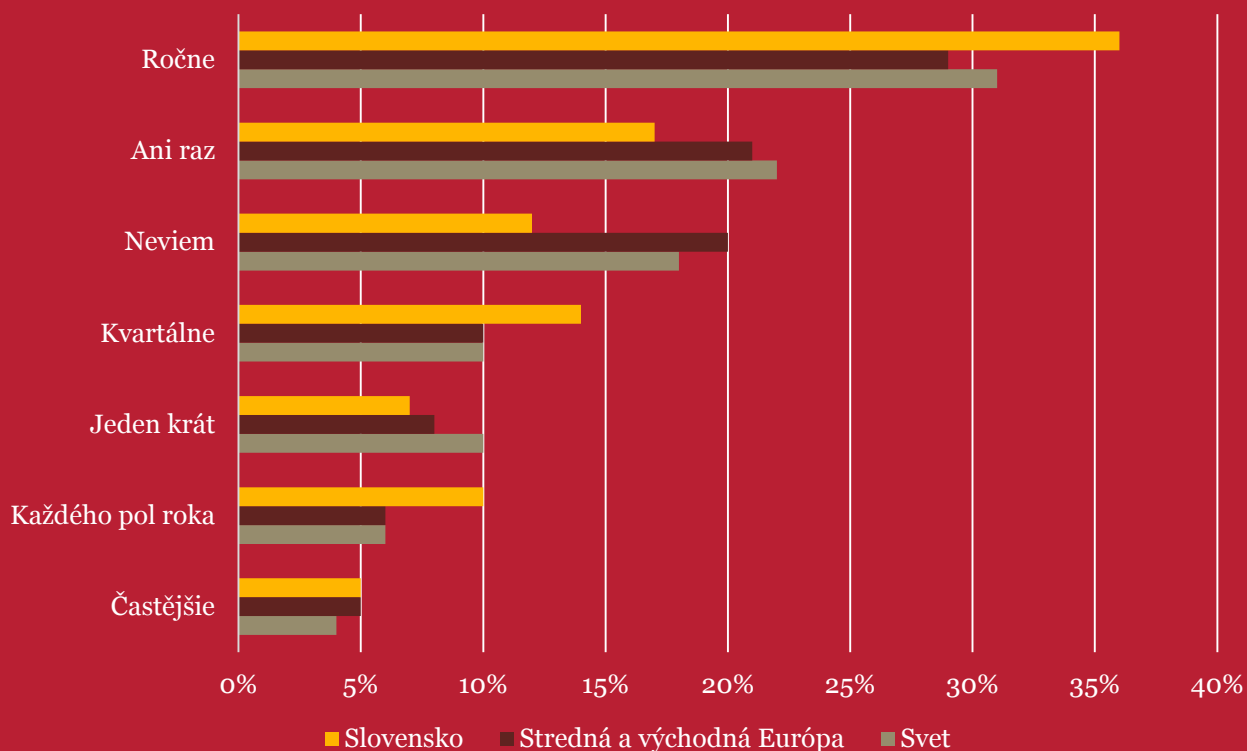
Detekčné metódy



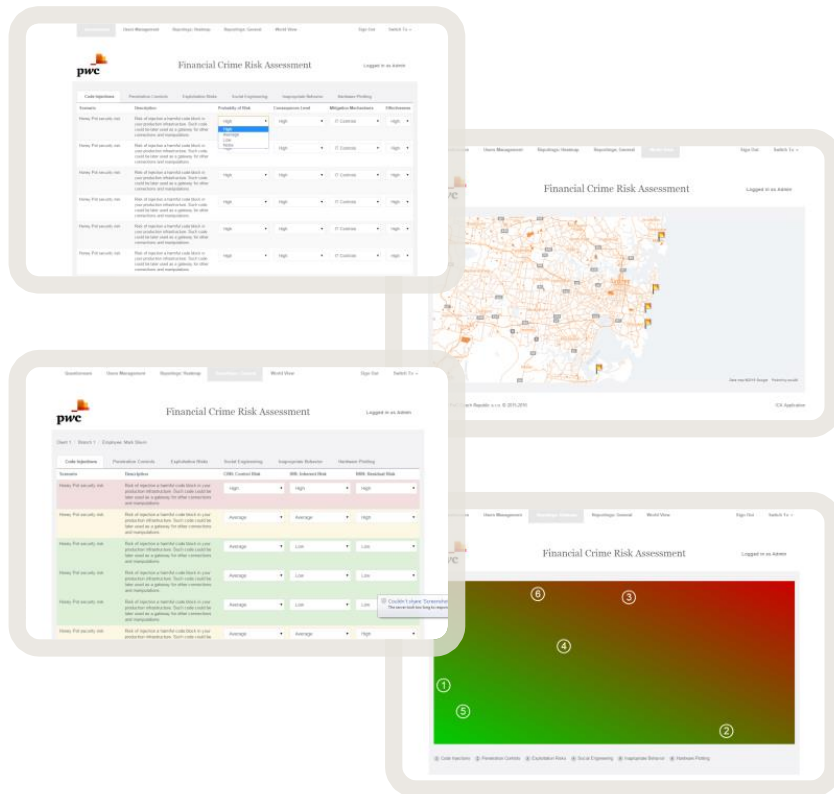
Viac ako polovica (64%) respondentov má zavedený systém riadenia rizík a použilo ho aspoň raz ročne. Toto zistenie je v súlade s hore uvedenými detekčnými metódami. Výsledky získané na Slovensku sú vyššie ako výsledky za Strednú a východnú Európu a svet (50% and 51%). Ďalších 7% slovenských spoločností (8% v krajinách strednej a východnej Európy a 10% celosvetovo) použilo v uplynulých 24 mesiacoch systém riadenia rizík.

