**Sborník vědeckých prací Vysoké školy báňské – Technické univerzity Ostrava**
číslo 1, rok 2005, ročník LI, řada bezpečnostní inženýrství

**Ingrid, MATOUŠKOVÁ*, Roman RAK****

# BEZPEČNOSTNÍ MANAŽER – JEHO ROLE A OSOBNOST

SAFETY MANAGER - ROLE AND PERSONALITY

**Abstrakt**

Příspěvek si bere za cíl komplexní pohled na bezpečnostního manažera. Charakterizují se specifičnost, náročnost a souvislosti jeho práce při prosazování bezpečnosti v instituci. Důraz je kladen na personální charakteristiky a profesní předpoklady pro výkon jeho práce, která je ve své podstatě velmi složitá a svým způsobem i nevděčná, se silnými vlivy na jeho psychiku. V souladu s praktickými potřebami autoři definují základní osobnostní požadavky na roli bezpečnostního manažera a zamýšlejí se nad způsoby a možnostmi jeho výběru při obsazování této významné manažerské pozice v instituci, která je zde chápána obecně – od IT prostředí v komerčních či státních firmách a institucích, až po profesionální bezpečnostní organizace.

**Abstract**

The main aim of the contribution is to provide a detailed review of the role of the safety manager, and to describe the specific demands of his work when enforcing safety in an institution. Attention is given both to the personal characteristics and professional qualifications necessary for performance of his work, which can be complex but also thankless, and also the psychological influences. From a practical standpoint the authors define the essential personal characteristics for the position of a safety manager, and consider ways and options on how to best select a safety manager when filling this important managerial post in an institution, from the IT environment in businesses and state entities, to professional security organisations.

**Key words:** safety manager, personal characteristics, demands, chois, risks, Information and Communication Technologies.

## Úvod

O bezpečnosti se mluví stále častěji a na nejrůznějších fórech. Události 11. září 2001 v USA a srpnové povodně v roce 2002, útoky spojované s mezinárodním terorismem a poslední válka v Iráku se staly mohutným impulsem pro rozvoj bezpečnosti jako takové.

---

* Mgr., Bankovní institut vysoká škola, a.s., Ovenecká 9/380, 170 00 Praha 7, Pražská teplárenská, a.s., Partyzánská 7, 170 00 Praha 7

** Ing. Bankovní institut vysoká škola, a.s., Ovenecká 9/380, 170 00 Praha 7, Pražská teplárenská, a.s., Partyzánská 7, 170 00 Praha 7

Na trhu ICT technologií se objevují stále novější technologické produkty, jejichž cílem je ochránit bezpečnost informací, specializované firmy se předhánějí v nabídkách svých služeb (analýzy rizik, bezpečnostní audity, různé penetrační testy, certifikace podle mezinárodně platných bezpečnostních standardů atd.). V určitém slova smyslu se bezpečnost stala pro obchodníky s těmito technologiemi zlatým dolem, někdy i zaklínadlem, které dovoluje i leccos prodat, aby společnost (firma, instituce, stát) byly „IN“ současným bezpečnostním trendům. Dokonce i tehdy, kdy společnost ve skutečnosti nepotřebuje, nebo ne v takové míře, nejnovější technologické produkty. Na téma bezpečnosti se konají mezinárodní konference, o IT bezpečnosti se přednáší zejména na technických vysokých školách.

Historie nás ale opakovaně tvrdě zkouší a učí, že i ty nejmodernější a nejdražší technologie, při nedodržení určitých elementárních zásad, za jistých okolností, nešťastných souběhů různých událostí nebo nepředpokládaných („projekčně nereálných“) náhod jsou velice zranitelné a překonatelné. Někdy dokonce s minimem úsilí nebo finančních či jiných nákladů, minimálními znalostmi nebo zkušenostmi, mnohdy bez hlubšího vzdělání, takže nakonec dochází nejenom k neočekávaným a zároveň překvapivým bezpečnostním incidentům, kterým jsme chtěli původně zabránit, ale i svým způsobem ke znehodnocení finančních prostředků a lidského úsilí, vložených do bezpečnostních technologií a s nimi souvisejícími opatřeními. V důsledku je pak zpochybněna bezpečnost jako taková.

Technicky orientovaní tvůrci bezpečnostních produktů a služeb vidí často nezbytná opatření jen na technické úrovni. Podobným způsobem mnohdy přemýšlí i IT specialisté, managementy institucí, jejich vlastníci, akcionáři. A to jen v těch případech, kdy si aspoň uvědomují, že bezpečnost by se měla nějak řešit. Nejlépe ovšem s minimálními náklady a „obtěžováním“ zaměstnanců nebo majitelů.

Hovořit, že bezpečnost je zejména a především o lidech, je možná nošením dříví do lesa. Občas se v praxi výjimečně setkáme s objasňováním pojmu „sociotechnika[1]“ a s opatřeními, které by ji měly maximálně omezit nebo minimalizovat na přijatelnou hranici. Ve společnostech, kde je vysoké společné povědomí o bezpečnosti, jsou zaměstnanci průběžně školeni, jak rozeznávat příznaky či projevy sociotechnických útoků.

Chceme-li poznat důsledky jevů, musíme pochopit jejich příčiny. Zamezíme-li vzniku nebo rozvoji příčin negativních jevů, máme určitou šanci je dostat pod kontrolu.

V odborné literatuře se začínají stále více objevovat příběhy hackerů, kteří se staly díky své kriminálními činnosti slavnými. Někteří se vrátili na stranu „dobra“ a své (mnohdy již překonané) zkušenosti za finanční úplatu předávají těm, kteří jsou ochotni za ně zaplatit.

[1] „**Sociotechnika** je ovlivňování a přesvědčování lidí s cílem oklamat je tak, aby uvěřili, že sociotechnik je osoba s totožností, kterou předstírá a kterou si vytvořil pro potřeby manipulace. Díky tomu je sociotechnik schopný využít lidi, se kterými hovoří, případně dodatečné technologické prostředky, aby získal hledané informace [1]“. Jinými slovy sociotechniky jsou specifické metody využívající člověka pro přístup k informacím, jež jsem určitým způsobem chráněny. Sociotechnické metody nevyužívají primárně technických prostředků k získání informací, ale velmi účinně, se znalostí prostředí, psychologie lidí, ovlivňují druhé. Osoba, jež je předmětem nebo prostředkem útoku, pak nevědomě napomůže útočníkovi obejít technické nebo organizační obranné mechanismy.

V zahraničí se objevují první studie, zabývající se psychologií útočníků, využívajících ICT prostředky jako prostředek nebo cíl svých útoků. Těchto studií je ovšem jako šafránu.

## Proč zrovna osobnost bezpečnostního manažera je klíčová?

Opomíjenou oblastí, ať už v rovině teoretického rozpracování nebo jejího praktického prosazování v běžném životě společnosti, je osobnost bezpečnostního manažera, na kterého je kladena velmi vysoká zodpovědnost. V případě bezpečnostního incidentu to je právě on, kam směřuje velice intenzivní a ostrá kritika nebo v krajních případech dokonce i trestní oznámení na zanedbání povinností podle příslušných paragrafů zákona.

Základní povinností bezpečnostního manažera je jednoduše řečeno metodicky připravovat a následně realizovat (přesněji řečeno vytvářet podmínky pro realizaci), či kontrolovat množinu bezpečnostních opatřeních, jejichž cílem je ochrana informačních či jiných aktiv společnosti v plném souladu s celkovou strategií společnosti v intencích reálného, podnik obklopujícího světa, který je dnes plný nejrůznějších střetů zájmů, konfliktů; s vysokou mírou neurčitosti či nestability. Není podstatné, zda původcem tohoto nepřehledného chaosu je člověk, jím vytvořená technologie, samotná matička příroda nebo příroda ovlivněná necitlivými či sobeckými zásahy lidstva.

