UNIVERZITA JANA AMOSE KOMENSKÉHO PRAHA

BAKALÁŘSKÉ KOMBINOVANÉ STUDIUM

2013-2017

BAKALÁŘSKÁ PRÁCE

Václav Pavlis

Analýza možných aktivit zaměstnanců směřujících proti hospodářským zájmům zaměstnavatele. Možnosti obrany a prevence proti takovému jednání ze strany managementu firmy

Praha 2017

Vedoucí bakalářské práce: Dr. Jindřich Nový, Ph.D.

JAN AMOS KOMENSKY UNIVERSITY PRAGUE

BACHELOR COMBINED STUDIES

2013-2017

BACHELOR THESIS

Václav Pavlis

Analysis of possible activities of employees against the economic interests of the employer. Possibilities of defense and prevention of such behavior by the management of the company

Prague 2017

The Bachelor Thesis Work Supervisor: Dr. Jindřich Nový, Ph.D.

Prohlášení

Prohlašuji, že předložená bakalářská práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem při zpracování čerpal, v práci řádně cituji a jsou uvedeny v seznamu použitých zdrojů.

Souhlasím s prezenčním zpřístupněním své práce v univerzitní knihovně.

V Praze dne 21. 5. 2017 Václav Pavlis

Poděkování

Chtěl bych poděkovat Dr. Jindřichu Novému, Ph.D. za vedení mé bakalářské práce.

Anotace

Bakalářská práce je koncipována jako teoreticko-empirická.

První část se zabývá nejčastějšími typy jednání a popsáním důvodů, proč se zaměstnanci takového jednání dopouštějí.

Ve druhé části uvádím konkrétní postupy a procedury, které riziko nekalého jednání podstatné snižují. Uvádím dále konkrétní řešení, které podnikům pomáhají s bojem proti nekalým aktivitám jejich zaměstnanců.

Klíčová slova

Firmy, korupce, kriminalita, podvod, podniky, prevence, zaměstnanci

Annotation

The bachelor thesis is conceived as a theoretical-empirical.

The first part deals with the most common types of frouds and describes the reasons why employees commit such behavior.

In the second part I present specific procedures which reduce the risk of unfair behavior substantially. I also mention a specific solution that helps businesses to fight their employees' abusive activities

Keywords:

Business, companies, crime, corruption, employees, fraud, prevention

ÚVOD

Pracovněprávní vztahy jsou nedílnou součástí života každého jedince, přičemž otázky související se správným a efektivním výkonem práce jednotlivých zaměstnanců jsou tématem, kterému je nutné věnovat v rámci řízení společnosti pozornost. Velmi často dochází k situacím, kdy zaměstnanci poruší své povinnosti, na což musí poté zaměstnavatel patřičně zareagovat. Do popředí zájmů se stále častěji dostávají tzv. hospodářsko-právní delikty, které jsou páchány právě zaměstnanci. Dnes není již příliš vhodné spoléhat se pouze na loajalitu a morálku pracovníků – je nutné je kontrolovat a také monitorovat během výkonu jejich práce.

Většina firem se v současné době setkává s aktivitami zaměstnanců na všech úrovní, které jsou způsobilé poškozovat jeho ekonomické zájmy.

Podniky v rámci systému ekonomické bezpečnosti realizují celou řadu opatření, jak těmto negativním jevům čelit.

Cílem práce je na základě seznámení se s teoretickými předpoklady připravit návrh možností prevence a obrany podniků proti základním typům podvodů.

Jedná se o velmi rozsáhlé téma a rozsah práce mi neumožňuje se věnovat celé problematice, proto se v této práci zaměřuji pouze na některé části problému.

TEORETICKO – METODOLOGICKÁ ČÁST

1 VYMEZENÍ ZÁKLADNÍCH POJMŮ A KATEGORIÍ

Hospodářskou kriminalitu je nutné vnímat jako závažnou hospodářskou trestnou činnost, která se zabývá primárně trestnými činy, které směřují proti daňové soustavě, proti měně či se zabývá podvody. *„Společenská nebezpečnost ekonomické kriminality je tedy evidentní. Nejde přitom jen o výši způsobených škod, byť je ohromující. Jde také o to, že případy ekonomické kriminality působí destruktivně na společenské vědomí, jak přímým poškozováním občanů (např. jako vkladatelů u napadených finančních institucí, zaměstnanců tzv. vytunelovaných podniků), tak jejich obtížným odhalováním, dokazováním a stíháním. Negativně může působit i skutečnost, že mezi pachateli ekonomické kriminality je zastoupen i nový typ pachatelů – kvalifikovaných odborníků, často prvopachatelů, zaujímajících (a zneužívajících) odpovědná místa ve struktuře řízení podniků a institucí. To může navozovat představu praktické nepostižitelnosti některých těchto případů a pachatelů, což ve svém důsledku vede k oslabování důvěry v instituce a garance demokratického právního státu.“*[1]

Protiprávní jednání na pracovišti, především ze strany zaměstnanců má bohatou historii a jedná se o velký problém pro ekonomiku každého státu. S podvodným jednáním se setkáváme na všech úrovní. Od řadových zaměstnanců až po vrcholné manažery.

Všechny uvedené skupiny mají jeden společný znak. Většina těchto lidí nepřijali danou práci za účelem poškozovat zaměstnavatele a nemají žádnou kriminální minulost.

Výzkumy uvádějí, že většinou hlavním důvodem není příležitost se obohatit, ale hlavním faktorem je motivace. Čím více nepokojený zaměstnanec, tím větší má náklonnost k páchání zločinu na úkor zaměstnavatele. Každý zaměstnanec má představu o svých osobních schopnostech a jak by měly být zaměstnavatelem ohodnoceny. Pokud

[1] Odbor hospodářské kriminality. *Policie.cz* [online]. 2017 [cit. 2017-05-09]. Dostupné z: http://www.policie.cz/clanek/sluzby-odbory-skupiny-odbor-hospodarske-kriminality.aspx

se tato představa diametrálně liší od reality, zvětšuje se tím riziko náklonnosti ke spáchání zločinu.

Ke konkrétním důvodům, vedoucím k páchání podvodu zaměstnanci patří:

- Neschopnost zaměstnance splácet své dluhy.
- Problémy plynoucí z osobního selhání (např. v důsledku drogové závislosti, alkoholismu).
- Pracovní neúspěchy (problémy v zaměstnání).
- Fyzická izolace zaměstnance (izolace od lidí, kteří by mu mohli pomoc).
- Ztráta statusu (zaměstnanec chce získat společenské uznání, ale nemá na to kvalifikaci ani jiné prostředky).
- Vztah mezi zaměstnancem a zaměstnavatelem (zaměstnanec se cítí být poškozován, zneužíván nebo nedoceněn).
- Příležitost pro páchání podvodů (zaměstnanec zjistil, že ve společnosti nefungují kontrolní mechanismy).
- Zdůvodnění (pomsta zaměstnavateli, osobní přesvědčení že prostředky po vyřešení problémů vrátí).

Jednou ze základních povinností vyjmenovaných v ustanovení zákoníku práce je povinnost řádně hospodařit s prostředky svěřenými zaměstnavatelem a přežit a ochraňovat majetek zaměstnavatele před poškozením, ztrátou, zničením a zneužitím a nejednat v rozporu s oprávněnými zájmy zaměstnavatele. Jak dovodil Nejvyšší soud České republiky v několika svých rozhodnutích, výše uvedené povinností představujíc mravní imperativ kladený na každého zaměstnance, jenž ve svém obsahu znamená určitou míru loajality ve vztahu ke svému zaměstnavateli a zároveň též i obecnou prevencí povinnost zaměstnance ve vztahu k majetku a oprávněným zájmům zaměstnavatele. Jde o požadavek na určitou úroveň kvality chování zaměstnance.

Zákon zde vedle povinností vyplývajících z právních předpisů a jiných předpisů vztahujících se k práci zaměstnance ukládá zaměstnanci, aby celým svých chováním v souvislosti s pracovním vztahem nezpůsoboval zaměstnavateli škodu, ať už majetkovou nebo morální.

Takového jednání se zaměstnanec může dopustit i za situace, že bude zcela dodržovat všechny právní a ostatní předpisy vztahující se bezprostředně k práci jím vykonávané.

Rozhodující pro posouzení toho, zda se zaměstnanec chová v souladu.

2 ANALÝZA SOUČASNÉHO STAVU V PODMÍNKÁCH ČR

V roce 2016 téměř 35 % společností v České republice prodělalo jeden či dokonce i více případů hospodářské kriminality, přičemž 36 % těchto případů tvořila počítačová kriminalita.

Dle studie společnosti PricewaterhouseCoopers, která se věnovala výskytu hospodářské kriminality v České republice, je možné konstatovat, že hospodářská kriminalita i dnes představuje velmi závažný problém, který ovlivňuje chod společností, a to nejenom v podmínkách českého podnikatelského prostředí, ale i celosvětově. V roce 2016 se s hospodářskou kriminalitou setkalo 35 % respondentů, což je stav, který je srovnatelný se situací ve střední a východní Evropě. I přesto, že ve srovnání s předcházejícím rokem počet výskytů hospodářské kriminality poklesnul o 13procentních bodů, není důvod se příliš radovat.

V rámci vývoje současných rizik totiž řada podniků musí dnes a denně čelit dosti sofistikovaným podvodům, které je velmi obtížné včas odhalit, a které mohou tak ve firmě probíhat dokonce i řadu let. Tyto, mnohdy skryté a dlouhotrvající podvody, mají poté na podnik katastrofální dopady, protože jsou mnohem více nebezpečné než jednorázové incidenty, a jsou doprovázeny taktéž i vyššími náklady. Mezi nejčastější typy hospodářské kriminality, se kterými je možné se v Česku setkat, patří nadále i zpronevěra majetku, která je všeobecně vnímána jako podvod, který je snadné odhalit ve srovnání s ostatními typy této kriminality. Dle průzkumů je možné mezi další nejčastější typy podvodů zařadit počítačovou kriminalitu, podvody v rámci nákupního procesu, podplácení a korupce a účetní podvody. Převážná většina podvodů je však v Česku odhalena prostřednictvím podnikových kontrol – jedná se až o téměř 68 % těchto podvodů. Avšak i přesto je možné konstatovat, že každý pátý případ podvodu je odhalen ve své podstatě způsobem, na který nemá dnes ani management firmy téměř žádný vliv, a to naprostou náhodou, ve 14 % případů. V roce 2016 počet podvodů, které

byly spáchány externím pachatelem, mírně převažuje nad podvody, které byly spáchány interním pachatelem. [2]

Obecně se dá říci, že společenské klima v ČR má stále vysoký kriminogenní potenciál – tj. je velmi příznivé pro páchání trestné činnosti. Statistikami orgánů činných v trestním řízení lze doložit, že mezi osobami – pachateli trestné činnosti mají stále velmi vysoký podíl osoby dosud netrestané a osoby poprvé trestně stíhané v tzv. produktivním věku. Přitom věk bývá tím faktorem, který má často rozhodující vliv na vznik rizikového jednání občanů. Dalším důležitým prvkem, který kromě zvyšujícího se věku brání vzniku rizikového, konkrétně kriminálního chování, bývá hrozba postihem, trestem, policejním vyšetřováním a soudním řízením. Zdá se, že oba tyto faktory dnes svou funkci plní jen částečně, nebo nedostatečně.

