

Personální bezpečnost v IT, prevence vnitřní počítačové kriminality

Průzkum PricewaterhouseCoopers (dále PwC) ukazuje, že hospodářská kriminalita stále patří k největším problémům podnikání ve světě. V České republice je jevem mnohem běžnějším, než bychom si mysleli. **Celkem 48 % respondentů uvedlo, že za posledních 24 měsíců se jejich společnost stala obětí hospodářské kriminality.** To je jednoznačně nad regionálním i celosvětovým průměrem (38 %, respektive 37 %). V porovnání s výsledky předchozího průzkumu z roku 2011 jde o výrazný nárůst, a to o více jak dvě třetiny. Celkem 44 % organizací, které čelily hospodářské kriminalitě, odhadlo, že jejich finanční ztráty dosáhly 100 tisíc amerických dolarů nebo více.

Majetková zpronevěra tradičně zůstává nejběžnějším typem hospodářské kriminality (80 %). Pachatelé však vyhledávají stále nové způsoby, jak společnosti poškodit, např. narůstá počítačová kriminalita.

Nepoctivý, neloajální zaměstnanec představuje pro firmu jedno z největších rizik, přičemž důsledky jeho skutků jsou větší než přímá majetková újma. Navíc musíme počítat s velkou latencí, nižší objasněností a nesmírnými škodami. Míra ohrožení nesouvisí s velikostí, prosperitou ani zaměřením firmy či organizace.

Výzkum nezahrnuje neloajální jednání, které není trestné, tak lze předpokládat jeho vyšší výskyt než u hospodářské kriminality. Přesto podnik poškozuje materiálně - ušlým ziskem, anebo morálně - ztrátou dobrého jména. Nezanedbatelný je i vliv na morálku zaměstnanců. V tomto ohledu bychom rádi upozornili na fakt, že negativní dopad na morálku zaměstnanců může být příčinou dalších následných podvodů, kterých se frustrovaní či demotivovaní zaměstnanci dopouštějí. Slovy „dělají to všichni“ nebo „patří jim to“ si podvodníci již mnohokrát zdůvodnili své první podvodné jednání!

Zda pracovník stávající situaci a příležitost zneužije, záleží především na jeho morální integritě, na jeho charakterových vlastnostech.

Pojmy „interní firemní kriminalita“ a „personální bezpečnost“ se týkají všech firem a organizací. Ty musí permanentně řešit problém, jak ochránit společnost před nepoctivými, neloajálními a nespolehlivými spolupracovníky.

Specifika počítačové kriminality

V českých firmách zejména výrazně stoupá počet podvodů formou počítačové kriminality. Zvláště nebezpečné pro firmu je proniknutí do utajovaných firemních tajemství, zcizení vynálezů, projektů, technologií, osobních údajů nebo poškození dobrého jména a obchodní značky společnosti. V roce 2011 představovala počítačová kriminalita zhruba 13 procent z celkových podvodů v českých firmách. **V roce 2014 ale její podíl skočil až na 31 procent.** To je výrazně více než průměr této formy podvodů ve firmách střední a východní Evropy (ten je 22 procent), ale i ve srovnání s celosvětovým průměrem (24 procent). **Zhruba 80% incidentů v této oblasti má na svědomí tzv. insider (tedy člověk „uvnitř“).**

Podstatně se tak rozšiřuje oblast, kterou je třeba chránit, a je nutné se vypořádat s prostředím, jež není plně pod kontrolou společnosti. Mění se i pachatelé počítačové kriminality. Nemusí se vždy jednat o zaměstnance firmy, ale ani o externí spolupracovníky. Pachatelé mohou být kdekoli na zemi, jsou organizovaní, někteří z nich mohou dokonce jednat na popud států.