Približne tri štvrtiny spoločností, tak na Slovensku, ako aj v Strednej a východnej Európe a celosvetovo, používajú interné zdroje na vyšetrovanie identifikovaných prípadov hospodárskej kriminality, zatiaľ čo jedna tretina spoločností aj kontaktuje právneho zástupcu. Ostatné osoby, na ktoré sa spoločnosti zvyčajne obrátia, sú externí audítori, prípadne si najmú špecializovaného forenzného vyšetrovateľa. Len 10% slovenských spoločností, ktoré sa stretli s kriminalitou, kontaktovalo forenzného vyšetrovateľa. Globálne toto percento dosahuje 20% hranicu. Pomerne prekvapivo, 7% slovenských spoločností (10% v Strednej a východnej Európe a 11% celosvetovo) volí ako odpoveď na zistenú hospodársku kriminalitu vyčkávanie, či sa podobné indikátory potenciálneho podvodu objavia v rovnakej oblasti aj neskôr.

Systém riadenia rizík za posledných 24 mesiacov



Príklad ako môže vyzerat' výstup zo systému riadenia rizík



Znaky efektívnej anonymnej linky

- Súčasť etického a compliance programu spoločnosti
- Rôznorodé druhy komunikácie (napríklad špeciálna telefónna linka, emailová schránka, kontaktné pracovisko) na uľahčenie prístupu a jednoduché na použitie všetkými zamestnancami a oznamovateľmi mimo organizáciu)
- Anonymita a dôvera
- Ochrana oznamovateľa voči pomste
- Komunikácia a vzdelávanie
- Pozitívny príklad vedenia
- Analýza prijatých podnetov a príprava štatistík
- Zverejňovanie vyriešených podnetov
- Možnosť vonkajšieho poskytovateľa

Páchatelia hospodárskej kriminality

Aký je typický profil páchatela podvodu?

Historicky, páchatelia pochádzali z externého a interného prostredia, viac-menej rovnakým pomerom. Tohtoročný prieskum na Slovensku naznačuje, že interný páchatel podvodu bol častejší (52%) oproti externému (38%). Zvyšné oslovené organizácie nevedeli, či bol páchatel zvnútra spoločnosti alebo z vonkajšieho prostredia.

V prípade, že išlo o externého páchatela, celosvetové výsledky ukazujú, že vo väčšine prípadov išlo o zákazníka (25%). Zákazníci mali vyšší podiel oproti zástupcom a sprostredkovateľom (títo viedli rebríček v predchádzajúcom prieskume, v roku 2014) alebo dodávateľom (po 17% a 10%).

Ako sa môžu spoločnosti brániť voči útokom z vonkajšieho prostredia? Jedno zo základných odporúčaní je preverenie si svojich obchodných partnerov. Skôr než spoločnosť začne s niekým obchodovať, mala by si osvojiť techniky nazývané corporate intelligence a due diligence. Tieto procedúry pomôžu spoločnostiam pri identifikovaní svojich obchodných partnerov a pri overení ich morálnej stránky a čestnosti. Akákoľvek negatívna správa z minulosti týchto obchodných partnerov môže indikovať prípadné problémy pre spoločnosť. Tieto procedúry by mali byť zavedené takým spôsobom, aby kontrolovali prípadný vývoj povesti obchodných partnerov v čase. Navyše, v súčasnosti pri množstve sankcií a vzrastajúcich požiadaviek regulačných orgánov sú tieto metódy odhaľujúce transparentnosť obchodných partnerov ešte dôležitejšie.