Dále lze konstatovat z výzkumů a statistik zjištěnou skutečnost, že se v české společnosti formuje skupina profesionálních pachatelů trestné činnosti – nikoli klasických recidivistů, ale ve smyslu trestné činnosti jako svébytného druhu podnikatelských aktivit. Jsou to lidé, kteří jsou vzdělaní, díky svému intelektuálnímu a sociálnímu charakteru by se ve společnosti velmi dobře uplatnili na vysokých postech a kriminální činnost, kterou provozují, není způsobena hmotnou nouzí, nebo palčivou potřebou tohoto směru. Podle zjištěných charakteristik, původu a vzdělání jsou to lidé tzv. slušní, jsou tím „lepším vzorkem“ běžné populace. Vyznačují se profesionální a intelektuální zdatností bez morálních zábran, což je v tomto případě nejvíce zneklidňující skutečností.

[2] Celosvětový průzkum hospodářské kriminality 2016: Zpráva za Českou republiku. *Pwc.com* [online]. 2017. [cit. 2017-05-09]. Dostupné z: https://www.pwc.com/cz/cs/hospodarska-kriminalita/assets/pdf/global-economic-crime-survey-2016-cz.pdf

PRAKTICKÁ ČÁST

3 NEJČASTĚJŠÍ TYPY JEDNÁNÍ PROTI ZÁJMŮM ZAMĚSTNAVATELŮ

3.1 Hospodářská kriminalita

V ekonomicky vyspělých zemích je hospodářská kriminalita považována za závažný společensko – politický problém, zejména proto, že způsobuje vysoké škody materiální, ale také morální škody ve společnosti. Nebezpečnost hospodářské kriminality spočívá v tom, že se rozrůstá do různých směrů a odvětví a její součástí se stává stále více účastníků hospodářských vztahů. V mnoha vyspělých zemích se součástí hospodářské kriminality stává také organizovaný zločin a tím je znesnadněno její odhalování a potrestání pachatelů. Také vznik mezinárodních společenství způsobil, že hospodářská kriminalita se může snadněji šířit přes hranice jednotlivých států, stává se tudíž mezinárodním problémem, který je třeba řešit nejen na národní ale také na mezistátní úrovni, který nutně vyžaduje stálou, soustředěnou a neustávající pozornost.

V historickém vývoji byla hospodářská kriminalita definována různě:

- r. 1935 pohlížel Albert Morris na hospodářskou kriminalitu jako na působení kriminálního podsvětí, které páchá tzv. běžnou trestnou činnost, na kriminální nadsvětí, které se pro změnu zabývá hospodářskou kriminalitou.
- r. 1939 Edwin H. Sutherland rozšířil od té doby populární název „kriminalita bílých límečků (white collar crime)“ a definoval hospodářský zločin jako jednání, které spáchala vážená, vysoce postavená osoba v rámci svého povolání, využívajíc své důvěry vyplývající z jejího vysokého sociálního statusu a prestiže r. 1950 Frank E. Hartung dále rozpracoval teorii bílých límečků a chápe ji jako porušení hospodářského zákona, které je pácháno pro finanční zisk a to firmou, s její pomocí, nebo prostřednictvím jejích pracovníků při plnění jejich obchodní činnosti.

- r. 1952 B. Clinard navázal na předchozí teorii doplněním, že se jedná o porušení zákona především skupinou obchodníků, svobodných pracovníků a úředníků v souvislosti s jejich prací.
- r. 1968 Edward A. Ross viděl problematiku páchání hospodářské trestné činnosti především v osobách jejích pachatelů, kteří jsou často podle zákona vinní, ale jsou oceňováni společností a sami své jednání nespatřují jako kriminální.

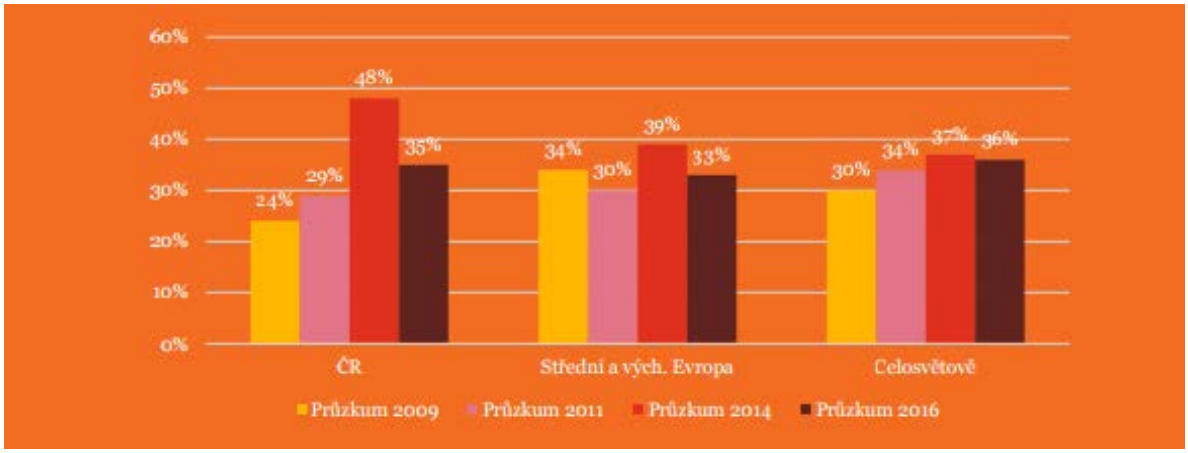
S vymezením okruhu pachatelů se pojí také společné prvky chování a jednání pachatele hospodářské kriminality. Obecně je kriminální chování v této oblasti výsledkem svobodného chování jedince, vycházející v první řadě z ekonomického kalkulu. Velice problematickou skutečností je fakt, že pachatelé hospodářské kriminality vychází z řad vzdělaných, vysoce postavených, společností uznávaných a sofistikovaných lidí. Jejich nezákonná činnost bývá vykonávána dlouhou dobu, přičemž navenek neviditelná a velmi obtížně odhalitelná. Stopy zanechané pachateli hospodářské trestné činnosti jsou velice specifické a ve své podstatě diametrálně odlišné od stop běžné kriminality.

Dalším zásadním problémem je mnohdy úplná latence. Ve spoustě případů spáchaných deliktů se skutek jako takový nepodařilo nikdy zjistit. Další možností je sice zjištění, ale neoznámení skutku orgánům činným v trestním řízení. Společnosti raději oželí nemalé finanční ztráty, než aby kontaktovaly orgány činné v trestním řízení a absolvovaly zdlouhavou a mnohdy neúčinnou proceduru vyšetřování trestné činnosti. Tím však také přispívají k tomu, že se pachatel může o své jednání pokusit znovu a ve většině případů poučen, lépe připraven a tím obtížněji zjistitelný. Následně způsobená škoda také bývá mnohem větší.

Je nutné upozornit na to, že hospodářská kriminalita se od ostatních druhů kriminality dnes značně liší, a to především proto, že schéma jejich aktivit se shoduje se schématem legálního ekonomického života. *„Hospodářské trestné činy, i když se dotýkají individuálních práv, jsou téměř vždy ziskem motivované a převážně latentní útoky proti kolektivním právům, proti hospodářskému systému jako celku nebo proti některému jeho institutu, zejména proti organizaci trhu, zájmům spotřebitelů, regulaci zahraničního obchodu, hospodářské činnosti podniků, regulaci finančního systému a zčásti i proti*

ochraně životního prostředí. Zjednodušeně řečeno, hospodářské delikty jsou trestné činy, které jsou páchány ze sféry hospodářství do sféry hospodářství".[3] Lze konstatovat, že hospodářská kriminalita je dnes důvodem obav velkého množství společností, a to různých velikostí, odlišných průmyslových odvětvích a taktéž různých vlastnických struktur. V rámci srovnání se střední a východní Evropou je výskyt hospodářské kriminality v Česku častější, avšak jedním pozitivem je fakt, že hospodářská kriminalita klesá, což je patrné z Graf 1.

Graf 1: Výskyt hospodářské kriminality v České republice

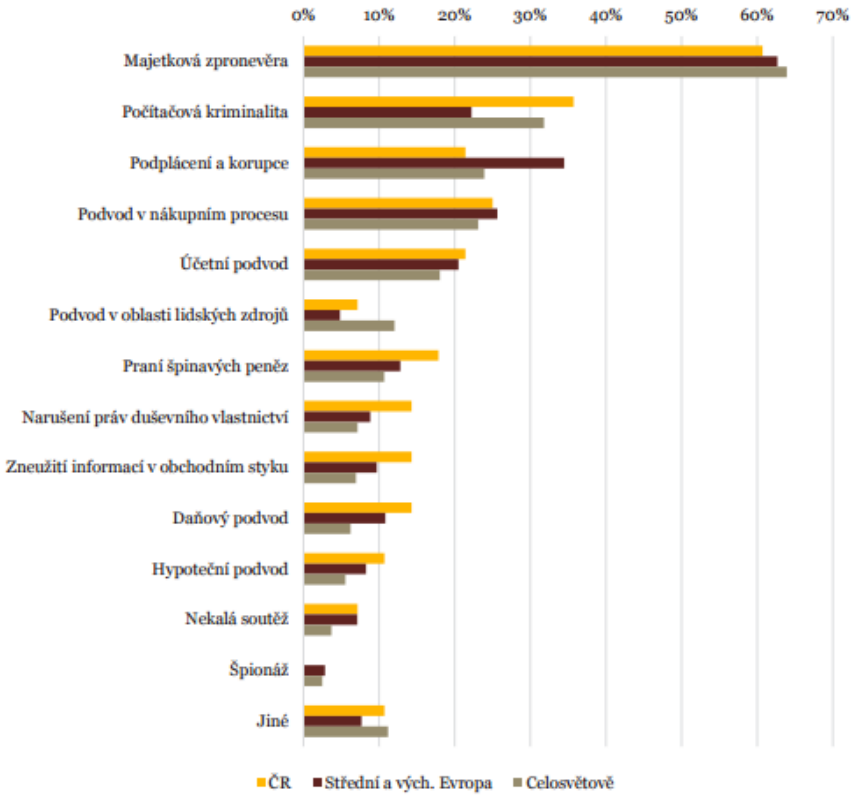


Zdroj[4]

[3] TOMKOVÁ, V. Výzkum ekonomické kriminality. *Ok.cz: Institut pro kriminologii a sociální prevenci v Praze* [online]. Praha, 2004 [cit. 2017-05-09]. Dostupné z: http://www.ok.cz/iksp/docs/308.pdf

[4] Celosvětový průzkum hospodářské kriminality 2016: Zpráva za Českou republiku. *Pwc.com* [online]. 2017. [cit. 2017-05-09]. Dostupné z: https://www.pwc.com/cz/cs/hospodarska-kriminalita/assets/pdf/global-economic-crime-survey-2016-cz.pdf

Graf 2: Typy hospodářské kriminality



Zdroj[5]

3.2 Počítačová kriminalita

Počítačová kriminalita je velkou množinou kriminálních aktivit, které jsou spojeny s počítačem jako nástrojem či popřípadě také cílem dané trestné činnosti. Počítač je zapotřebí v tomto směru vnímat jako soubor veškerých technických a programových vybavení, a to včetně dat, které jsou v něm uloženy. Počítač je nosičem informací, což je významné především z pohledu ustanovení § 257a trestního zákona. *„Kdo získá přístup k nosiči informací a v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch takových informací neoprávněně užije,*