Charakteristické rysy počítačové kriminality, její odlišnosti od jiných forem interní hospodářské delikvence:

- počítačová kriminalita je nebezpečná zejména proto, že poškozené společnosti nemusí probíhající útok vůbec odhalit, k odhalení dochází často náhodně, dokazování bývá složité a

často chybí dostatek důkazů vypovídajících o činnosti konkrétního pachatele. Počet „skrytých“ (neidentifikovaných) případů počítačové kriminality je větší než například v případě majetkové zpronevěry;

- páčání usnadňují rozvíjející se technologické vymoženosti, zároveň slouží jako prostředek k jejich zakrytí, likvidaci důkazů apod.;
- počítačové kriminalitě napomáhají stále složitější firemní IT systémy, možnost vzdáleného připojování a přístupů - lidé pracují z domova s využitím vlastních zařízení připojených na firemní systémy;
- digitální stopy jsou mnohdy neviditelné, nestálé, značně rozsáhlé a dynamické, tedy proměnlivé v čase i místě spáchání skutku;
- škody způsobené kybernetickou kriminalitou se obtížně zjišťují a vyčíslují;
- **převažuje pachatel coby jednotlivec, organizovaná skupina je spíše výjimkou. Většinou se jedná o využití příležitosti (86%) nebo možnosti pachatele při zajišťování rutinních pracovních operací. Čím jsou postavení pachatele a jeho možností vyšší, tím se stává tato činnost nebezpečnější, lze očekávat vyšší škody pro napadenou organizaci, činnost takového pachatele je komplikovanější a odhalování složitější;**
- **podvodná jednání jsou většinou prováděna dlouhodobě (v průměru cca 2 roky) a opakovaně;**
- **pachatelé počítačových podvodných jednání využívají mezery ve vnitřních procedurách a kontrolních mechanismech společnosti (34%);**
- zneužívá se především znalosti hesel, přístupových profilů do systému apod. Většinou nejsou nutné specifické znalosti vzhledem ke skutečnosti, že pachatelé při provádění vnitřních podvodných jednání zpravidla využijí svou rutinní, každodenní pracovní činnost;
- výpočetní technika může sloužit jako prostředek k falšování identity a používání padělaných dat a dokumentů;
- charakteristická je variabilita, pachatelé neustále vymýšlejí nové originální metody k překonání stávajících ochranných prostředků a procedur;
- většinou není zcela zjevné, zda se vůbec jedná o činnost zaměřenou proti zájmům organizace vzhledem ke skutečnosti, že je zakryta „legálními“, respektive „požadovanými postupy“;
- vyšetřování takových trestných činů je náročné a komplikované, často je nezbytné vyžádat spolupráci počítačového odborníka;
- důkazní materiál mnohdy nelze zajistit stejně jako ostatní stopy na místě klasického trestného činu;
- oběti i pachatele této kriminality nelze často vystopovat;
- **pachatel je převážně zaměstnanec organizace (v cca 80%), který využívá svého postavení k osobnímu obohacení v souvislosti se svou pracovní činností;**

- má informace o systému, jaké externí útočník nemůže nikdy získat. Zná jeho slabiny i silné stránky, podílí se na jeho vytváření, činnosti a denně s ním pracuje. Ví, jak bezpečnost doopravdy funguje.
- vnitřní nepřítel má často i silnou motivaci: neloyalita (40%) spory s nadřízenými či kolegy, zneuznání, ukončení pracovního poměru, snaha zvýšit svoji cenu na trhu práce, stát se důležitým...
- nejmodernější technické vymoženosti ovlivňují požadovaná bezpečnostní opatření, včetně personální bezpečnosti, na kterou se často zapomíná.

Kriminologové a vyšetřovatelé podvodů se shodují na tom, že pro spáchání podvodu musí být splněny **tři podmínky**:

- **příležitost - podmínky na straně společnosti – úroveň kontroly (34%) a firemní kultura/etika;**
- **pohnutka: finanční stimul – např. touha po penězích (hamižnost - 71 %) a potřeba udržet nákladný životní styl (59 %);**
- **schopnost zdůvodnit si takové jednání (na straně pachatele): nízký práh pokušení (54 %) a nedostatečné vědomí pachatele, že jeho jednání je nesprávné (40%). Druhé platí zejména u zcizování a zneužívání firemních dat a zcizování softwaru.**

Většina firem a organizací se v rámci prevence počítačové kriminality zaměřuje primárně na **technická opatření (hardware a software) a zlepšování odborné způsobilosti personálu**. Přestože naprostou většinu těchto skutků mají na svědomí vlastní zaměstnanci a manažeři, tak **je velmi podceňovaná oblast personální bezpečnosti. Bezpečnostní prověrky uchazečů a pracovníků na rizikových postech a hodnocení jejich morální integrity/loajality a poctivosti se provádějí výjimečně. A to i přesto, že osobnostní příčiny, dle odborných studií, hrají klíčovou roli. Osvědčuje se u těchto osob sledovat v jejich chování příznaky, které mohou signalizovat jejich podvodné jednání ve firmě. A také symptomy tzv. kriminálního osobnostního sklonu – disociační poruchy osobnosti.**