Role bezpečnostního manažéra je nesmírně náročná, složitá a svým způsobem velmi nevděčná. Jeho pozice často kromě organizace samotných bezpečnostních opatření vyžaduje profesně řešit i antagonistické požadavky, vyplývající z podstaty nebo fungování instituce, kde bezpečnostní manažér vykonává svou činnost.

Podobně jako vedení problematiky ICT manažery IT (CIO[2]), tak i vedení bezpečnosti IT klade velmi vysoké nároky na osobu bezpečnostního manažera, a to nejen z pohledu porozumění technologiím a systémům, bezpečnosti jako takové, ale vyžaduje i znalost a schopnost vnímání obchodních potřeb, stejně jako ekonomických vazeb a znalost pochopení vztahů a primární motivace akcionářů a vlastníků, vrcholového managementu [4].

Bezpečnost musí být dnes i ekonomicky zdůvodnitelná a přijatelná, alespoň v komerčním světě tomu tak je. V intencích států, národů vstupují do hry i jiná kritéria, než jsou peníze – národní, (ale taky ekonomická) samostatnost, politická, kulturní nebo náboženská svébytnost, národní hrdost, hegemonie, cena „existence státu“ a lidského života.

Jaké znalosti, dovednosti a zejména charakterové vlastnosti by bezpečnostní manažer měl mít, aby obstál při komplexním řešení netriviálních úloh a v maximální míře ochránil svou instituci před všemi případnými ztrátami? Jaké jeho vlastnosti jsou rozhodující pro realizaci bezpečnostních opatření? Co je specifické pro práci bezpečnostního manažera? Co všechno může stát v cestě budování a udržování přijatelné bezpečnosti pro instituci a jak tyto překážky překonávat? Jak vyhledávat a vybírat bezpečnostního manažera? Jaká jsou výběrová nebo srovnávací kritéria?

Pokusíme se proto o stručný pohled na danou problematiku, o určitá zobecnění nebo paralely z příbuzných oborů, které mohou, ale nemusejí vždy fungovat.

[2] CIO – Chief Information Officer

I když budeme poměrně často směřovat k psychologickému a jinému profilování bezpečnostního manažéra IT, řada zkušeností a postřehů je obecně platná pro bezpečnostního manažera jako takového, který se nemusí nutně zabývat jen bezpečností IT nebo informací, ale např. i bezpečností fyzickou, krizovým managementem apod.

Proto osobu bezpečnostního manažera v tomto příspěvku rovněž záměrně umisťujeme do prostředí jeho instituce, kde pracuje. Pod institucí si pak můžeme představit konkrétní firmu (s českým nebo zahraničním majitelem(y), nadnárodní koncern, bezpečnostní agenturu nebo státní bezpečnostní službu – policejního nebo zpravodajského charakteru apod.), s přihlédnutím k jejich shodným a i rozdílným specifikám. Ve státních institucích je pojem bezpečnostního manažera nahrazován funkcemi vnitřní inspekce, auditu, orgány interního defenzivního zpravodajství, útvary pro vnitřní záležitosti atd. I bezpečnostní složky musí dbát o svou vnitřní bezpečnost, chránit své informace (a jejich zdroje).

Bezpečnostní management v komerčním sektoru je součástí „core businessu“. Pro zahraniční, nadnárodní podniky to je samozřejmostí, ve středních a malých českých firmách se tomu teprve učíme. Bezpečnost je v některých případech vnímána ne zcela komplexně. Firmy už většinou „slyší“ na pojem IT bezpečnost nebo fyzická bezpečnost, ale ne vždy si uvědomují širší význam termínu informační bezpečnost. Nejedná se jenom o ochranu před příležitostí odcizit na stole zapomenutý dokument procházejícím návštěvníkem nebo zkratové jednání nespokojeného vlastního zaměstnance.

Na zahraničních univerzitách nebo vysokých školách ekonomického nebo komerčního zaměření (zejména ve Francii[3] nebo Japonsku) existují nové, civilní studijní obory tzv. „kompetitivního zpravodajství[4]“. Ve své podstatě se nejedná o nic jiného než o ofenzivní zpravodajství či klasickou průmyslovou špionáž aplikované do komerčního světa. Jen výklad (často podpořených etikou podnikání) diplomaticky vysvětluje opodstatnění operativních metod využívajících lidské nebo technické prostředky pro získání nezbytných informací, jejichž cílem je dominance nad konkurentem (odsud milý název „kompetitivní“, který odráží „hravost“ a „soutěživost“ podnikání). Učí se zde základy sběru a analýzy informací, lobování, aktivní ovlivňování a vlivová opatření atd. Uvědomíme-li si drsnou realitu kultu peněz, pochopíme, že ve skutečnosti se jedná o razantní, někdy až nevybíravou cestou za informacemi (byť potenciální) konkurence. A není rovněž žádným tajemstvím, že v globalizovaném světě státní zpravodajské instituce (zejména světových velmocí) získávají informace ekonomického nebo vědeckotechnického charakteru, aby podpořili nejen obranu státu, ale zejména aby zajistili jeho ekonomický rozvoj. Jinými slovy – mohou pracovat na objednávku pro velké privátní instituce nebo komerční firmy!

I malá firma, která se rodí na základě nějaké převratné nebo aspoň originální myšlenky, nápadu nebo know-how, musí umět ochránit své informace. Jinými slovy – na bezpečnostního manažera v malé instituci jsou kladeny požadavky na vysoké odborné znalosti (tedy i na defenzivní zpravodajství) a zejména na jeho osobnost ve všech aspektech.

[3] Titul z oblasti komerčního zpravodajství lze například získat na École Superieure du Commerce v Dijonu nebo na Université de Marne-la-Vallée.

[4] Pro pojem „kompetitivní zpravodajství“ (competitive intelligence) se rovněž používá synonymum ofenzivní podnikatelské (komerční) zpravodajství.

Komplexní bezpečnost má pak zcela jiný rozměr a tím i nároky na bezpečnostního manažera, který musí být schopen danou situaci uřídit.

## Specifičnost práce bezpečnostního manažera

Bezpečnost můžeme velmi zjednodušeně definovat jako neustálou činnost, zajišťující kontinuitu určitého klíčového procesu. Tím procesem může být např. zachování existence státního zřízení (bezpečnost státu), trvalých příjmů z podnikatelské činnosti (bezpečnost firmy, Business Continuity Planning - BCP), pouhého lidského života (bezpečnost a ochrana zdraví – při práci, v soukromém životě).

Činnost bezpečnostního manažera je možné charakterizovat následujícími specifikami, které zároveň po bezpečnostním manažerovi vyžadují specifické vědomosti, dovednosti, zkušenosti a osobní předpoklady, které jsou rozhodující pro úspěšné vykonávání jeho role:

Jeho činnost je většinou zaměstnanců instituce subjektivně vnímána jako nadbytečný, omezující nebo kontrolní faktor a tato funkce je málokdy obecně přijímána zaměstnanci pozitivně a nepatří zrovna k oblíbeným. Bezpečnost se ve své podstatě vždy zásadně vynucuje (nařízení, předpisy, zákony, technologické restrikce, přístupová práva, prověrky, kontroly, nácviky apod.), obvykle proti dosud obvyklému (vžitému a pohodlnému) způsobu chování zaměstnanců. Při nedodržování základních zásad pak po upozornění následují sankce. Na druhé straně existuje skutečnost, že prosazování bezpečnosti lze realizovat lidsky, inteligentně a decentně, kulturně. Takto realizovaná bezpečnost bývá zpravidla velmi úspěšná. Rozhodující roli pak hrají právě osobnost bezpečnostního manažera (a jemu bezprostředně organizačně nadřízené i podřízené struktury).

Bezpečnost je dnes technologicky velmi složitá a vyžaduje hluboké odborné znalosti v mnoha disciplínách. Současně musí ale existovat harmonie mezi technologickým, administrativním, organizačním a personálním způsobem bezpečnostních řešení. Bezpečnost nesmí být řešena pouze technokratickými prostředky, jinak poměrně rychle selhává. Bezpečnostní manažer musí být proto mnohem více, než jen úzce zaměřený specialista.