[5] Celosvětový průzkum hospodářské kriminality 2016: Zpráva za Českou republiku. *Pwc.com* [online]. 2017. [cit. 2017-05-09]. Dostupné z: https://www.pwc.com/cz/cs/hospodarska-kriminalita/assets/pdf/global-economic-crime-survey-2016-cz.pd

informace zničí, poškodí, změní nebo učiní neupotřebitelnými, nebo učiní zásah do technického nebo programového vybavení počítače nebo jiného telekomunikačního zařízení, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty.“ [6] V roce 2016 více jak 1/3 respondentů, kteří se s podvodem setkali, uvedla, že tento podvod se týkal počítačové kriminality, což mírně převyšuje dokonce celosvětový průměr i průměr ve střední a východní Evropě. Na základě realizovaného výzkumu je možné identifikovat dosti významným poznatek, a to je změna v oblasti celkového vnímání počítačové kriminality. Již dávno neplatí, že počítačová kriminalita je jen „IT problémem“ – jedná se o zásadní hrozbu, která má vliv na podnikatelskou činnost a taktéž na provoz podniku jako celku, což je nutné si uvědomit. Výskyt počítačové kriminality má v případě Česka rostoucí trend, přičemž počet účastníků průzkumu, kteří se s počítačovou kriminalitou setkali, v posledních letech vzrostl z 13 % na 36 %. Jelikož se podnikatelské prostředí neustále mění, většina komunikace, dokumentů i transakcí probíhá již pouze prostřednictvím digitální formy. I proto je dnes počítačová kriminalita vnímána jako jedna z největších hrozeb v podniku. Více jak 1/3 společností dnes dokonce očekává, že v dalším roce bude opět počítačovým podvodem ohrožena, přičemž téměř 60 % dotazovaných je toho názoru, že rizika spojená s počítačovou kriminalitou rostou vlivem technologických změn, čímž se vnímání počítačové kriminality rozšiřuje. Mezi systémy, které jsou dnes počítačovou kriminalitou ohroženy, patří jak počítače, tak i mobilní telefony, dále také zařízení, která jsou připojena ke cloudu či automobily a zařízení v domácnosti, která jsou k internetu připojena. Je nutné dále taktéž uvést, že i z finančního hlediska je počítačová kriminalita dosti nákladnou záležitostí – více jak ¼ firem v rámci celého světa uvádí, že za poslední roky utrpěla vlivem počítačové kriminality velké ztráty, a to až ve výši 1 200 000 Kč. [7]

[6] ČESKÁ REPUBLIKA. Zákon č. 140/1961 Sb., trestní zákon: Trestní zákon. In: *Sbírka zákonů ČR*. 1961.
[7] Celosvětový průzkum hospodářské kriminality 2016: Zpráva za Českou republiku. *Pwc.com* [online]. 2017. [cit. 2017-05-09]. Dostupné z: https://www.pwc.com/cz/cs/hospodarska-kriminalita/assets/pdf/global-economic-crime-survey-2016-cz.pdf

3.3 Podplácení a korupce v podniku

Pokusy o podplácení a korupci mohou přicházet nejenom z externího prostředí společnosti, ale především také i ze strany vlastních pracovníků. Dle studie společnosti PricewaterhouseCooper se korupce a podplácení umístily na 4. místě v „žebříčku" nejvíce páchaných činnosti hospodářské kriminality v Česku. Pozitivní zprávou je však to, že více jak 86 % dotazovaných uvádí, že v podniku je nastavený tzv. etický a compliance program – tato hodnota se nachází lehce nad průměrem východní a střední Evropy i celého světa. Je nutné uvést, že pojem „compliance" není právní, ale korporátní a společensko-podnikovou kategorií, která je všeobecně vnímána jako vymezení a také dodržování právních a etických pravidel chování obchodní společnosti či korporace a jejich pracovníků, a to nejenom v rámci čistě obchodních vztahů, ale i v dalších oblastech existence a činnosti společnosti. Cílem definování těchto standardizovaných pravidel chování, které jsou dobrovolně přijímány prostřednictvím závazného vnitřního předpisu podniku, a jsou označovány za compliance program, je výslovným a jednoznačným způsobem deklarovat tzv. korporátní závazek, a to jak navenek, tak i dovnitř společnosti, z hlediska toho, že chování podniku je v rámci obchodních a s tím souvisejících vztahů, v plném souladu s etickými a také především právními pravidly hospodářské soutěže, daňové i finanční integrity, ochrany v oblasti životního prostředí a zaměstnaneckých vztahů, a to včetně zajištění rovných příležitostí v podniku. [8] V uvedeném průzkumu je až 80 % respondentů toho názoru, že jejich etický kodex pokrývá nejvýznamnější rizika a oblasti, a správně specifikuje i hodnoty dané společnosti. *„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*

[8] KOUKAL, P. Korporátní pravidla Compliance a nový trestní zákoník. *Ihned.cz* [online]. Praha, 2010 [cit. 2017-05-09]. Dostupné z: http://pravniradce.ihned.cz/c1-40730210-korporatni-pravidla-compliance-a-novy-trestni-zakonik

etickým principům firmy. Pravidelná školení zaměstnanců proto doporučujeme všem společnostem.“ [9]

3.4 Sociálně patologické jevy na pracovišti

Co se týče dalších jevů v oblasti hospodářské kriminality, je nutné zmínit patologické jevy a diskriminaci na pracovišti, ke které dnes taktéž velmi často v prostředí českých společností dochází. Je více než jasné, že na pracovišti jsou sociálně patologické jevy naprosto nežádoucí, a proto je nutné jim věnovat dostatečně velkou pozornost. Ani dnes není možné tyto jevy z prostředí pracovišť zcela odstranit, takže je zapotřebí přijímat rozhodnutí, která povedou k jejich minimalizaci. To, co jedince v životě ve velké míře ovlivňuje, je samozřejmě práce, přičemž se nejedná pouze o pracovní činnost, kterou člověk realizuje proto, aby za ni dostal patřičnou odměnu – jedná se o i seberealizaci, pocit uplatnění, pocit uspokojení, získání naprosto nových zkušeností a taktéž kontakt s jinými lidmi, který je nesmírně důležitý. Pokud je tedy pracovní klima bezpečné, existuje zde i větší pracovní spokojenost. To, co tudíž člověka každý den ovlivňuje, jsou pracovní vztahy a klima celého pracovního prostředí. Proto je velmi důležité s kolegy v práci vycházet, stejně jako vycházet i se svými podřízenými a nadřízenými. *„Klima, které panuje na pracovišti, ovlivňuje psychiku pracovníků a také jejich pracovní výkon, a to jak pozitivně, tak i negativně. V klimatu bezpečné kultury podávají lidé větší výkon a taktéž dokážou řešit obtížné nebo krizové situace rychleji a účinněji, snadněji přebírají osobní zodpovědnost a dělají méně chyb. Důvěřují svým spolupracovníkům, vztahy na pracovišti jsou v klimatu bezpečné kultury kultivovanější, kvalitnější a profesionálnější. Větší je též identifikace s firmou, otevřenost ke kolegům, důvěra ve vedení a chuť se angažovat. To vede ke spokojenosti zaměstnanců a kvalitnějšímu výkon celé organizace. Naopak nebezpečná kultura na pracovišti zvyšuje riziko vztahových patologií – šikanování, psychického teroru, různých forem nátlaku a*

[9] Celosvětový průzkum hospodářské kriminality 2016: Zpráva za Českou republiku. *Pwc.com* [online]. 2017. [cit. 2017-05-09]. Dostupné z: https://www.pwc.com/cz/cs/hospodarska-kriminalita/assets/pdf/global-economic-crime-survey-2016-cz.pdf

diskriminace, které lze nazývat jako mobbing.“ [10] Zmíněné jevy negativním způsobem působí jak na postižené jednotlivce, tak i na celou společnost. Mezi sociálně patologické jevy je možné zařadit např. mobbing, bossing, staffing či sexuální obtěžování. Je více než jasné, že ty patologický jevy ovlivňují tedy i ekonomické zájmy společnosti. Dnes existuje velké množství nejrůznějších studií, které hovoří o vzájemné závislosti, která vzniká mezi úrovni pracovních vztahů a pracovním výkonem, a proto je především i v zájmu samotného podniku, aby pečoval o pracovníky, vytvářel jim dostatečně vhodné podmínky pro výkon jejich práce, a především včas identifikoval patologické jevy na pracovišti. To vše má poté pozitivní vliv na výkon zaměstnanců. Škody, které vznikají vlivem patologických jevů, tak nemají vliv pouze na samotné pracovníky, ale přináší obrovské negativní dopady v podobě narušení vztahů na pracovišti, vznik různých skupin, které mezi sebou poté soutěží, znevažování se navzájem, neochota v týmovou spolupráci s kolegy a v konečném důsledku i naprostá deformace v oblasti dobré pověsti podniku. To vše má samozřejmě negativní vliv na hospodářské zájmy společnosti, a proto by měla být prevence těchto jevů pro podnik dnes prioritou. [11]

[10] PROVAZNÍKOVÁ, R. Patologie v pracovních vztazích – mobbing. *Cssz.cz* [online]. 2013 [cit. 2017-05-09]. Dostupné z: http://www.cssz.cz/cz/casopis-narodni-pojisteni/archiv-vydanych-cisel/clanky/renata-provaznikova-patologie-v-pracovnich-vztazich-mobbing-1.htm

[11] CHROMÝ, J. *Násilí na pracovišti. Charakteristika, rizikové faktory, specifické formy a právní souvislosti.* Praha: Wolters Kluwer, 2014. 216 s. ISBN 978-80-7478-552-8, s. 13

4 MOŽNOSTI PREVENCE

4.1 Prevence proti vznikům podvodů

Lze konstatovat, že samotný pojem rozvíjení odolnosti vůči určitému problému není až tak neznámý pojem, protože je možné se s ním setkat i v osobním životě, kdy např. jedince usiluje o vypěstování si určité odolnosti vůči onemocněním, jako je chřipka, rakovina či nachlazení, aj. Velmi podobně jsou i ve firmách již řadu let zaváděny nejrůznější interní systémy, které slouží k rozvoji odolnosti vůči omylům v podniku a taktéž slouží jako prevence proti vzniku podvodu, a to ze strany zaměstnanců. Dnes je možné setkat se s ratingy, které jsou orientovány na zlepšení odolnosti vůči špatnému hospodaření či hamižnosti v podniku. Tyto ratingy jsou v současné době velmi často realizovány prostřednictvím srovnávacích testů, měření či rozšíření vedení podniku a společenské odpovědnosti firem. Podnik tak může implementovat interní systém, který dále povede k růstu odolnosti společnosti vůči nejrůznějším podvodům a korupci, a je orientován také na zlepšení v oblasti rentability a výkonu firmy. *„Mezi dodatečné cíle je možné zařadit zvýšení hodnoty kodexu chování a reakce na vnější požadavky a tlaky na dobře vedenou a transparentnější organizaci bez korupce. Organizace by si měly usnadnit život a zacházet s podvodem a korupcí jako s jednotným problémem, alespoň z podnikového nebo organizačního hlediska. Nejasné hranice mezi podvodem a korupcí, mnoho popisů podvodu, které již zahrnují slova korupce a uplácení, a četné další vágní a různorodé existující definice korupce naznačují, že je čas přestat se zabývat formulacemi a jednoduše integrovat tyto dvě položky pod jednu střechu.“* [12] I v České republice dnes nastal čas akceptovat fráze, jako jsou např. ty, že jedním ze způsobů, jak lze dnes vydělat peníze, je přestat je ve společnosti ztrácet, nebo že prevence je efektivnější a méně nákladná než léčba, aj. [13] V rámci prevence podvodů je i dnes v českém prostředí využíván anglický termín fraud management, který byl již v textu blíže specifikován. *„Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo*

[12] INTERNÍ AUDIT A STRUKTURÁLNÍ FONDY EU. *Interniaudit.cz* [online]. 2013 [cit. 2017-05-09]. Dostupné z: http://www.interniaudit.cz/download/clenstvi/casopis/auditor0806.pdf
[13] Tamtéž.

propadnutím věci nebo jiné majetkové hodnoty. Podvod je úmyslný čin jednoho nebo více jedinců z okruhu managementu, osob pověřených vedením, zaměstnanců nebo třetích stran, s účelem získat neoprávněnou či nelegální výhodu.“ [14] V rámci fraud managementu je však termín „podvod“ využíván v širším slova smyslu, a úzce souvisí s navrhováním nejrůznějších opatření, které slouží k prevenci podvodů a korupce ve společnosti, a to ze strany vlastních pracovníků organizace. Na tyto opatření v podobě prevence jsou dnes vynakládány v Česku značné finanční prostředky, avšak je nutné si uvědomit, že podvody a korupce způsobují společnostem nemalé finanční ztráty, a proto jsou tyto vysoké náklady odůvodněné. V rámci preventivních opatření je možné se v případě podnikatelské praxe inspirovat i u jiných společnost či si najmout na tuto oblast dokonce i poradenskou firmu, která se na zmíněnou problematiku orientuje. Lze konstatovat, že společnosti v České republice v posledních letech věnují prevenci dostatečnou pozornost a nepodceňují ji.