Osobnostní zdroje neloyalního jednání a interní kriminality

Typickým podvodníkem je muž ve věku mezi 31 a 40 lety, který strávil ve společnosti od tří do pěti let. Velice problematickou skutečností je fakt, že pachatelé interní kriminality vychází z řad vzdělaných, bezúhonných, vysoce postavených, společností uznávaných, sofistikovaných a vysoce inteligentních lidí. Bohužel, mohou to být i naši společníci, dobří známí, přátelé a příbuzní.

Jde o výrazně složitý a specifický problém. Poškození organizace může mít totiž různé vnitřní zdroje a vnější podoby - od neloyalnosti (donášení konkurenci, preferování osobních zájmů...), přes úmyslné vynášení firemního know-how, až po jednoznačně kriminální jednání (podvod, korupce, zmanipulování veřejné soutěže...).

Musíme proto zároveň sledovat a vyhodnocovat více vlastností mající vliv na oblast loajality a poctivosti zaměstnance či manažera. **V odborné literatuře jsou nejčastěji uváděny tyto osobnostní zdroje neloyalního a nepoctivého jednání:**

- a) **neloajalita (40%)** - negativní až nenávistný vztah k firmě, pracovišti či k nadřízenému je významnějším faktorem než vnitřní kontrola!
- b) **pracovní nespokojenost a frustrace**, pocit ukřivděnosti a ublíženosti, nízká pracovní angažovanost, až pohrdání "všední" prací
- c) **hamižnost, chamtivost** - nepřiměřené finanční a materiální nároky
- d) **nepřiměřená ambicióznost, nezdravé aspirace**
- e) **egocentrismus až egoismus**
- f) **nezdravě vysoké sebevědomí a sebedůvěra**, přeceňování svých schopností
- g) **tolerance k podvodům, nepoctivost** v pravém slova smyslu
- h) **lhavost**, někdy až přímo záliba ve lhaní
- i) **kriminální osobnostní sklon**
- j) **celková psychopatie/abnormita**, poruchy osobnosti, organická postižení mozku
- k) **kladný vztah k návykovým látkám, včetně alkoholu**
- l) **citová oploštělost**, nedostatek empatie a altruismu, až bezcitnost
- m) **sociální nevázanost až nestoudnost**, nepřizpůsobivost, nezodpovědnost, odmítání norem a pravidel
- n) **malé sebeovládání a snížená sebekontrola**, impulzivní sklon agresivně a nepřátelsky řešit i běžné zátěžové a konfliktní situace
- o) **zvýšená nevyrovnanost**, snadné nabuzování, vzrušivost, vnitřní napětí a neklid, rozladěnost.

Nejdůležitějším motivem je tedy hamižnost - dominantní a extrémní potřeba peněz a majetku, získaných jakýmkoliv způsobem, bez ohledu na jiné lidi (a často bez ohledu na aktuální finanční a majetkovou situaci pachatele).

Druhou vnitřní příčinou je nepoctivost – tolerance k podvodům.

Ve výčtu vnitřních zdrojů zaujímá důležité místo neloajalita, někdy až nenávistný vztah k firmě, který většinou vzniká jako důsledek konfliktů se spolupracovníky a s nadřízenými. Dokonce může vést k poškozování firmy bez zjevného osobního obohacení – vynášení a zneužívání dat, sabotáže, anonymní výhrůžky bombami, dezinformování zákazníků...

Dalším významným rizikovým osobnostním faktorem je nepřiměřená snaha prosadit se a výrazná orientace na osobní kariéru, tedy tak často skloňovaná ambicióznost. Většinou je spojena s egocentriem a nezdravě zvýšeným sebevědomím. Navenek jsou tito lidé přátelští, snadno vstupují do účelových koalicí, chybí jim ale sociální citlivost. Často u nich bývají v rozporu výsledky psychologických testů a subjektivního hodnocení. Dokážou při rozhovoru udělat dobrý dojem i na zkušeného personalistu.