Profil interného páchatela



Profil externého páchatela

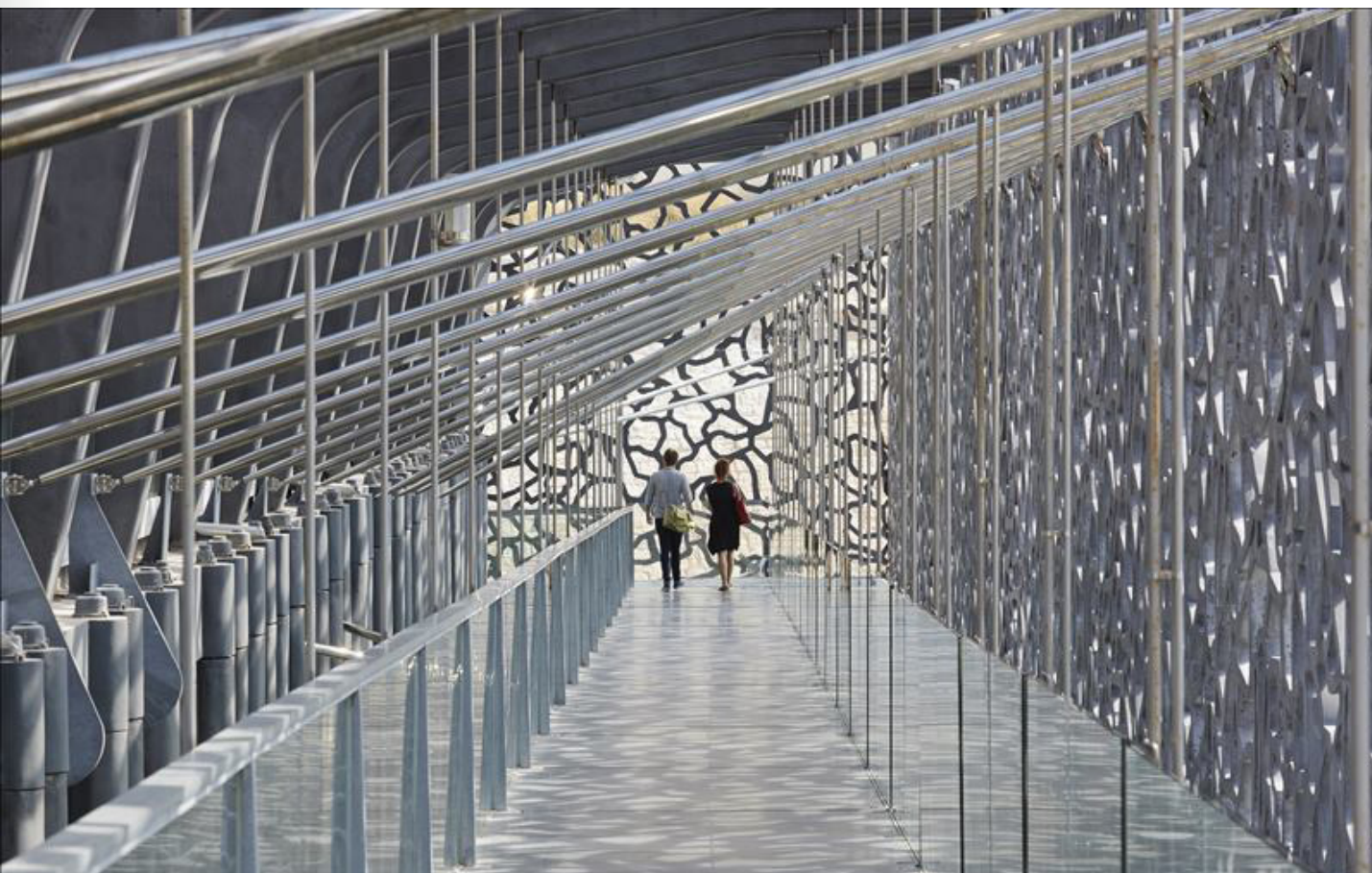
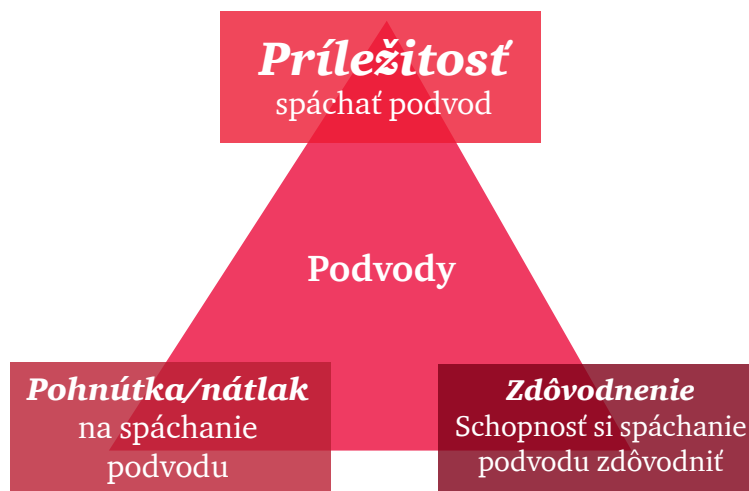