Bezpečnost má profylaktický charakter. Všechna opatření se realizují proto, aby byly eliminovány potenciální rizika vyplývající z bezpečnostních analýz nebo auditů, prognóz či obecných trendů. Bezpečnost se často neobejde bez technologických řešení, které mohou být finančně nákladné. Z pohledu managementu, akcionářů nebo vlastníků není vidět žádný primární, přímý přínos těchto investic. Dobře realizovaná bezpečnost se vlastně nijak navenek viditelně a zásadně neprojevuje. Bezpečnostní projekty patří většinou k infrastrukturálním projektům (procházejícími napříč celou firmou), které se velice těžko ekonomicky zdůvodňují. Nelze zpravidla stanovit přesnou návratnost investice (Return On Investment – ROI nebo s využitím jiné ekonomické metody). Můžeme spíše argumentovat ochranou již vložených investic nebo (informačních) aktiv instituce. „Co se může stát, když není realizováno …?“. „Jak velká to bude pro společnost ztráta, když nebude několik dní fungovat e-mail?“ Argumentace bezpečnostního manažera musí být ale velmi citlivá a diplomatická, musí být plně respektován svým okolím a požívat důvěru.

Řešení bezpečnosti musí být komplexní a systematické. Bezpečnost je tak zranitelná, jak je zranitelný její nejslabší článek. Cíl (předmět) útoku (nebo jiného bezpečnostního incidentu) je zpravidla znám, lze jej za určitých předpokladů vytypovat. Existuje však velice mnoho způsobů, jak útok realizovat. Míra neurčitosti je velmi vysoká. Bezpečnostní manažer musí

mít proto velmi dobrý přehled o již proběhlých bezpečnostních incidentech. Neocenitelné jsou zkušenosti a znalosti i z organizací jiného typu, jiných zemích, než kde je bezpečnostní manažer právě zaměstnán. Z pochopitelných důvodů málokterá instituce přiznává na veřejnosti své bezpečnostní incidenty, způsoby jejich provedení a dopady. Bezpečnostní manažer kromě znalostí, zkušeností a analytických schopností musí být obdařen i předvídavostí, profesní intuicí a fantazií, kreativitou, aby se dokázal vžít do role potenciálního útočníka nebo odhalit skryté hrozby (technického, přírodního charakteru atd.), které ještě nebyly nikde realizovány. Kromě životní, profesní zkušenosti musí existovat i určitá profesní podezíravost, jejímž cílem je odhalovat slabá místa. Podezření nesmí ale nikdy sklouznout k osobním výpadům proti komukoliv, musí být respektována prezumce neviny. Hypotézy podezření je třeba objektivně, skrytě prověřovat před tím, než vyslovíme nahlas na laické nebo nepovolané veřejnosti jakýkoliv názor!

Bezpečnostní manažer je ve své pozici často osamocen. Musí dokázat dobře a efektivně komunikovat s podřízenými i nadřízenými, dodavateli nejrůznějších technologií, neustále řeší konfliktní a citlivé situace. Řada akcí probíhá s určitým stupněm utajení. Na bezpečnostního manažera je kladena vysoká zodpovědnost a při tom nemá někdy dostatečné prostředky pro realizaci bezpečnostních opatřeních v takovém rozsahu, jak vyžaduje situace, teorie nebo jeho vlastní představy, aby dokázal nést zodpovědnost, která je na něj vložena. Míra zodpovědnosti s ohledem na vysoká rizika nemusí vždy v instituci odpovídat pravomocím či prostředkům, kterými bezpečnostní manažer disponuje. U bezpečnostního manažera se vyžaduje vysoká míra loajality a spolehlivosti, mlčenlivosti. Mohou nastat situace, kdy bude ovlivňován vrcholovým managementem v rozporu s jeho posláním. Nejčastěji to je právě vrcholový management, který představuje pro instituci vysoké riziko (ztráta, krádež, odcizení citlivých informací), protože se mnohdy nedokáže nebo „z principu“ nechce ztotožnit s elementárními zásadami bezpečnosti a nebo je přímo úmyslně obchází z nejrůznějších důvodů (pocit moci, výjimečnosti svého postavení, nezranitelnosti a nebo i v krajním případě dokonce práce pro třetí stranu či vědomé a cílené zneužívání svého postavení pro osobní obohacení). Pokud to někdo takto chápe a v praxi realizuje, bezpečnostní manažer mu stojí v cestě a zcela automaticky se stává jeho protivníkem. Dokázat unést tíhu některých poznatků a nesdělit je nějaké třetí straně (včetně svému životnímu partnerovi, rodinným příslušníkům, přátelům) není v praxi taktéž pro bezpečnostního manažera triviální záležitostí. V některých výjimečných případech (státní bezpečnostní složky operativního charakteru) je po bezpečnostních manažerech navíc vyžadováno, aby skrývali svou občanskou identitu před svými civilními kolegy, přáteli či známými a zároveň používali legendu odlišného zaměstnavatele a profese, aby před svou rodinou a okolím zatajili své skutečné zaměstnání. V takovémto případě se profesionálně klame a využívá řady prostředků na podporu tzv. „krycí legendy“. Na psychiku bezpečnostního manažera jsou kladeny extremní nároky, aby dokázal „žít dvojím způsobem“.

Globalizovaný svět, prostředí, instituce, ve kterém je realizována bezpečnost jsou dnes velmi dynamické, s vysokou mírou neuspořádanosti, neurčitosti, chaosu. S probíhajícím velkým množstvím změn (konkurenčních, strategických, organizačních, personálních atd.), které jsou provázány i negativními emocemi zaměstnanců, dochází k časté pracovní fluktuaci. Jakákoliv nestabilita se do bezpečnostních opatření promítá negativně a je nevyhnutelností být schopen adekvátně a včas reagovat, optimálně se přizpůsobovat momentální situaci a trendům.

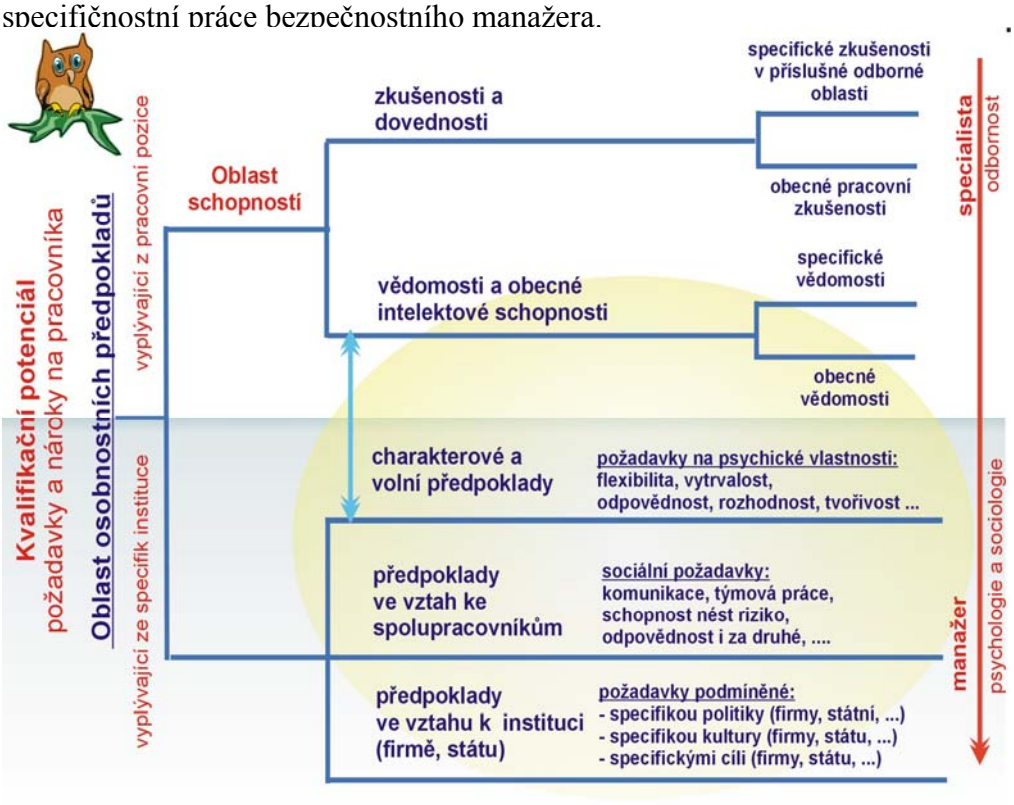
Bezpečnostní manažer musí být připraven a schopen vykonávat svou činnost za každých okolností. Může se sám stát rovněž předmětem zájmu někoho jiného, a proto je vyžadován