Rozpoznání neloajálních a nepoctivých zaměstnanců a manažerů

Úvodem je nutno uvést, že se nám, stejně jako v zahraničí, při našich sondách do firem v ČR opakovaně prokázal negativní vliv nepoctivosti a nízké loajality na pracovní úspěšnost, kontraproduktivní pracovní chování a celkové hodnocení pracovníků (výkon, vliv, obliba a manažerský potenciál). Nepoctivý a neloajální zaměstnanec je pro firmy nejen potenciálním bezpečnostním rizikem, ale má i aktuálně horší pracovní výsledky, chová se častěji kontraproduktivně a je tedy pro organizaci celkově méně přínosný.

Proceduru hodnocení morální integrity využíváme buď již v průběhu přijímacího řízení, anebo u stávajících pracovníků. Druhé možnosti bývá použito např. po mimořádné události, při podezření na nepoctivé jednání. Pochopitelně lépe je nečekat pasivně na problémy a rizikové osoby preventivně vyhledávat. Například v rámci personálního či forenzní psychologického auditu.

S nadprůměrnou rafinovaností, inteligencí a vzdělaností pachatelů počítačových trestných činů rostou také nároky na jejich identifikaci. Je jasné, že to nemají napsáno na čele a se svými minulými prohřešky se chlubit nebudou. **A úspěšný podvodník umí působit velmi důvěryhodným dojmem, je to základ jeho know-how.**

Dalšími možnými problémy jsou sklon stavět se do společensky příznivějšího světla (sociální desirabilita – SODE) a sebeklam testovaného. Tendence vytvářet dobrý dojem je zesílena situací zkoušky, hodnocení a výběru. Řešením jsou kontrolní škály obsažené v dotaznících, speciální osobnostní inventář sebeklamu a vytváření dobrého dojmu (lhavosti). A to, že stejný osobnostní rys hodnotíme vícero odlišnými postupy, které se vzájemně doplňují a potvrzují. Máme k dispozici také ověřené metody, které jsou pro vyšetřované zcela neprůhledné, a proto se nemohou při nich stavět do lepšího světla.

Při rozpoznávání těchto rizikových osob nejsme tedy v žádném případě bezmocní. Můžeme využít poměrně citlivých, dá se říci, že i sofistikovaných metod. **Nedoporučuje se izolované hodnocení loajality a poctivosti, ale zároveň diagnostikovat i další dimenze osobnosti důležité pro pracovní oblast.**

Jednoznačná je situace, když je někdo při neloajálním či nepoctivém jednání přistižen nebo je mu takové chování následně prokázáno. Ale to už bývá pozdě. Toto jednání mohou pomoci zachytit vhodně nastavené vnitřní kontrolní mechanismy. Velmi se v praxi osvědčuje telefonní linka pro zaměstnance, na kterou mohou anonymně toto neloajální nebo nepoctivé jednání ohlásit.

Když používáme **rozhovor a analýzu anamnestických údajů**, tak se musíme smířit s tím, že zákon nám neumožňuje získat kompletní údaje o nezákonném chování v minulosti (opis trestů), ale pouze výpis trestů, ve kterém chybí již zahlazené tresty. Při pohovoru a analýze životopisu musíme počítat s tendencí stavět se do příznivějšího společenského světla, která bývá zesílena situací výběru. Navíc protřelí podvodníci mají nadprůměrné sociální a komunikační dovednosti a umí zanechat velmi dobrý dojem. Lze využít **posuzovací škálu**, která obsahuje známky disociálních poruch chování a osobnosti. Je zaměřena na formy chování signalizující nebezpečí budoucího delikventního vývoje osobnosti. Platí ověřená zákonitost, že specifické problémy v chování mohou signalizovat budoucí nezákonné jednání. Zjednodušeně řečeno: kdo dříve lhal, může nyní krást v naší firmě. Pouze výjimečně se stává, že pachatelé úmyslných trestných činů neměli dříve problémy např. ve škole, v práci, v oblasti blízkých vztahů, mezi vrstevníky...