Čo je hlavným motivačným faktorom hospodárskej kriminality?

Keď sme sa pýtali respondentov, aký faktor podľa nich najviac prispel k hospodárskej kriminalite spáchanej interným páchatelom, tak nie prekvapujúco väčšina odpovedala, že hlavným motivátorom je príležitosť pre spáchanie podvodu.

Avšak príležitosť sama o sebe nie je dostatočným faktorom na to, aby bol podvod spáchaný. Páchatel musí mať pohnútku alebo nátlak podvod spáchať a musí byť schopný tento svoj čin zdôvodniť. Výsledky naznačujú, že spoločnosti považujú za najdôležitejší faktor príležitosť a pritom zabúdajú na význam ďalších dvoch faktorov.

V prípade, že kľúčový faktor je príležitosť spáchať podvod (globálne 69%), potom najlepším spôsobom ako predchádzať podvodom je posilnenie kontrol.



Etika & Compliance: Zladenie rizík a povinností s hodnotami a stratégiou v spoločnosti

Štyri základné oblasti záujmu na zlepšenie a zefektívnenie compliance programu



Ľudia a kultúra

Jasne nastavené procesy a pravidlá, kultúra, v ktorej je compliance pevne previazané s hodnotami a meraním a ocenením chceného správania.



Role a kompetencie

Formalizovaná compliance štruktúra a uistenie sa o správnom previazaní so súčasnými rizikami.



Oblasti s vysokým rizikom

Lepšia implementácia a testovanie v oblastiach vysoko rizikových trhov a oddelení.

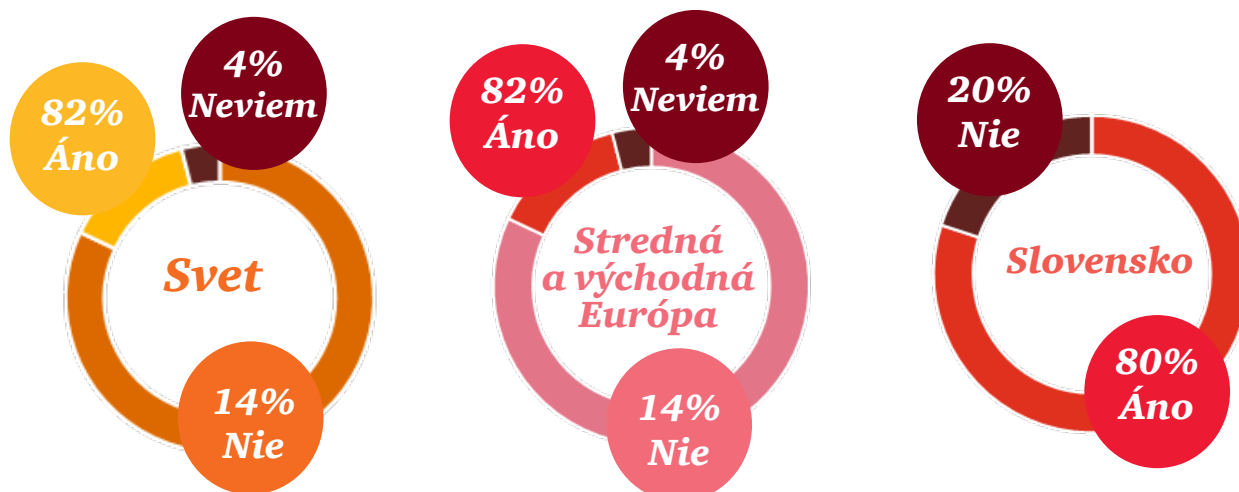


Technológie

Lepšie využitie detekčných a preventívnych nástrojov vrátane dátovej analýzy.