silný charakter, neúplatnost. Musí mít takové osobnostní charakteristiky, chování a profesní i soukromou minulost, aby nebyl nijak zranitelný a ovlivnitelný. Nesmí proto potenciálně existovat žádné důvody, aby mohl být vydírán nebo kompromitován. Musí být připraven odolávat velkému množství osobních útoků z nejrůznějších důvodů a rozumně jim čelit. Zároveň musí umět nést zodpovědnost za rizika, kterých bývá v praxi velké množství. Bezpečnostní manažer musí umět pochopit profesionální filosofii, že buď někoho nebo něco prověřuje či kontroluje, nebo je sám někým kontrolován. Z tohoto pohledu musí v rozumné míře dokázat pracovat transparentně vzhledem k nadřazeným kontrolním institucím.

Nejasnost kompetencí. V praxi nejsou při práci bezpečnostního manažera vždy jasně vymezeny jeho kompetence a může docházet i k profesním střetům uvnitř organizace, které je nutno citlivě a účelně řešit. Ne vždy je totiž jasně vymezena hranice mezi IT bezpečností, fyzickou a obecná bezpečností, a hlavně pak mezi interními auditní orgány, risk managementem apod. Konflikty mohou vznikat tehdy, jestliže v instituci je na bezpečnostní scéně více profesionálních hráčů bez stanovených pravidel, což má negativní dopad na celkovou bezpečnost. V organizaci pak interně dochází k vnitřním šarvátkám, na úkor primárního cíle zajišťovat bezpečnost.

## Kvalifikační potenciál aneb požadavky a nároky na bezpečnostního manažera

Pro názorné pochopení požadavků a tedy nároků na bezpečnostního manažera je účelné tento požadovaný kvalifikační potenciál rozčlenit do určitých logických kategorií, tak jak je znázorněno na Obr. 1. Autoři vycházejí ze teoretického, základního kvalifikačního potenciálu libovolného pracovníka, který dále bude podroben diskusi spojené se specifičnostní práce bezpečnostního manažera.




*Obr. 1 Požadavky a nároky na (bezpečnostního) manažera.*

## Oblast schopností

Při diskusi o práci bezpečnostního manažera se často setkáváme s otázkou, na kolik procent se jedná o práci manažerskou nebo práci odborného specialisty. V literatuře [11] můžeme najít poměr 60:40%, tj., že z 60% převládá manažerská činnost. Kloníme se však k názoru, že nelze jednoznačně stanovit žádný takový poměr, byť název bezpečnostní manažer nabádá k myšlence, že se jedná především o práci manažerskou (tedy „alespoň 50%“). Podstatná je spíše ale skutečnost, jaké je postavení bezpečnostního manažera v instituci, kam je organizačně začleněn, jaké jsou jeho zodpovědnosti a pravomoci, kolik má přímo podřízených osob v jím vedeném bezpečnostním útvaru, jak spolupracuje s managementem společnosti nebo jejími zaměstnanci. Podle výše uvedených různých modelů organizačního začlenění bezpečnostního manažera v organizační struktuře instituce a podle náplně činnosti je zřejmé, že se může jednat v krajních případech o práci úzkého IT specialisty (model minimální technologické bezpečnosti), kde se o manažerské činnosti téměř nedá hovořit až po skutečně manažerskou činnost (model rozsáhlé institucionální bezpečnosti), kde téměř 100% činnosti manažera je orientováno na spolupráci a koordinaci mezi nejrůznějšími odborníky, zaměstnanci, managementem a akcionáři instituce.

V tomto příspěvku se nebudeme zabývat ani analýzou požadovaných zkušeností a dovedností, vědomostí, které jsou kladeny na bezpečnostního manažera. I zde platí, že požadavky vyplývají ze samotné instituce. V oblasti IT to můžou být např. znalosti nejrůznějších síťových protokolů, šifrovacích algoritmů a technologií, firewallů, databází atd. Obecně to může být ale i fyzické zabezpečení objektů, nejrůznější postupy při ochraně informací před defenzivním (kompetitivním) zpravodajstvím, personální bezpečnost atd.

## Oblast osobnostních předpokladů

Osobnost je člověk jako celek po stránce duševní. Osobnost má větší nebo menší svéráz. Psychologie osobnosti se proto zaměřuje jednak na rozbor celku, jednak na stanovení svérázu.

Zkoumáme-li osobnost určitého člověka, odpovídáme na otázku jaký je. Zjišťujeme, co je pro něho po duševní stránce příznačné, typické, čím se podobá ostatním a v čem je odlišný. Snažíme se zjistit, co umí, o co a jakým způsobem usiluje.

Pojem osobnost postihuje skutečnost, že naše chování a prožívání má ve své proměnlivosti a mnohotvárnosti celostní povahu, jednotný ráz. V každém okamžiku dění v nás pracuje "já", do kterého se začleňují (integrují) výsledky našeho konání. Osobnost tak garantuje kontinuitu prožívání v čase.

Pojmem osobnost zdůrazňujeme tedy celostní, integrativní povahu duševního dění. Druhým podstatným znakem je jedinečnost. Osobnost člověka je vždy jedinečná. Z pohledu psychologie nemohou existovat dva lidé s identickou osobností. Zatímco je známo, že se vyskytují dvojníci ve smyslu fyzické podobnosti, je po psychické stránce shoda duševních parametrů vyloučena. Prakticky to znamená, že nikdo neuvažuje do detailů shodně jako "já". Psychologické chápání jedinečnosti nejlépe přibližuje známé tvrzení, že každý člověk je v některých ohledech:

stejný jako všichni ostatní
stejný jako někteří ostatní a současně v některých ohledech
jako žádný jiný člověk.

Celostní uspořádání duševního dění je v tomto smyslu jedinečné a neopakovatelné.

V psychologii existuje mnoho různých definic osobnosti. Pomocí různé terminologie vyjadřují podstatu pojmu: osobností rozumíme relativně trvalé uspořádání biologických, psychologických a sociálních charakteristik do jedinečného celku duševního dění, který každý z nás prožívá jako své vlastní "já".

Pro hodnotitele, vnějšího pozorovatele představuje naše osobnost individuální, jedinečný "mix" obvyklých a třeba i neobvyklých, vzácných schopností a vlastností. Tím se dostáváme k otázce, co tvoří osobnost, z čeho se osobnost každého člověka skládá. Odborně řečeno jde o problém struktury neboli skladby osobnosti.

Problém struktury osobnosti lze přiblížit názorně na jednoduchém příkladu. Je známo, že ve stejné situaci se různí lidé zachovají různým způsobem. Například na kritiku nadřízeného reagují někteří podrážděným odmítáním výtek, jiní obviňují z chyb druhé spolupracovníky a další si třeba odreagují svůj rozlad na rodinných příslušnících. Tyto rozdíly v pozorovaném chování lze vysvětlit rozdílností jejich osobností, tj. rozdíly ve struktuře a dynamice osobnosti.