Diskutabilní je **využití referencí**, neboť přes svoji oblíbenost nebyla doposud prokázána jejich dostatečná platnost a spolehlivost. Z odborných studií vyplývá, že nadřazený většinou hodnotí podřízené méně objektivně než např. jeho spolupracovníci. A běžně se setkáváme s případy, kdy jsou reference v pozitivním či negativním směru záměrně zkresleny.

Psychologické metody musí mít příslušné parametry - zejména platnost (validitu) a spolehlivost (reliabilitu), proto mohou do značné míry rozlišit loajální a poctivé od nepoctivých, neloajálních, nespolehlivých, pro firmu potencionálně rizikových zaměstnanců.

Testy integrity patří v ČR a Evropě dosud mezi spíše ojedinělé, přesto lze konstatovat, že jejich popularita značně stoupá. Naopak jsou již déle vyvíjeny v USA. Hlavním účelem těchto metod je ověřování důvěryhodnosti, morálního a etického cítění i tendence ke kontraproduktivnímu pracovnímu chování (CWB). Do CWB tradičně řadíme krádež, poškozování majetku, neposlušnost, zneužití informací, zneužití času, absence, nedochvilnost, užívání drog a alkoholu, nízkou kvalitu práce, sabotáže, nevhodné fyzické či verbální akce, chování neslučitelné s bezpečností práce či výpověď ze strany zaměstnance.

Integritu chápeme jako chování, které odpovídá požadavkům zaměstnavatele, u kterého se nepředpokládá, že by jeho požadavky byly neetické. Pracovní role vytváří morální stres, napětí a dilemata, která jsou součástí i rutinní práce, i když nemusí být vědomě, zjevně, prožívána jako v rozporu s požadavky pracovní role.

Dosavadní výzkumy vykazují relativně vysokou prediktivní validitu vyvolávající stále větší zájem praxe. Metaanalýza prokazuje, že testy integrity významně přispívají k predikci pracovního výkonu a kontraproduktivního chování, jako jsou krádeže, disciplinární problémy, absence. Validita se zvyšuje, když testy integrity zkombinujeme s dalšími psychologickými metodami. Výsledky také ukázaly signifikantní a pozitivní vztah mezi morálním usuzováním a úrovní výkonnosti.

Příklad baterie testů hodnotící loajalitu a poctivost psychickou způsobilost
(metody jsou uvedeny v pořadí, v kterém obvykle následují při vyšetření)

Test neverbální inteligence – intelektového potencionálu

Kromě vrozené inteligence zkouška zjišťuje také způsobilost odhadnout své schopnosti (viz bod f). Využívají se dvě formy testu – podle vzdělanostní úrovně testovaných osob.

Úvodní technika baterie slouží jako „rozcvička“ před dalšími metodami.

CAE – chromatický asociační experiment

Klíčová komplexní metoda baterie zachycuje, krom bodu h), všechny výše uvedené příčiny osobnostního rizika neloajálního a nepoctivého jednání. Metodu lze přizpůsobit konkrétní situaci. Můžeme testovat také kupř. orientaci na zákazníka, vztah ke kolegům, konkrétním osobám, flexibilitu, ochotu se učit atd. Jedná se o barvově-slovní projektivní (tzn. objektivní) osobnostní test, který svou konstrukcí znemožňuje vyšetřovanému stavět se do lepšího světla. Proto jeho závěry bývají často v rozporu s výsledky méně platných, objektivních a spolehlivých metod – např. rozhovoru.

Získáme informace vícero typu: vědomé: „to správné“ a očekávané hodnocení podnětového slova (např. respondent uvádí kladný postoj k firmě), ale hlavně nevědomé: nezkeslené snahou vylepšovat se (skutečný negativní vztah k zaměstnavateli). V tomto případě konstatujeme též závažný vnitřní konflikt. Také zjistíme, do jaké míry se respondent s firmou identifikuje (vůbec až absolutně - dle těsnosti asociace podnětových slov „já“ a „firma“). CAE umožňuje současně zachytit asociační řetězce slov, jakési nevědomé minipříběhy. Příklad jednoho hororového: „firma“ – „já“ – „podvod“ – „peníze“.

Do hloubky psychiky zasahující projektivní postup „rozhýbe“ podvědomí a nevědomí testované osoby, ta potom méně zkresluje své odpovědi v dotazníku.