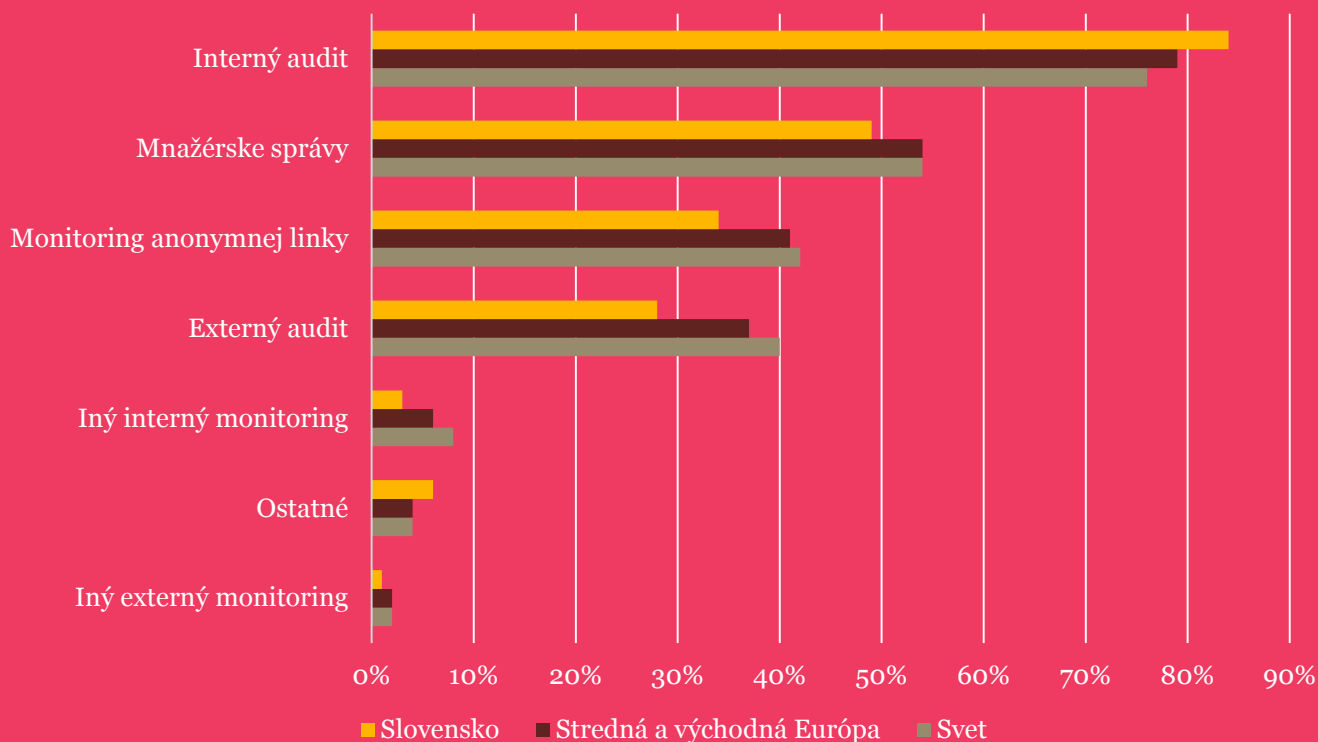
Podľa prieskumu je zavedený formálny etický a compliance program v 80% spoločnostiach. Aj keď je toto číslo vysoké, stále existuje priestor na zlepšenie. Podobne ako v Strednej a východnej Európe a celosvetovo, vedúci compliance oddelenia zodpovedá za etickú stránku podnikania a compliance program (51% na Slovensku, 38% v krajinách strednej a východnej Európy a celosvetovo).

Etický a compliance program v spoločnosti



Ak kľúčovým faktorom je príležitosť spáchať podvod (globálne 69%), potom najlepším spôsobom ako predchádzať podvodom je posilnenie kontrol. Aby spoločnosti zabezpečili efektívny etický program, 84% z nich má interný audit, 49% používa manažérske správy a 34% sleduje podania z anonymnej linky.

Ako vaša spoločnosť zaisťuje efektivitu etického a business programu?