Abychom mohli postihnout, v čem se jednotlivci odlišují, je nutné rozčlenit osobnost na dílčí složky. Rozdíly mezi lidmi spočívají pak v tom, jaké složky jsou v jejich osobnosti zastoupeny a současně jakou silou působí, tj. jak intenzivně se projevují. Členění osobnosti na dílčí složky a jejich vzájemné vazby tvoří základní problematiku struktury osobnosti.

Struktura osobnosti odráží to, co je na daném člověku po psychické stránce stálé, co ho charakterizuje a to, čím se v proměnlivých okolnostech vždy v nějaké míře projevuje. Z toho plyne, že na strukturu osobnosti běžně usuzujeme z chování jedince. Je důležité pochopit, že z osobnostní struktury se v každé situaci může projevit jen určitá část s tím, že dále je pozorované chování vyprovokováno situací.

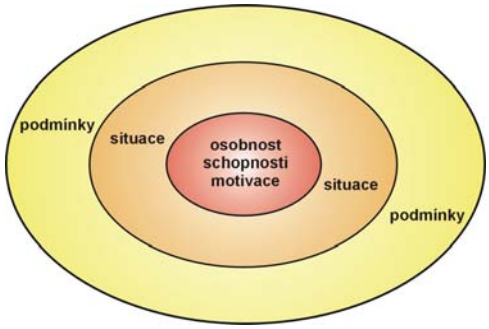
Vliv situace známe z vlastní zkušenosti. Každý z nás dovede být přátelský, ale i odměřený, nepříjemný. Který vzorec chování se projeví, záleží na aktuální situaci. Vůči osobě, kterou chceme zaujmout a kterou si chceme naklonit, dovedeme být přímo líbezní. A naopak, vůči jedinci, kterého nemůžeme vystát a který nás obtěžuje svou přítomností, vystupujeme odměřeně, přísně a podrážděně. Tato situační proměnlivost našeho chování je přirozená. Současně však každý z nás má tendenci či sklon vystupovat v (citově neutrálních) interakcích s druhými pro něho příznačným, typickým způsobem např. přátelsky a otevřeně či spíše rezervovaně, zdrženlivě. Hovoříme o dispozici neboli o vlastnosti, která jedince charakterizuje. Strukturou osobnosti se rozumí relativně stálé charakteristiky osobnosti, které jsou dispoziční povahy. Struktura osobnosti tvoří individuální základ pro chování a prožívání, který se v závislosti na situaci aktualizuje.

Pojem struktury osobnosti přirozeně předpokládá strukturaci duševního celku, tj. členění jednotné osobnosti na ohraničitelné, relativně samostatné složky. V psychologii existují různé názory na to, jaké složky vytváří ve svém souhrnu strukturu osobnosti. Jednotlivé přístupy se liší zejména počtem a typem vyčleňovaných složek.

## Interakční model osobnosti manažera

Efektivní práce manažera a dlouhodobé dosahování vynikajících výsledků záleží především na třech základních faktorech, určujících výkonnost manažera:

Schopnostech a motivaci manažera;
Modelových i reálných situacích, ve kterých pracuje;
Podmínkách pro výkon práce.




Obr. 2 Interakční model osobnosti manažera.

Schopnosti a motivaci – zjišťujeme při výběru manažera pro danou pozici a dále v průběhu profesní praxe je neustále rozvíjíme.

Situace – je nezbytné vytvořit model profese, kde zachycujeme typické pracovní situace v nichž se pracovník nejčastěji ocitá, které představují psychickou zátěž. Patří sem ale i ty nepředvídané situace, v nichž se ocitá občas, jsou neznámé, a k jejich řešení je nutná vysoká kreativita.

**Podmínky – jsou o firemní kultuře, o právních, personálních, bezpečnostních a jiných opatřeních, o konkrétních materiálních a finančních podmínkách v konkrétní instituci (firmě). Jejich ovlivněním lze nepřímo působit na motivační sféru všech pracovníků a tedy i manažerů.**

Základní požadavky na bezpečnostního manažera (dle Obr. 1) jsou názorně shrnuty do tří následujících tabulek podle výše uvedeného členění.

| ***Požadavky na osobu bezpečnostního manažéra*** | |
|---|---|
| ***Charakterové a volní požadavky na osobnost bezpečnostního manažera*** | |
| **Řešení problémů**<br>Bezpečnostní manažer projevuje dobré analytické dovednosti, zdravý úsudek a patřičně zvažuje všechny podstatné okolnosti.<br>jasně identifikuje úkol;<br>projevuje jasné chápání problému a s ním souvisejících otázek;<br>analyzuje problém přesně a s patřičným zdůvodněním;<br>umí stanovit jádro problému a klíčové body;<br>dokáže vzít v úvahu všechny podstatné informace; dokáže samostatně získávat informace z různých informačních zdrojů a nezávisle, nezaujatě je umí ověřovat, | **Nasazení a vytrvalost, motivace sebe i ostatních**<br>Předkládá řešení takovým způsobem, který přesvědčí ostatní o jeho přijatelnosti.<br>vytrvá a nepovolí v úsilí, setká-li se s odporem;<br>projevuje vysokou úroveň motivace, zaujetí a angažovanosti při řešení úkolu či problému;<br>projevuje schopnost motivovat jiné a budit důvěru<br>**Zvládání zátěže**<br>Konstruktivně reaguje na frustraci, je schopen |

| | |
|---|---|
| analyzovat;<br>je schopen samostatně získávat informace z různých informačních zdrojů a nezávisle, nezaujatě je dokázat ověřovat, analyzovat;<br>umí zdravý úsudek;<br>projevuje dobře organizovaný, naplánovaný a logický přístup;<br>je samostatný při řešení úkolů nebo problémů;<br><br>**Rozhodování**<br>Projevuje předvídavost, činí realistická rozhodnutí vycházející z dostupných zdrojů a je ochoten je převzít odpovědnost za svá rozhodnutí<br>činí rozhodnutí bez zbytečné prodlevy a jsou jasně formulovány;<br>opírá svá rozhodnutí o dodané informace a fakta;<br>prokazuje předvídavost a zvažuje krátko i dlouhodobé důsledky svých rozhodnutí;<br>stanovuje priority;<br><br>**Tvořivost**<br>Projevuje inovační přístup a originalitu při reagování na problémy a pružně posuzuje průběh akce.<br>zachovává si flexibilní přístup;<br>iniciuje používání alternativních postupů;<br>projevuje ochotu přijímat nové myšlenky, plány činností a rozhodnutí;<br>projevuje inovační, originální či laterální myšlení (využívající neobvyklých souvislostí)<br>vidí otázky a problémy se širší perspektivy, má cit pro detail ale neutápí se v něm;<br>je vizionářem, dokáže formulovat strategické vize a cíle ve svěřené oblasti; | přijmout kritiku, zachovává klid a umí řešit několik problémů najednou.<br>konstruktivně reaguje na neúspěch nebo frustraci;<br>je schopen zvládnout několik problémů najednou;<br>zůstává klidný, ovládá se a dokáže chladně uvažovat;<br>umí se vyhnout přehnaným reakcím;<br>zůstává tolerantní v konfliktní situaci, setká-li se s odporem.<br>je asertivní;<br>umí přijmout konstruktivní kritiku;<br>efektivně využívá čas<br><br>**Bezúhonnost**<br><br>Bezpečnostní manažer má takovou dosavadní praxi, která je příkladná a je nenapadnutelná, nezpochybnitelná z pohledu jeho důvěryhodnosti, spolehlivosti. Neexistují žádné předpoklady pro závislosti, ovlivňování, vydírání:<br><br>je beztrestný<br>nepoužívá návykové látky (drogy, alkohol apod.)<br>není rizikově závislý na penězích (zadluženost, hazardní hry, …)<br><br>**Osobní charisma**<br><br>je společensky i odborně uznávaný nebo akceptovatelný pro vrcholový i střední management, pro své bezprostřední spolupracovníky. |