Osobnostní dotazník DOPEN

Dotazník zachycuje dimenze zatvrzelost - body k) až n), extraverte - společenskost a družnost, emocionalita/nevyrovnanost - body o), částečně i n), lhavost a současně také tendenci stavět se do společensky příznivějšího světla a tzv. kriminální osobnostní sklon. Poslední uvedený rys rozlišuje osoby bezúhonné od osob páchající trestné činy. DOPEN diagnostikuje také základní čtyři typy temperamentu.

Test opakování série pohybů TOSP

Krátká pohybová neuropsychologická zkouška vyžaduje spolupráci obou mozkových hemisfér. Proto horší výsledek ukazuje, spolu s předchozí metodou, na případné organické postižení mozku (bod j). U delikventů je jejich výskyt více než 50%, u běžné populace 3-5%. Hodnotíme také úroveň pohybové a neverbální inteligence. Když porovnáme výsledek s prvním testem, tak zjistíme obecné předpoklady k učení. Jedná se o jedinou metodu, která se musí provádět striktně individuálně.

Dotazník žádoucího stylu odpovídání BIDR-CZ

Osobnostní inventář zjišťující **sebeklamání a vytváření dobrého dojmu a souhrnné skóre** obou rysů, který je standardizován pro českou populaci.

Zkouška skrytě odhalující podvodné jednání

Jde o krátkou zkoušku, která je vlastně testem morální integrity. Dosažení určitého výsledku je totiž možné pouze za předpokladu, že testovaná osoba podvádí. Zde je na místě předpokládat, že může v budoucnu podvádět i v jiných situacích. Zejména, když proto svědčí i výsledky ostatních metod.

Celá baterie zabere zhruba dvě hodiny. Vyhodnocení, interpretace a sepsání zprávy několik hodin. Testuje se v malých skupinách nebo individuálně. Pokud to umožňuje situace, tak je před sepsáním závěrečné zprávy užitečný krátký psychologický rozhovor.

Po odevzdání definitivních výsledků je žádoucí, aby psycholog adekvátní formou seznámil testovaného s celkovými výsledky – informoval ho o jeho silných stránkách, případných rezervách a poskytnul mu konkrétní doporučení pro jeho další osobnostní a kariérní rozvoj.

Současně se diagnostikují psychická způsobilost, kladné silné stránky na pozice se zvýšenou odpovědností. U nejlépe pracovně a celkově hodnocených zaměstnanců a manažerů jsme zaznamenali tyto osobnostní rysy psychické způsobilosti (seřazeno odshora podle statistické průkaznosti):

- **realističtější vnímání skutečnosti**, minimální tendence k extrémním hodnocením,
- přátelské vztahy k lidem, výrazný pocit sounáležitosti s nimi (**sociabilita** čili schopnost vycházet s lidmi může u některých profesí ovlivňovat pracovní úspěšnost až z 85 %),
- **poctivost**, čestnost a smysl pro etiku,
- pozitivní známky duševního zdraví, celková přizpůsobivost a **psychická rovnováha**,
- **malá unavitelnost**,
- **pozitivní pracovní postoje** a zaměstnanecká loajalita - vztah k práci, pracovišti, firmě a povinnostem a stupeň ztotožnění se s nimi,
- **minimální delikventní sklon**,
- nadprůměrný **intelektový potenciál - analytické schopnosti**, schopnost řešit problémy,
- **odmítavý postoj k alkoholu** (ne přímo abstinence, ale netolerování alkoholu při práci a řízení motorových vozidel),
- **psychická odolnost**, citová stabilita, případně ještě subjektivní pocit zdraví.

Celá baterie zabere zhruba dvě hodiny. Vyhodnocení, interpretace a sepsání zprávy několik hodin. Testuje se v malých skupinách nebo individuálně. Pokud to umožňuje situace, tak je před sepsáním závěrečné zprávy užitečný krátký psychologický rozhovor.

Po odevzdání definitivních výsledků je žádoucí, aby psycholog adekvátní formou seznámil testovaného s celkovými výsledky – informoval ho o jeho silných stránkách, případných rezervách a poskytnul mu konkrétní doporučení pro jeho další osobnostní a kariérní rozvoj.

PhDr. Miroslav Pokorný,
forenzní a personální psycholog,
pokornymir(zav.)seznam.cz