4.2 Detekční metody

Lze konstatovat, že samotný pojem rozvíjení odolnosti vůči určitému problému není až tak neznámý pojem, protože je možné se s ním setkat i v osobním životě, kdy např. jedince usiluje o vypěstování si určité odolnosti vůči onemocněním, jako je chřipka, rakovina či nachlazení, aj. Velmi podobně jsou i ve firmách již řadu let zaváděny nejrůznější interní systémy, které slouží k rozvoji odolnosti vůči omylům v podniku a taktéž slouží jako prevence proti vzniku podvodu, a to ze strany zaměstnanců. Dnes je možné setkat se s ratingy, které jsou orientovány na zlepšení odolnosti vůči špatnému hospodaření či hamižnosti v podniku. Tyto ratingy jsou v současné době velmi často realizovány prostřednictvím srovnávacích testů, měření či rozšíření vedení podniku a společenské odpovědnosti firem. Podnik tak může implementovat interní systém, který dále povede k růstu odolnosti společnosti vůči nejrůznějším podvodům a korupci, a je orientován také na zlepšení v oblasti rentability a výkonu firmy. *„Mezi dodatečné cíle je možné zařadit zvýšení hodnoty kodexu chování a reakce na vnější požadavky a tlaky na dobře vedenou a transparentnější organizaci bez korupce. Organizace by si měly usnadnit život a zacházet s podvodem a korupcí*

[14] ČESKÁ REPUBLIKA. Zákon č. 140/1961 Sb., trestní zákon: Trestní zákon. In: *Sbírka zákonů ČR*. 1961.

jako s jednotným problémem, alespoň z podnikového nebo organizačního hlediska. Nejasné hranice mezi podvodem a korupcí, mnoho popisů podvodu, které již zahrnují slova korupce a uplácení, a četné další vágní a různorodé existující definice korupce naznačují, že je čas přestat se zabývat formulacemi a jednoduše integrovat tyto dvě položky pod jednu střechu.“ [15] I v České republice dnes nastal čas akceptovat fráze, jako jsou např. ty, že jedním ze způsobů, jak lze dnes vydělat peníze, je přestat je ve společnosti ztrácet, nebo že prevence je efektivnější a méně nákladná než léčba, aj. [16] V rámci prevence podvodů je i dnes v českém prostředí využíván anglický termín fraud management, který byl již v textu blíže specifikován. *„Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty. Podvod je úmyslný čin jednoho nebo více jedinců z okruhu managementu, osob pověřených vedením, zaměstnanců nebo třetích stran, s účelem získat neoprávněnou či nelegální výhodu.“* [17] V rámci fraud managementu je však termín „podvod“ využíván v širším slova smyslu, a úzce souvisí s navrhováním nejrůznějších opatření, které slouží k prevenci podvodů a korupce ve společnosti, a to ze strany vlastních pracovníků organizace. Na tyto opatření v podobě prevence jsou dnes vynakládány v Česku značné finanční prostředky, avšak je nutné si uvědomit, že podvody a korupce způsobují společnostem nemalé finanční ztráty, a proto jsou tyto vysoké náklady odůvodněné. V rámci preventivních opatření je možné se v případě podnikatelské praxe inspirovat i u jiných společnost či si najmout na tuto oblast dokonce i poradenskou firmu, která se na zmíněnou problematiku orientuje. Lze konstatovat, že společnosti v České republice v posledních letech věnují prevenci dostatečnou pozornost a nepodceňují ji.

[15] INTERNÍ AUDIT A STRUKTURÁLNÍ FONDY EU. *Interniaudit.cz* [online]. 2013 [cit. 2017-05-09]. Dostupné z: http://www.interniaudit.cz/download/clenstvi/casopis/auditor0806.pdf
[16] Tamtéž.
[17] ČESKÁ REPUBLIKA. Zákon č. 140/1961 Sb., trestní zákon: Trestní zákon. In: *Sbírka zákonů ČR*. 1961.

4.3 Počítačová bezpečnost

Lze konstatovat, že samotný pojem rozvíjení odolnosti vůči určitému problému není až tak neznámý pojem, protože je možné se s ním setkat i v osobním životě, kdy např. jedince usiluje o vypěstování si určité odolnosti vůči onemocněním, jako je chřipka, rakovina či nachlazení, aj. Velmi podobně jsou i ve firmách již řadu let zaváděny nejrůznější interní systémy, které slouží k rozvoji odolnosti vůči omylům v podniku a taktéž slouží jako prevence proti vzniku podvodu, a to ze strany zaměstnanců. Dnes je možné setkat se s ratingy, které jsou orientovány na zlepšení odolnosti vůči špatnému hospodaření či hamižnosti v podniku. Tyto ratingy jsou v současné době velmi často realizovány prostřednictvím srovnávacích testů, měření či rozšíření vedení podniku a společenské odpovědnosti firem. Podnik tak může implementovat interní systém, který dále povede k růstu odolnosti společnosti vůči nejrůznějším podvodům a korupci, a je orientován také na zlepšení v oblasti rentability a výkonu firmy. *„Mezi dodatečné cíle je možné zařadit zvýšení hodnoty kodexu chování a reakce na vnější požadavky a tlaky na dobře vedenou a transparentnější organizaci bez korupce. Organizace by si měly usnadnit život a zacházet s podvodem a korupcí jako s jednotným problémem, alespoň z podnikového nebo organizačního hlediska. Nejasné hranice mezi podvodem a korupcí, mnoho popisů podvodu, které již zahrnují slova korupce a uplácení, a četné další vágní a různorodé existující definice korupce naznačují, že je čas přestat se zabývat formulacemi a jednoduše integrovat tyto dvě položky pod jednu střechu.“* [18] I v České republice dnes nastal čas akceptovat fráze, jako jsou např. ty, že jedním ze způsobů, jak lze dnes vydělat peníze, je přestat je ve společnosti ztrácet, nebo že prevence je efektivnější a méně nákladná než léčba, aj. [19] V rámci prevence podvodů je i dnes v českém prostředí využíván anglický termín fraud management, který byl již v textu blíže specifikován. *„Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty. Podvod je úmyslný čin jednoho nebo více jedinců z okruhu managementu, osob pověřených vedením, zaměstnanců nebo*

[18] INTERNÍ AUDIT A STRUKTURÁLNÍ FONDY EU. *Interniaudit.cz* [online]. 2013 [cit. 2017-05-09]. Dostupné z: http://www.interniaudit.cz/download/clenstvi/casopis/auditor0806.pdf
[19] Tamtéž.

třetích stran, s účelem získat neoprávněnou či nelegální výhodu.“ [20] V rámci fraud managementu je však termín „podvod“ využíván v širším slova smyslu, a úzce souvisí s navrhováním nejrůznějších opatření, které slouží k prevenci podvodů a korupce ve společnosti, a to ze strany vlastních pracovníků organizace. Na tyto opatření v podobě prevence jsou dnes vynakládány v Česku značné finanční prostředky, avšak je nutné si uvědomit, že podvody a korupce způsobují společnostem nemalé finanční ztráty, a proto jsou tyto vysoké náklady odůvodněné. V rámci preventivních opatření je možné se v případě podnikatelské praxe inspirovat i u jiných společnost či si najmout na tuto oblast dokonce i poradenskou firmu, která se na zmíněnou problematiku orientuje. Lze konstatovat, že společnosti v České republice v posledních letech věnují prevenci dostatečnou pozornost a nepodceňují ji.

[20] ČESKÁ REPUBLIKA. Zákon č. 140/1961 Sb., trestní zákon: Trestní zákon. In: *Sbírka zákonů ČR*. 1961.

5 FRAUD MANAGEMENT

Ve všech oblastech podnikání, kde zaměstnanci přicházejí do styku s finančními prostředky nebo mohou nějakým způsobem o finančních prostředcích rozhodovat či ovlivnit jejich použití, dochází v určité míře ke zneužívaní postavení konkrétních zaměstnanců, které vyúsťuje ve zneužití daného postavení, znalostí, přístupu k informacím a ve výsledku pak k finančnímu poškození zaměstnavatele.

Toto se tyká především (ale ne pouze) takových sektorů podnikaní, ve kterých se pohybují velké objemy finančních prostředků, ať již v podobě jednorázových zakázek nebo ve formě menších, ale opakovaných finančních transakcí. Namátkově můžeme jmenovat např. telekomunikace, zdravotnictví, pojišťovnictví, bankovnictví, ale i veřejný sektor, kterým, byť není podnikatelsky orientován, protečou obrovské finanční prostředky. V současné době již mají subjekty soukromé i veřejné sféry poměrně dobře zpracované a nastavené procesy pro nakládání s finančními prostředky a současně i procesy, které vymezují chování zaměstnanců v těch oblastech, které mají na finanční hospodaření vliv.

Stále více subjektů se začíná zabývat otázkou, jak ověřit, zda i při dodržení všech nastavených procesů a kontrolních mechanismů nedochází k situacím, kdy zaměstnanci cíleně zpronevěřují finanční prostředky anebo svým chováním, ať již vědomým nebo nevědomým, nezpůsobují finanční ztráty.

V této oblasti se pak uplatňují řešení a nástroje z kategorie Fraud detection, které umožňují analyzovat jednotlivé obchodní případy, transakce, činnosti a chování jednotlivců a porovnat je jak mezi sebou, tak na konkrétní procesy a prostředí, ve kterém vznikly, tak i z pohledu multidimenzionálních statistických analýz a objevit tak případy, které byť samostatně nebo i ve skupině působí zdánlivě neškodně a v pořádku, ale ve skutečnosti je za nimi skryto podvodné chovaní.

Nejtěžším aspektem v boji proti podvodům, je jejich identifikace. V oblasti telekomunikací je takovým podvodem např. hovor, za který nebylo zaplaceno – krádež služby. Podvod může mít různé formy, od pokusů o prolomení systému z obývacího

pokoje až po organizované skupiny. Společnosti musí čelit všem těmto hrozbám, a proto se systémy pro odhalování tohoto chování stávají stále komplexnější.