| *Požadavky na osobu bezpečnostního manažéra* | |
|---|---|
| ***Předpoklady ve vztahu ke spolupracovníkům*** | |
| **Komunikační dovednosti**<br>Bezpečnostní manažer je schopen komunikovat jasně a stručně, jak ústně, tak i písemně, bere ohled na potřeby příjemce. Při výběru musí umět prokázat:<br>jasné a výstižné vyjadřování;<br>vhodné používání slovní zásoby, stylistiky a gramatiky;<br>než začne mluvit nebo psát, přemýšlí;<br>vyjadřování je takové, že jeho projev je plně srozumitelný;<br>je schopen volit takovou komunikaci, která odpovídá typu příjemce;<br>dokáže se vyhnout žargonu a slangu;<br>dokáže komunikovat ve složitých krizových situacích;<br><br>**Mezilidské vztahy**<br>Je vnímavý k přáním a názorům jiných lidí a je schopen s nimi spolupracovat. Je taktní a diplomatický.<br>je schopen projevit takt a diplomacii při jednání s jinými lidmi a při řešení situací;<br>dokáže projevit vnímavost, citlivost a vstřícnost k názorům a pocitům jiných lidí;<br>zajímá se o účinek svých slov na jiné osoby;<br>rozvíjí pracovní spolupráci s jinými, i lidmi. . Umí být členem týmu i jej vést. Je schopen týmové spolupráce;<br>vyhýbá se předsudkům a dogmatickým názorům. | **Prezentační a pedagogické schopnosti**<br><br>přesvědčivě prezentuje myšlenky, plány činností a rozhodnutí;<br>dokáže prodávat sebe, svůj tým, organizační celek, řešený problém;<br>dokáže využívat nejrůznější technologie pro svou prezentaci;<br>dokáže složité a odborné věci vysvětlovat jasně, srozumitelně i laikům;<br>je trpělivý;<br>má dobrý písemný projev, dokáže tvořit jasné, srozumitelné a závazné dokumenty |

| *Požadavky na osobu bezpečnostního manažéra* | |
|---|---|
| ***Předpoklady ve vztahu k instituci*** | |
| **Reprezentace zaměstnávající instituce a identifikace se s ní.**<br><br>Bezpečnostní manažer vytváří celkový kladný | |

| | |
|---|---|
| dojem a příznivý obraz instituce, ztotožňuje se s jejím posláním a způsoby jejího prosazování.<br>působí pozitivním a přijatelným dojmem, a to neustále;<br>je k instituci loajální;<br>zůstává věrný ideím, zásadám, kultuře a institucionální etice. | |

Požadavky na bezpečnostního manažera vyplývají především z poslání instituce a mohou se zásadním způsobem mezi rozličnými institucemi lišit. Jiné požadavky (zejména ve vztahu k instituci) budou v menší firmě vlastněné českým majitelem, v nadnárodní společnosti (kde může být potlačována jakýkoliv vztah k českému jazyku, kultuře, náboženství, politické příslušnosti apod.), ve státních bezpečnostních složkách (apolitičnost, hájení českých zájmů a zájmů koaličních partnerů či spojenců), v bezpečnostních orgánech politických stran (zde naopak je požadován pozitivní stav, oddanost k určité politice apod.).

## Problém poznávání osobnosti

Poznávání osobnosti konkrétního člověka je prubířským kamenem psychologie. Prověřuje vztah mezi realitou a její psychologickou reflexí. Popíšeme-li osobnost určitého člověka, umožní nám to předpovědět v nějaké míře jeho chování a prožitky v různých situacích. Čím přesnější bude popis osobnosti, tím přesnější bude predikce pravděpodobného chování a prožívání. Praktická využitelnost poznatků o osobnosti se koncentruje do dvou výstupů. Jde o to :

1. porozumět již ukončenému chování (tj. vysvětlit vnitřní pohnutky překvapivého činu nebo přiřadit určité chování jeho pravděpodobným původcům). U bezpečnostních manažerů může jít např.o to, objasnit, proč doposud spolehlivý a loajální manažer se dopustil hrubého prohřešku či o problém vytipovat, kdo pravděpodobně vězí za objasňovaným incidentem, kdo byl pravděpodobně jeho iniciátorem a vůdčí osobností a kdo se pouze "svezl".
2. odhadnout či predikovat chování člověka (např. vybrat nejvhodnějšího uchazeče pro manažerský post apod.).

V obou dvou případech vycházíme z úvah o osobnosti, z postřehů o tom, jak se nám posuzovaní jednotlivci jeví.

Místo hledání a objevování osobnostních (trvalejších) vlastností a rysů, které představují výčet obecných vlastností „ideálního“ manažera, považujeme za funkční **interakční, dynamický přístup ke konkrétní osobnosti manažera. V požadavcích a profilech, modelech profese se vymezují maximalistické, často nereální požadavky ideálního plnitele, často saturované nicneříkajícími všeobecnými pojmy jako jsou spolehlivost, flexibilita, loajalita, kreativita (co když je „kreativní“ proti zájmům instituce, firmy?).** Stačí, aby z nějakého důvodu manažer ztratil motivaci být loajální pro svého zaměstnavatele a v tento okamžik se všechny jeho původně pozitivní vlastnosti a schopnosti, původně požadované ve výběrovém řízení, obracejí proti samotnému zaměstnavateli, kterému má sloužit. Navíc je dobré si uvědomit, že loajalita a spolehlivost

není něco je jednou provždy dané, neměnné, je třeba to pěstovat, kultivovat, vytvářet podmínky, posilovat vztah ke instituci. I ten nejloajálnější pracovník je uplatitelný, je to jen otázka ceny. Vstupní psychologické vyšetření, sestávající se často z psychologických metod a postupů, využívaných v klinické praxi, poskytuje pouze vstupní orientační údaje, informace o dispozicích, které je nutno průběžně verifikovat, doplňovat, registrovat eventuelní změny, mít o nich přehled, hodnotit je – k tomu je určen forenzně psychologický audit.

Psychologickým základem zmíněného přístupu a zároveň psychologickým nástrojem k poznání osobnosti, je identifikace a porozumění **postojům**, které jedinec zaujímá v **konkrétních (pracovních, řídících) situacích** (zejména v podmínkách zvýšeného psychického zatížení). Jedná se především o postoje jedince **k ostatním lidem** (vztahově významným osobám a jejich prostřednictvím k referenčním skupinám a celé společnosti), **k vykonávané profesionální činnosti, včetně podmínek, v nichž svoji činnost realizuje** (a potažmo k instituci a jejím cílům) **a k sobě samému** (v nichž se odráží jeho sebepojetí a sebehodnocení), **k situacím**, v nichž se ocitá**.**

V postojích se odráží **kognitivní** (poznávací), **emocionální** a **konativní** pohotovost jednat určitým způsobem. Kognitivní procesy nám přinášejí poznatky. V emocích prožíváme jejich význam. V postojích, které kognitivní a emotivní aspekty psychiky integrují, zaujímáme vůči objektům **hodnotící vztahy**, tj. přiřazujeme jim určitou hodnotu, jeví se nám v určité míře žádoucí nebo nežádoucí, dobré nebo špatné.

V každém postoji je přítomná **anticipace** – tj. hodnocení předpokládaného efektu činnosti. Postoj není jen subjektivním odrazem skutečnosti. Úzce souvisí se sebepojetím člověka. Postoj si vytváříme nejen na základě poznání reality, a zároveň odpovídá tomu, co je pro nás žádoucí.

Obecně lze říci, že postoje determinují způsob jednání, resp. jsou konzistentní se způsoby jednání, pokud to situace dovoluje. Postoj tedy zakládá určitou konativní pohotovost, jejíž realizace v příslušném jednání však závisí na situačních podmínkách. V kognitivní složce postojů, jako nezbytného předpokladu podání jakéhokoliv výkonu se projevují **schopnosti a motivace jedince.**

***Požadavky na osobu bezpečnostního manažera***

Při vymezování osobnostních předpokladů nutno vycházet ze specifik činnosti při výkonu funkce bezpečnostního manažera (při naplňování obsahu sociální- profesionální role bezpečnostního manažera) v každé konkrétní instituci.