Spoločnosti predpokladajú, že v najbližších 24 mesiacoch im vzniknú výdaje na compliance program na rovnakej úrovni ako doteraz. Jedna pätina spoločností očakáva zvýšenie týchto výdajov. Pri pohľade na to, kde sa nachádza etický a compliance program v spoločnosti vidíme, že 90% organizácií má etický kódex, ktorý pokrýva kľúčové riziká a smernice a zároveň uvádza hodnoty v spoločnosti.

Zrozumiteľnosť programu pre zamestnancov a celofiremná komunikácia sú základnými faktormi, ktoré prispievajú k efektívnemu compliance programu. Náš prieskum ukázal, že až 92% organizácií má hodnoty jasne stanovené a odkomunikované a 57% spoločností má pravidelné školenia k etickému kódexu a podobným smerniciam.

Viac ako tri štvrtiny respondentov (81%) si myslí, že vedenie ich organizácie vníma dôležitosť etického podnikania a samo ide príkladom. Tento prístup sa nazýva „tone at the top“ a určuje etické prostredie v organizácii a je dôležitým elementom v efektívnych interných kontrolách.

Napriek rastúcemu dôrazu na etické hodnoty v podnikovej komunikácii a rozšíreným obchodným etickým a compliance programom, spoločnosti stále môžu byť svedkami nesúlady medzi tým, ako sa k problematike stavia vedenie (tone at the top) a realitou v spoločnosti (či už v správaní alebo v rozpočtovom procese) čím je spoločnosť vystavená väčšej zraniteľnosti v dôsledku zlyhania v oblasti compliance.

Päť krokov na ceste k efektívnemu compliance programu

- Zaisťiť, že je program nastavený na jednej vlně s firemnou stratégiou. Potreba komunikovať, že program a stratégia spolu súvisia.
- Ohodnotiť a prípadne upraviť compliance pozíciu tak, aby sa dokázala prispôbiť prostrediu, v ktorom sa riziko a hrozby neustále menia.
- Zabezpečiť, že tí, ktorí majú program na starosti, rozumejú celkovému obrazu compliance programu v organizácii a svojej vlastnej role v rámci neho.
- Pamätajte na to, že nestačia len interné smernice a školenia, je potrebné sústavné a vytrvalé zapojenie celej organizácie.

Rozhovor

Kateřina Halásek Dosedřlová
Senior manařer, Forenznř služby



Akř sů najřastejšię vřzvy spojenř s compliance alebo etikou, ktorřm spoločnosti v sůčasnej dobe řelia?

Regulařnř prostredie, predovšetkřm v odvetvř finanřnřch sluřieb, sa stáva řoraz komplikovanejšię, existujř novř regulařnř pořiadavky, aj novovzniknutř regulařnř inřtitucie. Spoločnosti sů predmetom takmer neustálych zmien, napřiklad, řo sa třka oblastř celosvetovřch sankciř. V připade, ře spoločnosti nemajř zavedenř compliance program a vřhľadom na riziko meniaceho sa prostredia, ktorřho sů sůčasťou, sů zraniteľnejřie v připade, ře nesplnia regulařnř pořiadavky.

Ako sa zmenila compliance funkcia vřhľadom na vřvoj rizřk a řalřie nástrahy?

V sůčasnosti je rola compliance officera obsadená nielen vo finanřnřch inřtituciách a pobořkách zahraniřnřch firiem v řeskej republike a na Slovensku, ale aj v řeskřch a slovenskřch a řtátnych firmách. Je to pozitřvny signál. Na druhej strane, stáľe je veľa spoločností, ktorř považujř compliance funkciu iba za náklad a záťaž a snařia sa ho obmedziť na minimum. Nestař zriadiť compliance funkciu, len preto, aby sme splnili nejakř povinnosť. Dôležitř je, aby mala táto pozřcia dostatořnř právomoci a bola rovnocennřm partnerom vrcholovřho manařmentu, ktorř by mal poskytovať plnř podporu v oblasti compliance. Je nevyhnutnř, aby compliance funkcia fungovala efektřvne. A řo presne si pod třm predstavřť? Reagovať na vyvřjajřce sa riziká na zálade postupu zameranřho na riziká, nastaviť compliance program napřieč organizáciou, aby obmedzila riziko neplnenia compliance pořiadaviek, a mať vytvorenř eskalařnř a reportingovř mechanizmus pre připady, kedy je pokus o nesůlad alebo samotnř nesůlad s pořiadavkami compliance identifikovanř.

Ako by mal efektřvny compliance program fungovať?