Mezinárodní společnosti odhadují, že podvodné jednání je přivádí o 3 % až 6 % zisku. Autoři článku „Fraud Management System in Telecomunications: a practical approach“ definovali přístup „3M“ pro snadnější uchopení podvodného jednání v oblasti telekomunikací.

Důvod páchání podvodu.

- Podvod, jehož cílem není zisk, ale využívání určité služby s cílem vyhnout se nákladům spojeným s užíváním služby. Například zprostředkování služby přátelům nebo její využívání pro soukromé účely.
- Podvod spojený se ziskem – Means – způsob, kterým je naplněn prvotní motiv.
- Prodej hovorů s vyšším tarifem (např. mezinárodní hovory) pod cenou se záměrem vyhnout se platbě operátorovi.
- Surfování: použití služby někoho jiného, které mohou být dostupné např. zkopírováním SIM karty (klonování) nebo nelegálním získáním přístupových detailů.
- Přístup k citlivým informacím – zahrnuje cenné informace (např. detaily o VIP klientech, přístupová hesla, ...) a jejich prodej externím subjektům. Tento způsob podvodu je prováděn převážně interně.
- Krádež obsahu – zaměřuje se na získávání „obsahu s vysokou hodnotou“ (videa, vyzváněcí tóny, hry) zdarma.

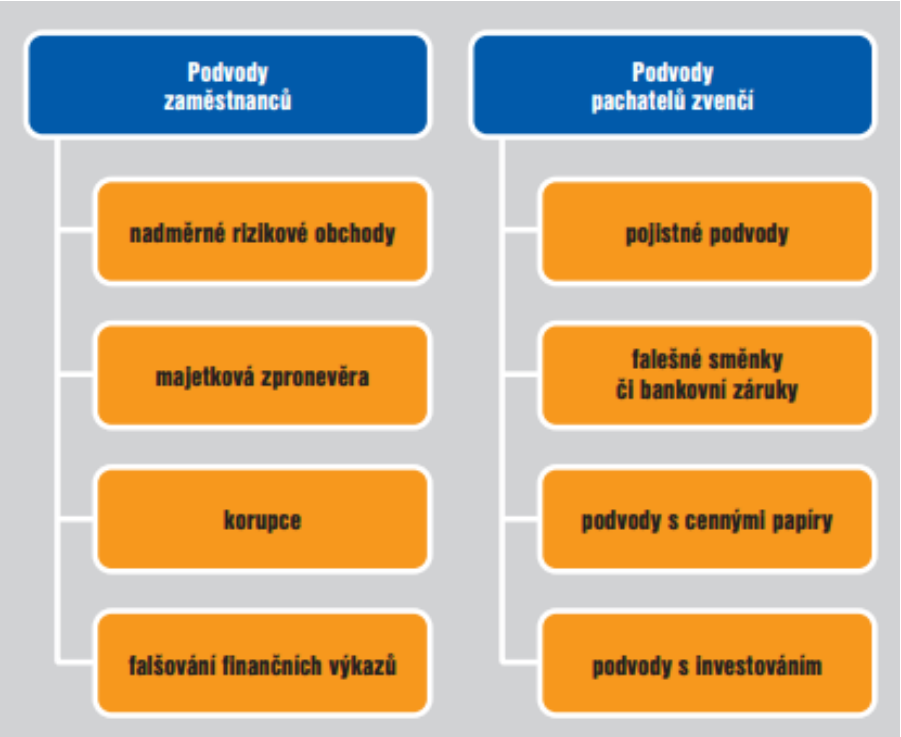
Obecné metody podvodů:

- Předplatné – získání předplatného s falešnými doklady a systematické vyhýbání se placení
- Podvod technického původu – náročnější podvod, který je založen na využití mezery nalezené v síti operátora
- Interní – zneužití informací z interních systémů
- Prodejní místo – prodejce manipuluje s informacemi o prodejích za účelem získání peněžní kompenzace od operátora

Je více než jasné, že podvody existují tak dlouho jak lidstvo samo, přičemž některé z nich jsou v současné době natolik důmyslné a promyšlené, že dokonce způsobují obdiv než pohoršení. Zločinci jsou mnohem nápadnější, čím důmyslnější bezpečností systém musí překonat v podniku. Finanční podvod je možné definovat jako *„nenásilný útok proti jednotlivci či společnosti, jehož výsledkem je finanční ztráta. Finanční podvody lze podle hlediska, kdo je pachatelem, rozdělit do dvou skupin: podvody zaměstnanců a podvody spáchané pachateli zvenčí“.* [21] Nejčastější podvody jsou prezentovány prostřednictvím Obr 3, přičemž zcela samostatně stojí praní špinavých peněz, počítačové podvody či krádeže identity, aj. Ze strany zaměstnanců se nejčastěji tedy jedná o nadměrné rizikové obchody, majetkovou zpronevěru, korupci či falšování finančních výkazů. Z hlediska zaměstnavatelů jde poté o pojistné podvody, podvody s cennými papíry, falešné směnky či podvody s investováním anebo také falešné bankovní záruky.

[21] BLAŽKOVÁ, L. Fraud management. *Statsoft.cz* [online]. 2015 [cit. 2017-05-09]. Dostupné z: http://www.statsoft.cz/file1/PDF/Fraud_management.pdf

Obrázek 1: Finanční podvody podle pachatele:



Zdroj[22]

Základem fraud managementu je z teoretického hlediska především identifikace příležitostí neboli určení klíčových oblastí, v rámci, kterých může k podvodu ve společnosti fakticky dojít. V tomto případě je nutné pozornost orientovat primárně na ty oblasti, u kterých je největší pravděpodobnost toho, že opravdu nastanou, a kde je taktéž dopad tohoto podvodu nejzávažnější, ať již z hlediska finanční ztráty, právních důsledků či poškození dobrého jména firmy, aj. Jednou z nejvíce významných oblastí jsou v současné době samozřejmě informační technologie, kdy je zapotřebí zabránit vzniku neoprávněného přístupu do systému firmy, neoprávněné změně práv či narušení integrity jak dat, tak i bezpečnostního systému. Je nutné upozornit na to, že systém musí být bezpečný vůči útokům zvenčí a taktéž i zevnitř – ze strany vlastních pracovníků organizace. Každý podnik musí tak zabezpečit správné nastavení interních bezpečnostních opatření a předpisů a také ochranných mechanismů, která zamezí

[22] BLAŽKOVÁ, L. Fraud management. *Statsoft.cz* [online]. 2015 [cit. 2017-05-09]. Dostupné z: http://www.statsoft.cz/file1/PDF/Fraud_management.pdf

vzniku podvodu. Jen tak může mít poté firma přehled o aktuálních podvodech. 23 Je nutné upozornit na to, že žádný systém ani dnes neposkytuje vůči neustále vznikajícím podvodům tzv. absolutní ochranu, a proto je nutné pravidelně kontrolovat, zda je systém dostačující, a patřičně ho poté aktualizovat a rozšiřovat o nové, žádoucí prvky. „S nástupem počítačů, elektronických transakcí a platebních karet se jako vhodné nástroje fraud managementu ukazují také moderní metody pro data mining.“ Jako nejvíce účinný způsob, kterým je možné rizika vznikající s podvodnou činností řídit, je těmto podvodům v praxi předcházet. Pokud podnik nastaví vysoká bezpečnostní opatření v podniku, pro řadu podvodníků je jejich obcházení z finančního hlediska nákladné, rizikové či pracné, a raději se o podvod poté nepokusí či pokusí, ale jinde. Míra podvodů může být ve společnostech snižována také prostřednictvím vzdělávání pracovníků, a to v podobě jejich školení, kde pracovníci získají patřičné informace o různých typech podvodů, přičemž poté jsou schopni mnohem rychleji tyto podvody odhalit a upozornit na ně, a jsou i mnohem více ostražití. Takto vyškolení pracovníci poté ví, jak na podvody zareagovat.

Společnost FICO vyvinula řešení Falcon Fraud Manager, které je využíváno pro odhalování podvodů spojených s kreditními/debetními kartami. Řešení je postaveno na servisně orientované architektuře a využívá pokročilých analytických technik, které jsou vyvíjeny na základě miliard informací o jednotlivých transakcích, které byly s kreditními kartami uskutečněny.

Řešení Falcon Fraud Manager zahrnuje:

- Patentované řešení pro profilaci držitelů karet – Identifikuje klíčové transakce pro každého držitele karty, aby bylo možné rozeznat neobvyklé chování, např.: nezvyklé výdaje
- Modelovací technika – neuronové sítě – Patentované analytické technologie, které poskytují prediktivní modely na základně transakčních dat z profilu držitele karty

[23] BLAŽKOVÁ, L. Fraud management. *Statsoft.cz* [online]. 2015 [cit. 2017-05-09]. Dostupné z: http://www.statsoft.cz/file1/PDF/Fraud_management.pdf

- Modely pro různé skupiny držitelů karet – Nástroj obsahuje data napříč tisíci držiteli karet a tvoří tak obrovskou základnu znalostí o vzorech podvodného chování, které jsou typické pro různé oblasti a portfolia.
- Přiřazování skóre jednotlivým transakcím – Analyzuje každou transakci, aby bylo možné zjistit riziko podvodných činností. Určí skóre, které indikuje pravděpodobnost toho, že účet je podvodný.
- Správa pravidel

6 MOŽNOSTI OBRANY PROTI FRAUDŮM ZE STRANY VEDENÍ FIRMY

6.1 Dopad nekalého jednání na společnost

Je více než jasné, že závažnost činů, které páchají zaměstnanci proti hospodářským zájmům své společnosti, je vysoká, a proto je nutné nyní pozornost orientovat nejenom na dopady hospodářské kriminality, ale taktéž na možnou obranu proti těmto nežádoucím aktivitám pracovníků.

Společnost jako taková má dnes řadu možností, jak se proti nežádoucím aktivitám svých pracovníků, které vedou k hospodářské kriminalitě, aktivně bránit.

Dnes je velmi prudký rozvoj podnikatelské činnosti, ke kterému v České republice došlo po roce 1989, doprovázen řadou změn nejrůznějších legislativních norem, které podnikání regulují, a také zcela novými typy kriminality, které není ani dnes možné dostatečným způsobem a s dostatečným předstihem ani předvídat. Řada ekonomických subjektů si totiž v minulosti transformaci ekonomiky směrem od plánované na tržní vyložila dosti po svém, a proto je možné po sametové revoluci identifikovat nárůst v oblasti hospodářské kriminality. [24] Když se vezmou v potaz finanční ztráty, které vlivem hospodářské kriminality vznikají, dle průzkumu společnosti Pricewaterhousecoopers lze konstatovat, že 40 % podniků v České republice, které se setkaly s hospodářskou kriminalitou, přišli téměř min. o 1,5 mil. Kč. Obrovské škody mají podobu nejenom finančních dopadů daného podvodu, ale také např. i škod, které poté souvisí s nutností přerušení provozu v podniku, či náklady na tzv. nápravná opatření, prevenci či vyšetřování, platba pokut či vyplacené honoráře za právní vyřešení 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*

[24] FRYŠTÁK, M. *Hospodářská kriminalita z pohledu teorie a praxe*. Ostrava: Key Publishing, 2007. ISBN 9788087134344, s. 5 – 7.