## Hlavní činnosti, které vykonává bezpečnostní manažer

K základním činnostem, které vykonává bezpečnostní manažer, patří zejména:

vytváření koncepce a systému (plány, opatření) bezpečnostních opatření v instituci;
činnosti na úseku prevence (předcházení), zamezování a odhalování jevů, ohrožujících vnitřní a vnější bezpečnost instituce, informační bezpečnost;

analýza hrozeb, typování rizik, rizikových pozic (součinnost s personálním útvarem – prověrky osob na bezpečnostně citlivých pozicích);
kontrolní činnost;
šetření mimořádných událostí (úniky informací, narušení systému, materiální a finanční škody atd.);
návrh, realizace adekvátních a včasných, proaktivních opatření;
školící (a osvětová) činnost;

## Požadavky na osobu bezpečnostního manažera:

Co považujeme za podstatné osobnostní kvality jsou **schopnosti a motivační sféra jedince.** (schopnosti – projevují se jako kompetence odborná, sociální – jednat s lidmi, motivovat je, úkolovat, hodnotit apod. V jeho motivační sféře se odráží i hodnoty, které jedinec uznává).
Jako každý manažer – **těžištěm jeho činnosti je práce s informacemi.** Projevuje se jako schopnost získávat, zpracovávat, analyzovat, hodnotit, využívat informace, a chránit je.
Oproti jiným manažerským pozicím – jejichž činnost je také založena na práci s informacemi – to, co odlišuje bezpečnostního manažera od ostatních manažerů je **charakter a obsah informací s nimiž pracuje, způsob jejich získávání** a **zacházení s nimi, využívání.**

Pro práci bezpečnostního manažera jsou vyžadovány klíčové kompetence, které mají následující strukturu:

**Sociální kompetence:**
- schopnost týmové práce
- kooperativnost
- schopnost čelit konfliktním situacím
- komunikativnost

**Kompetence ve vztahu k vlastní osobě:**
- kompetentní zacházení se sebou samým, nakládání s vlastní hodnotou
- schopnost reflexe vůči sobě samému
- vědomé rozvíjení vlastních hodnot lidského obrazu
- schopnost posuzovat sám sebe a dále se rozvíjet

**Kompetence v oblasti metod:**
- plánovitě se zaměřením na cíl uplatňovat odborné znalosti
- vypracovávat tvořivé, neortodoxní řešení
- strukturovat a klasifikovat nové informace
- dávat věci do kontextu, poznávat souvislosti
- kriticky přezkoumávat v zájmu dosažení inovací
- zvažovat šance a rizika

Kompetence sestávají z různých schopností a z jejich vzájemného ovlivňování. Získávají se reflexivně. V praxi jsou požadovány na bezpečnostním manažerovi především následující schopnosti:

**Komunikace a kooperace** – jako schopnost vědomě komunikovat a aktivně, tvůrčím způsobem přispívat ve skupinových procesech.

**Řešení problémů a tvořivost** jako schopnost poznávat problémy a odpovídajícím způsobem je tvořivě řešit

**Samostatnost a výkonnost** – jako schopnost samostatně plánovat, provádět a kontrolovat průběh prací a jejich výsledky.

**Odpovědnost** jako schopnost přijmout v přiměřeném rámci spoluodpovědnost.

**Přemýšlení a učení** jakožto schopnost dále rozvíjet proces vlastního učení a myšlení v souvislostech a systémově.

**Argumentace a hodnocení** jakožto schopnost věcně posuzovat a kriticky hodnotit vlastní, společné i cizí způsoby práce a výsledky.

Tyto kompetence nestojí vedle sebe izolovaně, ale tvoří harmonický celek.

***Jak hledat a vybírat bezpečnostního manažera***

Řada vlastností bezpečnostního manažera je obecně shodná s požadovanými vlastnostmi na výběr excelentního a v praxi úspěšného manažera v jakékoliv jiné lidské činnosti.

Americký týdeník Business Week každoročně vyhodnocuje nejlepší a nejhorší manažery nadnárodních gigantů. Při podrobné analýze rozhodujících kritérií, které určují „životnost“ bezpečnostního manažera, tj, jak dlouho se dokáže udržet ve funkci a vyhovět zájmům akcionářů, nezklamat jejich důvěru, uvádí tyto tři minimální a hlavní kritéria:

1) vysoký inteligenční a emoční kvocient;
2) vysoká odborná kvalifikace
3) dlouholetá zkušenost z výkonu manažerských funkcí

Dalšími rozhodujícími kritérii podle amerického týdeníku jsou kreativita a schopnost nést vysoké riziko. Zajímavou skutečností je fakt, že ani na dalších příčkách žebříčku nenalezneme nikde kritérium poctivosti.

Čtenáři jistě očekávají, že při vyhledávání a obsazování postu bezpečnostního manažera je třeba dodržovat velké množství specifických zásad. Je však účelné si uvědomit, že platí především zásady pro dobrou personální práci s následujícími aspekty:

Bezpečnostního manažera vybíráme jako každého jiného manažera, tj. při výběru dbáme na obvyklé požadavky na tuto pozici.

Při výběru navíc bereme v úvahu aspekty, týkající se specifik jeho bezpečnostní praxe v naší instituci (firmě).

Cíle, poslání, postavení instituce ve společnosti, ve státě nebo na trhu, kultura nebo mezilidské vztahy v instituci apod. mají rozhodující vliv jak na bezpečnostní politiku instituce, tak i na definování specifických požadavků a tedy i výběrových kritérií pro práci bezpečnostního manažera. Tato kritéria mohou být jedinečná a neopakovatelná, odlišná od běžné, podobné praxe v jiných institucích.

Velmi záleží na budoucím organizačním začlenění bezpečnostního manažera do hierarchické struktury organizace, na požadavcích na něj kladených a kompetencích, které má pro jejich realizaci.

Mimořádnou pozornost je žádoucí věnovat motivaci bezpečnostního manažera. Nemůžeme hodnotit motivaci jen v okamžiku výběru (nástupu), ale následně průběžně po celou dobu jím zastávané funkce. Musíme zajistit takové podmínky, aby bezpečnostní manažer pracoval loajálně ve prospěch instituce a minimalizovali jsme možnost personální fluktuace, která je z bezpečnostního pohledu velmi vysokým rizikem.

I s bezpečnostním manažerem je nutné neustále pracovat, motivovat jej, dávat prostor pro osobní rozvoj, kariérní růst, uplatnění, celkovou spokojenost.

V organizaci se doporučuje provádět forenzní audit (viz dále)s cílem nalézt všechny rizikové faktory personálního charakteru.

Musíme si rovněž uvědomit, že při výběru bezpečnostního manažera je třeba věnovat dostatek času i finančních prostředků. Při obsazování pozice bezpečnostního manažera v malé organizaci, která se začíná bezpečností teprve zabývat, může být alternativním řešením přijetí člověka bez potřebných bezpečnostních znalostí a odborností (ale při naplnění ostatních požadovaných kritérií) a následně zabezpečit jeho odborně-bezpečnostní růst. Při obsazování pozice bezpečnostního manažera ve velké instituci musí být na tuto pozici přijímán již „hotový" profesionál s odpovídající praxí. Zde je nutné ji věrohodně vyhodnotit. Běžně se používá ověřování referencí, ve státní sféře pak operativní bezpečnostní prověrky, které mohou trvat řádově i měsíce a které mají obvykle utajovaný charakter. Je tedy zřejmé, že toto úsilí mnoho stojí a musíme mít předem jasno, jaké bude mít bezpečnostní manažer v dané instituci úkoly.