Efektřvny compliance program by mal byť zameranř na riziká na zálade holistickřho přřstupu k rizikám hospodárskej kriminality napřieč spoločnosťou a jej slabosťami. Na jednej strane treba obmedziť relevantnř riziká a na strane druhej umořniť spoločnosti dosiahnuť jej ciele. Kľúčovř predpoklad efektřvneho compliance

programu je vhodná komunikácia napřieč spoločnosťou a jej prepojenie na řaždodennř řinnosti vo vřetkřch lokalitách. Compliance officer by mal zabezpečiť, aby bol program praktickř a aby malo oddelenie compliance otvorenř dvere pre zamestnancov spoločnosti bez ohľadu na ich pozřciu a aby im poskytlo připadnř vysvetlenie alebo odpovedalo na ad-hoc otázky. Vy, ako compliance officeri by ste si mali byť vedomř, ře zamestnanci sů preťaženi informáciami a ře v niektorřch odvetviach je fluktuácia zamestnancov dosť vysoká. Preto je potrebnř zvřžiť zabudovanie compliance tēm do pravidelnej komunikácie so zamestnancami v celej firme, relevantnřch oddeleniach, atď. Ako bolo spomenutř vyřřie, kľúčovou je podpora vrcholovřho manařmentu. Avřak, najdôležitejšia v komunikácii je zapojenie strednřho manařmentu na compliance programe. Strednř manařment je v dennom kontakte so zamestnancami a teda je poslom správ a vzorom. Ak zamestnanci uvidia, ře ich manařer řije compliance programom, zapoja sa a budř ho nasledovať.

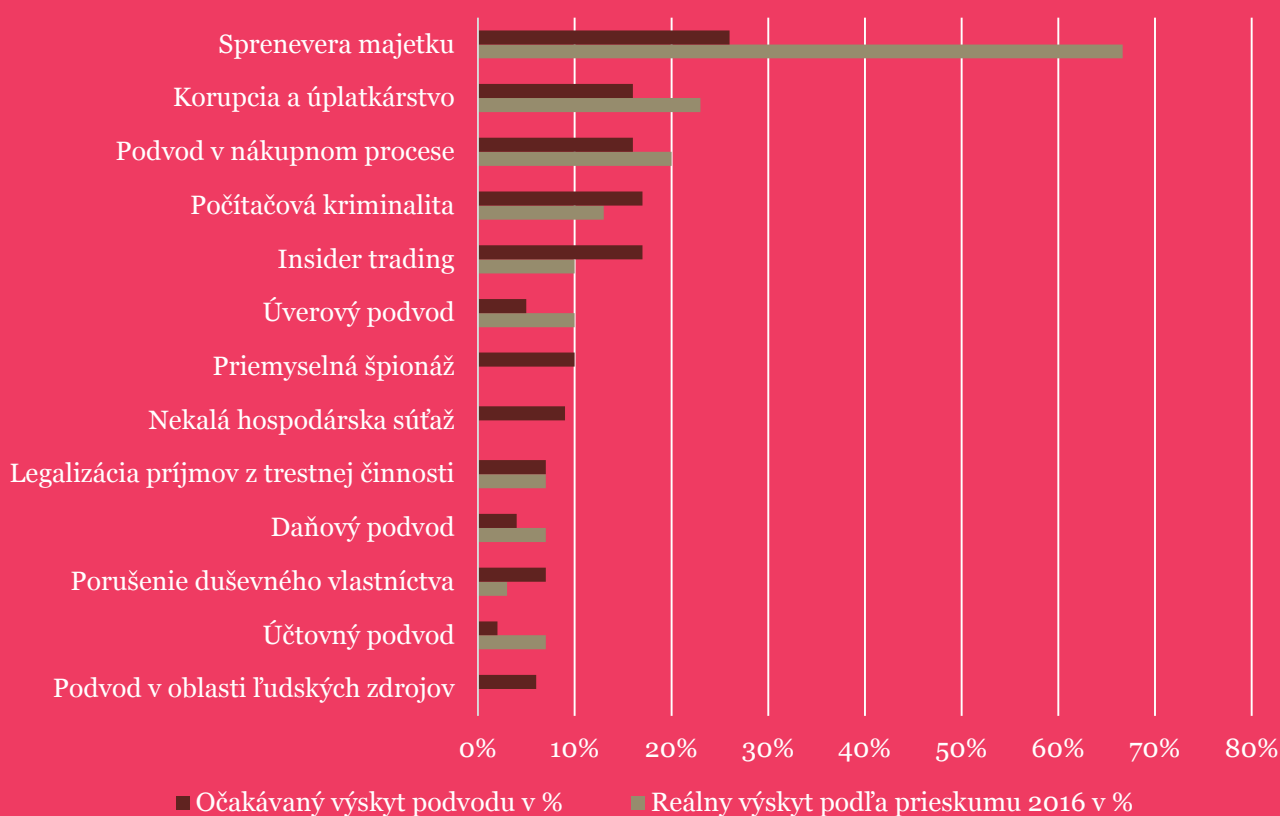
Na záver, mōžete uviesť typickř dôvody prečo compliance, respektřvie etickř funkcie nefungujř?