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.“ [25]

6.2 Základní předpoklady pro omezení rizik

Zaměstnanci jsou hlavním zdrojem navyšování výkonnosti produktivity společnosti. Výběr zaměstnanců, umění je ovládat, komunikace a spolupráce s nimi je základní dovedností úspěšných manažerů.

Již John Rockefeller zastával názor, že schopnost řídit lidí je vlastnost, která se spolu se správným zaměstnancem dá koupit a proto, když má možnost najmou toho správného zaměstnance, je ochoten za něj zaplatit více než za cokoliv jiného.

Výběr zaměstnanců je absolutně klíčovým okamžikem, když se rozhoduje, zda firma bude úspěšná či ne. Bez klasifikovaných zaměstnanců, se správným přístupem a morálkou není možné dosáhnou úspěchu. A právě při přijímání zaměstnanců dochází k ředě chyb.

I dnes dochází k tomu, že řada manažerů nepřikládá dostatečný význam, koho do firmy přijímají. Mají tendenci, že méně významná pozice tím méně ostražitosti. Ale k podvodným jednáním dochází ve všech vrstvách společnosti.

Pokud manažéři nedodržují stanovená pravidla, při přijímání nových zaměstnanců, riziko ohrožení společnosti roste.

[25] Celosvětový průzkum hospodářské kriminality 2016: Zpráva za Českou republiku. *Pwc.com* [online]. 2017. [cit. 2017-05-09]. Dostupné z: https://www.pwc.com/cz/cs/hospodarska-kriminalita/assets/pdf/global-economic-crime-survey-2016-cz.pdf

Pokud dochází k tomu, že postupy se dodržují pouze formálně a jejich provádění nemá jednotný postup, společnosti vzniká riziko, že příjme rizikového zaměstnance.

Postupy a kompetence personálních pracovníků musí být jasně vymezeny a musí být bez výjimek dodržovány.

Základním pravidlem by měla být vysoká pozornost při přijímacím procesu, tento proces by měl být formalizován a maximální pozornost při tomto procesu pomůže snížit riziko při získáváni nových pracovníků.

6.3 Výběr zaměstnanců

Přijímací proces je rozhodujícím faktorem, zda společnost bude úspěšná nebo ne. Pečlivý výběr pracovníků má obrovský vliv na snížení pozdějších rizik spojených s nekalým jednání zaměstnanců.

Pokud chceme vybrat správného zaměstnance, musíme mít dostatečné množství informací. Zodpovědný pracovník by si měl vyžádat doklady o vzdělání, potvrzení o dosavadní praxi, strukturovaný životopis s přiloženým motivačním dopisem, písemné vyjádření z minulých pracovišť s hodnocením jeho předchozích vedoucích pracovníků.

Další dokument, který bych doporučil je výpis z rejstříků trestů a strukturovaný dotazník, který nám zodpoví celou řadu otázek, které nejsou součástí běžného pracovního pohovoru

Životopis

Z tohoto dokumentu můžeme získat celou řadu cenných informací. Především o osobním a profesním vývoji uchazeče.

Dotazník

Jedná se o pečlivě připravený dokument, kdy se společnosti může zeptat na otázky, které společnosti pomohou získat detailnější informace o uchazeči. Tento dotazník nám pomůže blíže poznat osobu uchazeče, jeho názory a postoje. Jak se zachoval v různých situací a jaká je jeho představa o jeho profesní budoucnosti.

6.3.1 Metody výběru zaměstnanců

Nejenom pozornost, ale také metody, které používáme při výběru zaměstnanců mají rozhodující vliv na úspěch při výběru uchazeče.

Hlavním dokumentem je životopis uchazeče. Dává nám ucelený seznam jeho předchozích zaměstnání, vzdělám, kursy a dovedností, které si uchazeč během svojí dosavadní kariéry osvojil. Součástí životopisu by měl být i motivační dopis, ve kterém by měl uchazeč uvést proč se o danou pozici zajímá, proč by měl být vybrán a čím převyšuje ostatní uchazeče.

Zodpovědný pracovník by se měl zaměřit na informace o vzdělávacích institucích, které uchazeč navštěvoval, zda úspěšně dokončil uvedené vzdělání, dobu, kterou strávil v předchozích zaměstnáních, jaké jsou časové intervaly mezi nimi nebo zda došlo k nějakým mezerám mezi jednotlivými zaměstnáními.

Personalista muže vzít v úvahu časté změny v zaměstnání, nerovnoměrný kariérní postup, neobvyklé způsoby ukončení pracovních poměrů.

Dotazník je dalším pomocným dokumentem, který po uchazečích většinou požaduje určité a přesné údaje. Při pohovorech se uchazeč může vyhnou odpovědím na určité otázky, proto dobře strukturovaní dotazník může odhalit celou řadu nepoctivých informaci.

Dalším zdrojem užitečných informací je test. Je ovšem třeba zvážit, zda je to vhodné. K testu bychom měli přistoupit pouze v případě, že hledáme odborníka na určitou pozici. Test nám přinese doplňkové informace o profesních kvalitách daného uchazeče.

Testy nezjišťují pouze odborné znalosti uchazeče, ale také jeho zájmy, fyzické schopnosti, duševní rozpoložení, chování, temperament apod.

6.3.2 Etika uvnitř společnosti

Velkým rizikem pro společnost znamená i přesvědčení některých vedoucích pracovníků, že právě v jejich společnosti se toto stát nemůže.

Polevení v pozornosti může nahrávat zaměstnancům, kteří plánují porušení pravidel uvnitř společnosti. Jestli vedoucí pracovníci chtějí aktivity zastavit nebo je omezit na akceptovatelnou míru rizika, měli by implementovat do mechanismů uvnitř společnosti opatření pro minimalizaci rizika podvodu.

Znamená to nastavení etických standardů ve společnosti. Etické standardy ve společnosti mají velký význam při snižování rizik podvodů ve společnostech. Důležitost etického kodexu je především v jasném vymezení, co kdo může a nemůže. A když se zaměstnanec ocitne v situaci, kdy si neví rady, kdy neví, jak reagovat na určitou situaci, právě etický kodex by mu měl pomoci správně reagovat. Etický kodex vlastně plní funkci regulátora. Má ale nejen regulační charakter. Jeho funkcí je i faktor motivační, aspirační. Je nástrojem k vyvažování těchto funkcí.

Další funkce etického kodexu:

- Ochraňuje zaměstnance před tlakem vedoucích pracovníků, kteří by po nich mohli požadovat nekalé jednání
- Kladné působí na veřejnost, vystupování společnosti je daleko více srozumitelné pro veřejnost
- Je důležitým nástrojem k vytvoření kladného pracovního prostředí
- Pomáhá vytvořit prostředí, kde otevřená komunikace není problém
- Kladné působí na zaměstnance a umožňuje jim více pochopit cíle vedoucích pracovníků

Etika je součástí lidského života od pradávna. Člověk se s ní dostává do kontaktu po celý život. Je součástí nejen pracovního, ale i osobního života jednotlivce. Asi nejstarší příklad etického kodexu je lékařská etika, Hippokratova přísaha. Ačkoliv tato přísaha nese Hippokratovo jméno, není úplně jasné, jestli byla dílem jeho nebo jednoho z jeho

žáků. Co je však důležité, je skutečnost, že již ve starověku byl etice přikládám velký význam.

Později, docházelo k zakládání cechů, profesních organizací, což prokazuje důležitost etiky a její významné místo ve společnosti.

Prokazování trestné činnosti zaměstnanců bývá často složité a může být velmi nepříjemné pro společnost. Nejen proto, že to může být velice nákladné, ale také to může snížit reputaci společnosti před veřejností. Obecné je tedy žádoucí, aby se těmto jednáním spíše předcházelo a dbal se velký důraz na prevenci. Prevence je vždy lepší než řešení případných následků. Proto k zabránění nekalých jednání zaměstnanců je třeba nastavení velmi spolehlivého vnitřního kontrolního systému, který pak se skombinuje s aktivním a strukturovaným vyhodnocováním rizik podvodů.

Velmi silnou obranou, v rámci prevence, jak zabránit podvodům je, jak jsem již uvedl strukturovaný vnitřní kontrolní systém. Ten by měl bát provozován přiměřeně k velikosti rizik. Vedení podniků by se mělo zaměřit na systém, který svou strukturou bude možné podvodníky odrazovat.

6.3.3 Rozdělení odpovědnosti

V každé společnosti by měla být jasně rozdělena odpovědnost. Vytvoření systému řízení a kontroly, které se budou podílet na účinném fungování vnitřních předpisů, odhalování a následnou nápravu podvodů.

Hlavním cílem těchto opatření je, aby všechny strany jasně rozuměly svým povinnostem, závazkům a interně i externě informovaly všechny příjemce programu a daly jasný signál všem stranám, že organizace má koordinovaný přístup k boji proti podvodům.

6.3.4 Školení

V rámci řízení rizik by se podniky měly zaměřit i na školení, odborné kurzy a zvyšování informovanosti svých zaměstnanců. Toto lze provádět formálně i neformálně. Příkladem formálního přístupu mohou být různá organizovaná školení, besedy nebo kurzy.

Neformální pojetí zahrnuje různé brožury, aplikace, plakáty nebo intranetové stránky.

6.3.5 Vnitřní kontrola

Funkční vnitřní kontrolní systém je nejúčinnějším nástrojem, jak omezit protiprávní jednáním na pracovišti. Jestli vnitřní předpisy a provádění kontrol jsou v podnicích nastaveny správně a důkladně a opakovaně prováděny, rizika, vedoucí z nekalých praktik zaměstnanců se podstatně sníží.

6.3.6 Oznamování podvodů

Sebelepší preventivní opatření nám nezajistí kompletní ochranu. Ke snížení následků podvodných praktik zaměstnanců se třeba tyto aktivity odhalit co nejdřív.

V případě správného etického prostředí ve společnosti je možně spoléhat i na pomoc z řad ostatních zaměstnanců, kteří můžou na původce nekalého jednání upozornit. Je důležité se zaměstnanci neustále komunikovat a zajistit, aby pochopily, že:

- Koho a kdy by měli informovat, pokud mají podezření, že se někdo dopouští podvodného jednání
- Měli naprostou důvěru k vedoucím pracovníkům, že se tato skutečnost bude prověřovat
- Měli jistotu anonymity, že případné oznámení neovlivní negativně jejich postavení v kolektivu

7 COMPLIANCE

V posledních pěti letech se v českém podnikatelském prostředí objevilo slovo doposud neznámé. Tímto slovem je Compliance. Mnoho českých společností zavedlo Compliance proto, že se jedná o dceřiné firmy nadnárodních společností a jako takové musí přijímat a dodržovat politiku svých mateřských společností. Evropské nadnárodní firmy, obchodující na americkém trhu, jsou nuceny integrovat do svých procesů ustanovení platná v USA na potírání nelegálního chování (například FCPA – Foreign Corrupt Practices Act, zákon proti podplácení zahraničních představitelů o boji proti úplatkářství, slouží jako základ trestněprávních a občanskoprávních trestů za poskytování nepřípustných výhod představitelům zahraničních vlád). Po zavedení Compliance v českém podnikatelském prostředí vyžadují tyto dceřiné společnosti zavedení společensky odpovědného chování i od svých subdodavatelů, to jsou v současnosti i malé a střední podniky.

Compliance Program, Corporate Compliance Policy, Corporate Compliance nebo prostě Compliance je společensko podniková věda, kterou chce určitá obchodní společnost nebo podnikatelské skupiny (korporace) spolu se svými zaměstnanci vyjádřit, že jejich chování je v souladu s etickými a právními pravidly.