## Forenzně psychologický audit

K poznávání a odhalování příčin selhání lidského faktoru v instituci slouží tzv. **forenzně psychologický audit** (jako součást dalších auditorských aktivit instituce)**.**

**Forenzně psychologický audit** představuje postup, při kterém se pomocí psychologických prostředků, postupů a metod získává přehled o kvalitě lidského činitele v instituci, s cílem odhalit existenci faktorů a podmínek, které zvyšují potenciální či reálně nebezpečí projevů nepoctivosti ze strany zaměstnanců, vytváří vhodné podmínky pro vznik institucionální (firemní) kriminality.

Je **zaměřen** k posouzení sociálně psychologických podmínek v instituci (ve firmě), k analýze rizikových pozic (zejména manažerských) a osobností, tyto pozice zastávající.

Cílem forenzně psychologického auditu je na základě **posouzení rizikovosti konkrétní pracovní pozice,** s důrazem na zjištění **zdrojů a oblastí** forenzně psychologického zájmu (kdy výkon profesionální role s sebou nese potenciální možnost - příležitost k nepoctivému, neloajálnímu jednání jejího realizátora), a současně s tím posoudit **spolehlivost** (loajalitu) **pracovníka** zastávajícího tuto pracovní pozici.

Rizikovost konkrétní pracovní pozice představuje statickou část (související s funkčním zařazením), spolehlivost pracovníka při výkonu této pozice pak část dynamickou, jejíž smyslem je zachytit změny v chování, jednání, postojích, činnosti, profesní kariéře, osobním životě pracovníka za určité (hodnocené) období.

**Výsledkem** forenzně psychologického auditu je soubor psychologicky relevantních informací o faktorech a činitelích osobnostního i situačního rázu, a jejich vlivu na chování, jednání, postoje pracovníka. Jejich analýza a syntéza umožňuje vyslovit závěr o míře loajality (poctivosti) pracovníka vůči instituci, o změnách, k nimž ve sledovaném období u pracovníka došlo (a jejich vlivu na jeho spolehlivost), o přítomnosti potenciálních či reálných nebezpečí selhání, příp. o možných příčinách takového selhání (v případě provádění auditu ex post). Závěry forenzně psychologického auditu umožňují vedení instituce přijímat potřebná opatření právního, organizačního, bezpečnostního a personálního rázu.

Forenzně psychologický audit je proto zaměřen k postižení především následujících skutečností:

**1. týkajících se rizikovosti pracovní pozice**

- jaký je charakter (klíčové charakteristiky) činnosti, kterou pracovník na konkrétní pracovní pozici vykonává, pracovní režim (pracovní doba)
- začlenění zastávané pracovní pozice v hierarchii instituce
- prostředky, užívané pracovníkem k výkonu jeho pracovní pozice
- které zájmy instituce při výkonu své profesní role může pracovník ohrozit (materiální, finanční informační zdroje), jakým způsobem a v jakém rozsahu (problém jeho kompetencí)
- jaké kontrolní mechanismy (jejich četnost, hloubka) se ve vztahu k zastávané pracovní pozici uplatňují
- jaký je charakter (četnost, pravidelnost, obsah) kontaktů (v horizontální i vertikální rovině, uvnitř instituce a mimo ní), které souvisí s výkonem zastávané pozice
- materiální, finanční a další podmínky, související s výkonem zastávané pracovní pozice
- jaká bezpečnostní a režimová opatření ze strany instituce se vztahují na zastávanou pozici (ve vztahu k ochraně pracovníka na dané pozici)

**2.týkajících se spolehlivosti pracovníka**

- jak pracovníka uspokojuje jeho pracovní zařazení a činnost, která z něho vyplývá (uplatňuje své zkušenosti, dovednosti, znalosti)
- jak hodnotí kompetence, kterými s výkonem profesní role disponuje
- jak je spokojen s prostředky a podmínkami, které k výkonu své funkce má k dispozici
- jak je spokojen s finančním ohodnocením za vykonávanou práci, jaká je jeho představa o odpovídajícím hodnocení
- jak je spokojen s materiálním a technickým zabezpečením, případně dalšími firemními (zaměstnaneckými) výhodami
- jaké charakter interpersonálních vztahů na pracovišti převládá při kontaktu s nadřízenými, podřízenými, kolegy
- jak hodnotí kontrolní mechanismy v instituci (ve vztahu ke své pracovní pozici)
- jak hodnotí kontakty, do kterých vstupuje při výkonu své profesní role (dovnitř instituce, navenek)
- jak hodnotí své mimopracovní kontakty a vztahy

- v jakých interpersonálních konfliktech se v hodnoceném období pracovník ocitnul, s kým, z jakých důvodů
- potkaly zaměstnance v hodnoceném období závažné změny v pracovním či osobním životě (stresující události)
- jaké cíle chce pracovník dosáhnout v nejbližším období (profesní, životní)
- co ovlivňuje celkovou životní spokojenost pracovníka (zejména co snižuje jeho spokojenost?) aj.

**Literatura**


1. BRABEC, F. a kol., *Bezpečnost pro firmu, úřad, občana*. Public History: 2001. ISBN 80 86445-04-06
2. ČÍRTKOVÁ, L., *Kriminální pasychologie*. Praha: Eurounion, 1998. ISBN 80-85858-70-3
3. HALL, C., S., LINDZEY, G., *Psychológia osobnosti.* Bratislava: Slovenské pedagogické nakladateľstvo, 2002. ISBN 80-08-03384-3
4. JANÍČEK, P., ONDRÁČEK, E., *Řešení problémů modelováním*, Brno, Vysoké učení technické, 1998, ISBN 80-214-1233-X
6. KAPLANOVÁ, V., NOVÁČEK, J., *Teorie a praxe řízení ICT pro vrcholový management I*., zápisky z workshopu, 5.11.2003. Praha: Akademie ICT managementu.
7. KOHOUTEK, R., ŠTĚPANÍK, J., *Psychologie práce a řízení*. Brno: Akademické nakladatelství CERM, 1999. ISBN 80-214-1552-5
8. KULAJOVÁ, T., HALOUZKA, J., SEIGE, V., *Genesis aneb Jak vzniká bezpečnostní útvar*, DSM, č. 2, 2001, str. 32-35
9. MIKULÁŠTÍK, M., *Komunikační dovednosti v praxi*. Praha: Grada, 2003. ISBN 80-247-0650-4
10. MITNICK, K., SIMON, W., *Umění klamu* (překlad z originálu „The Art of Deception: Controlling the Human Element of Security"). Praha: HELION S.A., 2003. ISBN 83-7361-210-6
11. SPURNÝ, J., *Psychologie výslechu*. Praha: Portál, 2003. 114 s. ISBN 80-7178-846-5
12. Průzkum stavu informační bezpečnosti v ČR 2003, Praha, Ernst & Young, DSM, NBÚ, 2003. ISBN 80-902858-8-0


**Summary**


Safety is a theme discussed from the point of view of various aspects very often. In the commercial sphere, it is given into relation to the issues of financing, i.e. it must be economically worthwhile for the institution (firm, non-profit-making organisation, state agency and authority). It is not important whether it is a question of general (physical) safety or the safety of information systems, i.e. "information safety" as such.
At selection, by filling the position of safety manager by a specific person we always take into account requirements in relation to the abilities of the candidate. We analyse his/her experience and qualifications, knowledge and general intellectual capabilities, character traits and will qualities, prerequisites for good relations to colleagues and to the employer. In the contribution, all these attributes are analysed in detail.

Effective manager's work and long-term excellent results depend especially on the three basic factors that determine manager's performance, capabilities and motivation, on model and real conditions in which the manager works and on the conditions for performing his/her work.
In the contribution basic aspects of searching for and selecting a person for the position of safety manager are summarised. In the final part attention is paid to the forensic psychological audit, which is a tool for understanding and identifying causes of human failures in the institution.
As far as safety is concerned, it is not only the moment of selection of persons for safety-sensitive positions, but also the capabilities of these persons to be loyal to assigned tasks and the employer in the course of time that is decisive.