Ako uř bolo spomenutř, nie je to iba o vyřkrtávanř zo zoznamu. Aj keď je compliance neziskovřm oddelenřm vo firme, nemalo by mať kvōľi tomu podradnř úlohu. Skōr by to malo byť naopak. Aj v připade, ře vaša firma musř šetriť, vrátane nákladov na zamestnancov a školenia, nemalo by byť compliance oddelenie automaticky třm, ktorř sa zruřř. Toto by mohla byť chyba z pohľadu stratřgie. Riziká a hrozby sa neustáľe menia. Základ úspešnřho compliance programu je, ře dokáže predvřdať a odpovedať na zmeny v prostredř. Ĺalřřm problémom mōže byť neprepojenosť medzi compliance a beřnřm řivotom v spoločnosti. Prosřm, nezabůdajte, ře vařř zamestnanci, ři uř tř, ktorř prichádzajř do styku so zákazníkmi, alebo tř z podpornřch oddelenř, sů nazřvanř prvou lřniou v obrane proti hospodárskej kriminalite. Skůste ich preto zapojiť do compliance programu uř v přřpravnej fáze. Pravidelne s nimi komunikujř a dajte im pocit, ře sa na vás mōžu obrátiť so svojimi obavami alebo otázkou, keď budř chcěť.

Budúcnosť hospodárskej kriminality – realita hospodárskej kriminality verzus vnímanie rizika

Respondentov sme sa okrem iného spýtali, aký typ hospodárskej kriminality spoločnosti by ich mohol ohroziť v najbližších 24 mesiacoch.

Pomerne zaujímavé je porovnanie medzi vnímaním rizika a reálnym výskytom hospodárskej kriminality. Zdá sa, že spoločnosti podceňujú riziko sprenevery majetku napriek vysokému výskytu. Na druhej strane, vnímanie hrozby počítačovej kriminality je vyššie ako reálny výskyt.



Kontakty



Sirshar Qureshi

*Partner, Líder pre forenzné služby
v Strednej a východnej Európe*
+420 251 151 235
sirshar.qureshi@cz.pwc.com



Pavel Jankech

Direktor, Forenzné technológie
+420 251 151 336
pavel.jankech@cz.pwc.com



Kateřina Halásek Dosedělová

Senior manažér, Forenzné služby
+420 251 151 293
katerina.halasek-dosedelova@cz.pwc.com



Alexander Šrank

Partner, Líder oddelenia poradenstva
+421 2 59350 587
alexander.srank@sk.pwc.com



Pavol Adamec

Direktor, Riadenie rizík a informačné technológie
+421 2 59350 042
pavol.adamec@sk.pwc.com

Bratislava

PwC, Twin City/A, Karadžičova 2
815 32 Bratislava
tel.: +421 (0)2 59350 111

Košice

PwC, Aupark Tower
Protifašistických bojovníkov 11, 040 01 Košice
tel.: +421 (0)55 32153 11

www.pwc.com/sk

O prieskume

Globálny prieskum hospodárskej kriminality 2016 prebiehal počas augusta a septembra 2016. Prieskumu sa zúčastnilo 6 377 účastníkov z 115 krajín, vrátane 89 zo Slovenska. Z celkového počtu respondentov 63% boli vedúci pracovníci príslušných organizácií, 27% reprezentovalo spoločnosti kótované na burze a 43% organizácie s viac ako 1 000 zamestnancami. www.pwc.com/crimesurvey



© 2016 PwC. Všetky práva vyhradené. Názov "PwC" v tomto dokumente označuje spoločnosti PricewaterhouseCoopers Slovensko, s.r.o., PricewaterhouseCoopers Tax, k.s., PricewaterhouseCoopers Advisory, s.r.o. a PricewaterhouseCoopers Legal, s.r.o., ktoré sú členmi siete firiem PricewaterhouseCoopers International Limited, z ktorých každá je samostatným a nezávislým právny subjektom.