Tyto pravidla zahrnují dodržování finanční a daňové integrity, ochranu životního prostředí a dodržování zaměstnaneckých vztahů (jak ve vztahu k zaměstnanci, tak i ve vztahu zaměstnanců mezi sebou) včetně zajišťování rovných příležitostí. Tento soubor vnitřních předpisů společnosti upravuje v zásadě veškeré oblasti fungování společnosti. Reguluje chování jak uvnitř společnosti s možnými dopady navenek i dovnitř společnosti, tak v obchodních, finančních, daňových vztazích i v dalších oblastech činnosti společnosti. Tato politika zásadně ovlivňuje úspěšnost společnosti jako celku. Proto je problematice Compliance věnována v současné době taková pozornost, a proto se programy Compliance staly nedílnou součástí firemní podnikatelské kultury. V případě selhání, některých ze zásad společnosti, pro ni může znamenat zásadní ohrožení její důvěryhodnosti a možné negativní dopady, které mohou ohrozit její fungování, a dokonce i existenci. Tzv. Compliance manageři spolu s podporou právního oddělení jsou tvůrci firemních standardů. Odpovědnost za dodržování této politiky

nemají pouze vedoucí pracovníci, ale všichni zaměstnanci, v rámci jednotlivých organizačních úseků.

Compliance je sice dobrovolně integrovaná politika a liší se podnik od podniku, avšak vždy mají jedno společné – jejich politika je založena na právních předpisech, které musí dodržovat. Jejich interní předpisy jsou až nástavbou nad těmito právními předpisy.

Právní předpisy v každé vyspělejší společnosti slouží jako regulační činitelé trhu. Při tvorbě a aplikaci vnitropodnikových pravidel je proto vždy nezbytné brát ohled na to, aby tyto akty byly v souladu s platnými právními předpisy.

Vnitřní předpisy jsou písemné normativní nařízení firmy, zpravidla vydávané vedením společnosti prostřednictvím statutárního orgánu. Neřeší žádnou určitou situaci nebo problém, ale dávají obecný návod řešení možných konkrétních situací.

V boji proti hospodářské kriminalitě je možné využít také vnitřní předpisy a program Compliance. V rámci svých vnitřních předpisů může podnik jasně a přesně definovat konkrétní podmínky, které se týkají organizačního řádu, pracovního řádu, etického kodexu, aj. V tomto případě hraje velmi důležitou roli právě etické kodex. *„Požadavky na etické chování firem a zaměstnanců ze strany zákazníků, obchodních partnerů i širšího společenského prostředí dlouhodobě rostou. Tím se zvyšuje i význam etického kodexu organizace jako řídicího nástroje a součásti její kultury. Hlavním důvodem k vytvoření etického kodexu je jasně stanovit principy a pravidla etického jednání zaměstnanců, ať již navenek organizace nebo vůči sobě navzájem. K dalším důvodům patří zakotvit důležité zásady profesionálního postupu, posílit profesní identitu a odpovědnost zaměstnanců a nastavit normy sloužící k hodnocení osob.“* [26] Co se týče programů Compliance, tak ty se staly již nedílnou součástí podnikové kultury řady společností v České republice. Lze konstatovat, že problematika Compliance je vnímána také jako součást mnohem širší kategorie, a to je společenská odpovědnost firem, což je dnes jeden z nejdůležitějších faktorů mající vliv na ekonomický úspěch

[26] URBAN, J. Jak vytvořit etický kodex organizace. *Ihned.cz* [online]. 2011 [cit. 2017-05-09]. Dostupné z: http://kariera.ihned.cz/c1-53354960-jak-vytvorit-eticky-kodex-organizace

společnosti na trhu. [27] Důležitým předpokladem, který vede následně v praxi k efektivnímu uplatnění pravidel definovaných v rámci Compliance programu, je primárně disciplinovanost a také zásadovost celého managementu firmy, což poté slouží jako vzor pro všechny pracovníky firmy.

Compliance je jedním ze slov, které nepřekládá. Znamená nastavený způsob jednání, která jsou v souladu s pravidly a zákony. Slovo compliance se často vyskytuje své spojení se slovem governance a risk nebo ve zkratce GRC (Governance, Risk, Compliance).

Hlavním cílem governance je kvalifikované a odpovědné řízení a vedení společnosti. Risk se zabývá řízením rizik. Pojmy s sebou velmi úzce souvisejí.

Aby byly kompetence ve společnosti nastaveny správně, je třeba určit vhodnou osobu, která bude nastavená pravidla aktualizovat a dohlížet na jejich dodržování. Dohlížet především nad externími předpisy – zákony, nařízení a vyhlášky. A samozřejmě dohlížení na předpisy interními – interní předpisy, politika společnosti, hodnoty společnosti, dobrovolně přijaté principy

Osoba, která je zodpovědná na compliance ve společnosti se musí zabývat především zajištěním analýzy rizik, jejichž cílem je především rozlišit rizika na méně závažná, závažná a pravděpodobná rizika od těch méně pravděpodobných.

Je na této osobě také určit, jaké riziko je přijatelné a kdy musí nastoupit kontrolní mechanismy.

Koncept compliance ve společnosti nastaví hlavní oblasti, které se musí popsat v interních předpisech. Toto musí být snadno pochopitelné, srozumitelné a výstižné. Tyto nařízení si není možné vykládat několika rozdílnými způsoby. Nikdy se nesmí vydávat zpětně. V naších podmínkách je nečastější formou takového předpisu třeba pracovní řád nebo organizační řád.

[27] KOUKAL, P. Korporátní pravidla Compliance a nový trestní zákoník. *Ihned.cz* [online]. Praha, 2010 [cit. 2017-05-09]. Dostupné z: http://pravniradce.ihned.cz/c1-40730210-korporatni-pravidla-compliance-a-novy-trestni-zakonik

Compliance je podloženo právními úpravami České republiky týkajících se soutěžního práva, tj. práva ochrany hospodářské soutěže, dále práva obchodního (nekalá soutěž) i trestního. V případě, že by firma, nebo její zaměstnanci jednali protiprávně nebo neeticky, vedlo by toto chování k negativním obchodním důsledkům jako například právní postihy, trestní stíhání, ukončení obchodního vztahu apod. Proto je politika Compliance vnímána jako nedílná součást tzv. Společenské odpovědnosti firmy (Corporate Social Responsibility – CSR), která začíná být postupně považována za stěžejní faktor ekonomicky úspěšně fungující společnosti. Pojmem CSR je míněno dobrovolné integrování sociálních a ekologických hledisek do každodenních firemních operací a interakcí s firemními stakeholders.

Společnosti, aniž by přijaly jakékoliv standardy by si měly být vědomy, že by se měly chovat seriózně, že by se ke svým zákazníkům a partnerům měly chovat s náležitou péčí (odpovědně), starat se o své zaměstnance, chránit životní prostředí a další. Odpovědné podnikání by mělo znamenat nejenom myslet ekonomicky, ale i začlenit sociální a ekologické aspekty do své podnikatelské činnosti. Dalo by se tedy říci, že Compliance ve své podstatě nemůže být špatné nebo spíše nemělo by být špatné. Může se však stát, že jeho zavedení ve firmě může mít negativní důsledky. Pokud se tato politika „přežene“, může opravdu působit škodlivě. Ale jak poznáme hranici, kdy je tato politika prospěšná a kdy už ne?

Compliance by se mělo vytvářet pro každý podnikatelský subjekt v každém konkrétním prostředí individuálně. V České republice je například předávání darů v rámci obchodního jednání častým jevem vyjádření díků a nemusí mít žádné vedlejší postranní úmysly. Odmítnutí daru (k němuž je obchodník – prodejce přinucen politikou Compliance) tak může druhou stranu někdy až dokonce urazit. To pak může mít za následek pro obchodníka ztrátu příští zakázky.

Samozřejmě, že je problém stanovit, kdy ještě jde o dar, který pozbývá hlubšího významu, a kdy svým jednáním zamýšlíte určité zvýhodnění do budoucna.

8 POČÍTAČOVÁ BEZPEČNOST

8.1 úvod do počítačové bezpečnosti

Počítače spolu s dalšími elektronickými zařízeními jsou nedílnou součástí domácností i firem. Internet je absolutně neodmyslitelnou součástí našeho života a jeho používání bereme jako samozřejmost. Každodenní používání internetu v nás budí dojem, že se nemůže nic stát. Ale opak je pravdou. Používání počítačů připojeným k internetové síti spolu s mnoha výhodami přináší celou řadu rizik a nástrah.

Počítače a internet používáme nejen pro zábavu, ale především i v profesním životě. Komunikace s vnějším okolím firmy, uzavírání smluv, komunikaci s bankovními ústavy atd.

Je důležité si uvědomit, jaká rizika tato činnost přináší a zavést potřebná opatření, jak tato rizika omezit na přijatelnou úroveň.

V minulosti se tímto zavívali pouze počítačoví odborníci, ale vzhledem s tomu, jak počítače a internet pronikly do každodenního života, žádali se o bezpečnosti při užívání počítačů zabývat i běžní uživatelé.

Vynalézavost a postupy osob, které podniky ohrožují prostřednictvím počítačů se vyvíjejí velmi rychle, proto každý manažer by měl věnovat pozornost ochraně svých počítačových zařízení.

Informace, které jsou uloženy ve firemních počítačích by měly splňovat následující parametry:

- Dostupnost – data jsou dostupná autorizovaným uživatelům.
- Integrita – změnu dat smí provádět pouze autorizovaní uživatelé.
- Důvěrnost – přístup k datům, mají pouze autorizovaní uživatelé.
- Odpovědnost – uživatelé jsou odpovědni za své aktivity.

8.2 Historie počítačové bezpečnosti

Jedním z prvních článků ohledně počítačové bezpečnosti byl uveden v USA v 70. letech. V období, kdy vznikla síť Arpanet, která bylo předchůdcem internetu. Jednalo se o připojení několika desítek počítačů v armádním prostředí. A napadení této sítě je považováno za jeden z prvních útoků na počítač.

8.3 ochrana dat

Domácnosti a podniky, kteří používají počítače mají informace ve svých zařízeních uložených na disku ve formě počítačových souborů.

Ochranu počítačových dat můžeme rozdělit na:

- fyzickou ochranu dat,
- ochrana logického přístupu,
- ochrana před zničením,
- ochranu uložených dat,
- ochranu přenášených dat.

8.3.1 fyzická ochrana dat

Tato ochrana má za úkol ochránit data před tím, aby se k nim nedostala neoprávněná osoba. Žádná neoprávněná osoba by neměla mít přístup k uložišti dat, aby je mohla fyzickou silou zničit. Důležité je také chránit data před možným zničením působením živelných pohrom.

8.3.2 ochrana logického přístupu

Tento druh ochrany by měl zabezpečit ochranný operační systém. Pomocí tohoto systému můžeme nastavit práva k přístupu dále můžeme nastavit možnost ověření uživatele. To znamená, že kdokoliv chce přístup k datům, musí elektronicky ověřit svoji totožnost. Pokud ochranným protokolem neprojde, přístup mu je zamezen.

Přístup může být zabezpečen vlastnictvím, znalostí nebo vlastnictví. Přistup je pak povolen pouze uživateli, který vlastní bezpečnostní čipovou kartu, může se prokázat otiskem prstu, zná přístupové heslo atd.

8.3.3 ochrana před zničením

Ochrana dat může způsobit ochromující škody pro jakoukoliv sopečnost. Je třeba kontrolovat a monitorovat osoby, které přicházejí do budovy. Existuje celá řada opatření. Můžou to být bezpečností kamery, snímače pohybu. Může to být vchodový systém nebo jak bylo běžné i minulosti použití vrátného.

Záleží také na ochraně místnosti, kde jsou důležitá data uložena. Hlavní servery, uložiště dat, by neměli být opatřeny okny a jejich vchod by měl být zabezpečen ochrannými dveřmi. Dále klíče k vchodovým dveřím by měly být bezpečnostní, aby si kdokoliv nemohl opatřit jejich kopii.

8.3.4 ochrana uložených dat

Může se stát, že se pachatel dostane k uloženým datům i přes výše uvedené kontroly. V tomto případě by měl být nastaven vyšší stupeň kontroly, který tak zamezí nepovolaným osobám k přístupu k datům, které by mohli poškodit nebo zneužít.

Pro toto opatření známe dva způsoby:

- kryptografie,
- kryptoanalýza.

Kryptografie je věda, která se zabývá kódováním a dekódováním dat. Naproti tomu Kryptoanalýza má za úkol analyzovat data, která byla zašifrována a algoritmy.

8.3.5 ochrana přenášených dat

Existuje celá řada, jakým způsobem mohou být data přenášena. Mezi nejčastější způsoby patří elektronická média, papírová média a počítačová síť. Mezi nejvíce ohrazená data samozřejmě patří data přenášena počítačovou sítí. Největší ohrožení spočívá v kompromitování nebo modifikování těchto dat.

Jednejme z řešeních těchto problémů je použití digitálního otisku nebo digitálního podpisu.

8.4 útočníci na počítače

Osoba, která neoprávněné získá přístup k počítači nebo počítačovým datům je velkým nebezpečím pro každou společnost. Tyto útočníky můžeme dělit z několika hledisek.

Z hlediska polohy útočníka, z hlediska odbornosti útočníka a také podle cíle útočníka.

Útočníci z hlediska polohy jsou:

- Insider – jedná se o osobu, která má oprávnění sdílet soubory a snaží se o překročení nastaveným oprávnění nebo pravomocí.
- Outsider – tato osoba oprávnění k přístupu k datům nemá – snaží se odhalit nedostatky v zabezpečení a tím se dostat k neoprávněnému přístupu.

Podle odbornosti pachatele můžeme útočníky dělit na.

- amatéry,
- profesionály.

Amatéři obvykle nemají veliké znalosti a o útoky se jen pokoušejí. Většinou se snaží zkopírovat chyby, které již někde byly zveřejněny.

Profesionálové mají většinou značné vědomosti a patřičné vybavení, aby mohli konkurovat bezpečnostním oddělením ve společnostech.

8.5 Zabezpečení počítačů

Hlavní roli v tom, zda zabezpečení počítačů ve firmě bude úspěšné nebo ne hrají odpovědní pracovníci a uživatelé počítačů. Příležitost těm, kteří by chtěli zůstat užitek z neoprávněného přístupu k datům může dát každý i sebe menší chybou nebo nepozorností.

Odpovědní pracovníci by měli dbát především na prevenci. Měli by se zabývat také tím, kdo a proč by mohl mít zájem se k počítačům neoprávněně dostat a podle toho taky nastavit bezpečnostní systémy.

Základním pravidlem je pravidelná aktualizace softwaru. Uživatelům bez hlubších znalostí se doporučuje povolovat nastavené aktualizace, které by měli zabránit těm základním útokům ze strany neoprávněným osob.

Podstatnou roli hraje také tvorba hesel. Měla by se volit vhodná délka hesel a každé heslo by mělo obsahovat i několik znaků. Delší heslo s více znaky většinou znamená bezpečnější ochranu dat ve svém počítači.

Velkou chybou ale ne zcela ojedinělou je, že uživatelé si zapisují přístupová heslo na papír.

Podstatou přístupového hesla k počítači je že má být tajné. Uživatel by měl heslo držet v tajnosti a mít jistotu, že k němu nikdo nemá přístup. Existuje několik možností pro uživatele, kteří si jejich hesla nejsou schopni zapamatovat. Jedním ze způsobů je klíčenka Keepass.

Keepass je bezplatný program, do kterého si uživatel může vložit všechny jeho hesla. A přístup je pak umožněn pomocí jednoho hesla.

Pro vyšší bezpečnost se při tvorbě hesel doporučuje:

- Používat hesla nejméně o délce cca 10 znaků.
- Hesla by měla být složená z velkým i malých písmen doplněných o číslice.
- Heslo by si měl uživatel pamatovat, popřípadě používat zabezpečený software pro správu hesel.

- Pro různé účty používat různá hesla.

Zabezpečení pomocí antivirů

Programy, které mají za úkol ochraňovat náš počítač mají dlouhou historii. Tyto programy – antivirové programy by počítače měly chránit především pře malware and spyware.

Každý počítač ve všech firmách by měl mít oficiální, registrovaný antivirový program. Každý uživatel by měl po nainstalování takového programu provést kontrolu počítače.

Spyware

Spyware je program, který bez povšimnutí shromažďuje informace o uživateli osobního počítači. Zaznamenává jeho hesla, jména i stránky, které uživatel navštěvuje.

Tento virus je obvykle součástí nějakého programu, která si uživatel uložil, aniž by použit vhodný antivirový program.

Proto je důležité, aby každý uživatel pozorně četl všechny informace před nainstalováním neznámého programu.

Přihlašování k počítači

Podle průzkumů většina uživatelů k přihlášení k počítači používá osobní informace. Jedná se o nejrozšířenější chybu, a to může ohrozit fungování celé sopečnosti.

Ochrana počítače obecně

V současné době by si uživatelé, ale především firmy měli seznámit s počítačovou bezpečností a jak ochraňovat svoje data. Každý uživatel, odpovědný pracovník by měl vědět, jak ochraňovat svoje data.

ZÁVĚR

Práci s lidmi, zaměstnanci se ani v současné době nadává mnoho významu. Celé řada českých manažerů si myslí, že lidský faktor není tolik důležitý. Pravidla, jejich nedodržování a také jejich nesprávné nastavení je velmi častým problémem a je to zapříčiněno buď neschopným vedením společnosti nebo že se příjmu pracovníků neklade velký důraz.

Výsledkem pak bývá, že provádění kontrolních systémů není správné. Může za to, že tyto činnosti provádějí nekompetentní zaměstnanci nebo že svojí práci neodvádějí správně.

Dalším problémem, který může nastat je, že tyto pracovníci neodvádějí svoji práci správně.

Současný systém, prostředí, ve kterém žijeme je ovlivněn velikým množstvím globálních změn. Soutěžení, aby v něm jedinec obstál, tlak na zaměstnance na řídící pracovníky.

Hospodářská kriminalita patří mezi závažné a negativní společenské jevy, které ohrožují již i samotnou existenci společnosti. Rizika, která jsou s touto problematikou spojena, je nutné brát tudíž vážně a patřičně na ně reagovat. I přes rostoucí význam a uplatňování etických kodexů či rozšiřování compliance programů či uplatňování fraud managementu je možné stále v této oblasti identifikovat pro podnik velkou hrozbu, čímž se společnost stává mnohem více zranitelnou.

Cílem této práce bylo nejprve popsat prostředí, ve kterém se trestná činnosti zaměstnanců páchá. Kdo je tím pachatelem, jaké důvody ho to k tomuto jednání vedou a jak jim šéfové firem můžou zamezit.

V této práci jsem uvedl několik příkladů, jak je možné těmto aktivitám předením a jakým způsobem se před nimi podniky můžou chránit.

SEZNAM POUŽITÝCH ZDROJŮ

Seznam použitých českých zdrojů:

BLAŽKOVÁ, L. Fraud management. *Statsoft.cz* [online]. 2015 [cit. 2017-05-09]. Dostupné z: http://www.statsoft.cz/file1/PDF/Fraud_management.pdf

Celosvětový průzkum hospodářské kriminality 2016: Zpráva za Českou republiku. *Pwc.com* [online]. 2017. [cit. 2017-05-09]. Dostupné z: https://www.pwc.com/cz/cs/hospodarska-kriminalita/assets/pdf/global-economic-crime-survey-2016-cz.pdf

ČESKÁ REPUBLIKA. Zákon č. 140/1961 Sb., trestní zákon: Trestní zákon. In: *Sbírka zákonů ČR*. 1961.

FRYŠTÁK, M. *Hospodářská kriminalita z pohledu teorie a praxe*. Ostrava: Key Publishing, 2007. ISBN 9788087134344.

CHROMÝ, J. *Násilí na pracovišti. Charakteristika, rizikové faktory, specifické formy a právní souvislosti.* Praha: Wolters Kluwer, 2014. 216 s. ISBN 978-80-7478-552-8.

INTERNÍ AUDIT A STRUKTURÁLNÍ FONDY EU. *Interniaudit.cz* [online]. 2013 [cit. 2017-05-09]. Dostupné z: http://www.interniaudit.cz/download/clenstvi/casopis/auditor0806.pdf

KOUKAL, P. Korporátní pravidla Compliance a nový trestní zákoník. *Ihned.cz* [online]. Praha, 2010 [cit. 2017-05-09]. Dostupné z: http://pravniradce.ihned.cz/c1-40730210-korporatni-pravidla-compliance-a-novy-trestni-zakonik

MATOUŠKOVÁ, I. *Aplikovaná forenzní psychologie*. Praha: Grada Publishing, 2013. ISBN 9788024784229.

Odbor hospodářské kriminality. *Policie.cz* [online]. 2017 [cit. 2017-05-09]. Dostupné z: http://www.policie.cz/clanek/sluzby-odbory-skupiny-odbor-hospodarske-kriminality.aspx

PROVAZNÍKOVÁ, R. Patologie v pracovních vztazích – mobbing. *Cssz.cz* [online]. 2013 [cit. 2017-05-09]. Dostupné z: http://www.cssz.cz/cz/casopis-narodni-pojisteni/archiv-vydanych-cisel/clanky/renata-provaznikova-patologie-v-pracovnich-vztazich-mobbing-1.htm

TOMKOVÁ, V. Výzkum ekonomické kriminality. *Ok.cz: Institut pro kriminologii a sociální prevenci v Praze* [online]. Praha, 2004 [cit. 2017-05-09]. Dostupné z: http://www.ok.cz/iksp/docs/308.pdf

URBAN, J. Jak vytvořit etický kodex organizace. *Ihned.cz* [online]. 2011 [cit. 2017-05-09]. Dostupné z: http://kariera.ihned.cz/c1-53354960-jak-vytvorit-eticky-kodex-organizace

SEZNAM OBRÁZKŮ, TABULEK A GRAFŮ

Seznam obrázků:

Seznam grafů

BIBLIOGRAFICKÉ ÚDAJE

Jméno autora: Václav Pavlis
Obor: EHS
Forma studia: kombinovaná

Název práce: Analýza možných aktivit zaměstnanců směřujících proti hospodářským zájmům zaměstnavatele. Možnosti obrany a prevence proti takovému jednání ze strany managementu firmy

Rok: 2017
Počet stran textu bez příloh: 43
Celkový počet stran příloh: 0
Počet titulů českých použitých zdrojů: 12
Počet titulů zahraničních použitých zdrojů: 0
Počet internetových zdrojů: 12
Vedoucí práce: Dr, Jindřích Nový Ph.D.