KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČESKÉ REPUBLIKY

ČLENOVÉ KOMORY PODNIKŮ KOMEČNÍ BEZPEČNOSTI ČR

ČASOPIS BEZPEČNOST S PROFESIONÁLY VZNIKÁ DÍKY PODPOŘE TĚCHTO ČLENSKÝCH FIREM KPKB ČR:

SAFE Technology SAFETE, s.r.o.
Na Výsluní 519/17
100 00 Praha 10 – Strašnice
www.systemkiss.cz

HIGH SECURITY PRODUCTS, a. s.
Pod stárkou 378/3
140 00 Praha 4
www.h-s-p.cz

Agentura Pancéř, s. r. o.
K dubu 2330/2b, Chodov
149 00 Praha 4
www.pancer.cz

European Security Solutions s.r.o.
Tyršova 3214/8
695 01 Hodonín
www.eseso.cz

ATON Security s.r.o.
Na Stráži 1576/35
190 00 Praha 9
www.cleanline.cz

TRIVIS – Centrum vzdělávání, s.r.o.
Na terase 355/8
182 00 Praha 8
www.trivis.cz

ECES Institut, s.r.o.
Kutuzovova 547/13
703 00 Ostrava
www.eces.cz

WAKENHAT s.r.o.
Sazečská 560/8
108 00 Praha 10 Malešice
www.wakenhat.cz

SYBENAM - Systém bezpečnosti na míru
U Klavírky 2627/7
150 00 Praha 5
www.sybenam.cz

ELSERVIS - Ivo Kolář
Dědinská 898/15
161 00 Praha 6

SIMACEK FACILITY CZ spol. s r. o.
Trnkova 34
628 00 Brno
www.simacek.cz

UNISEC s.r.o.
Riegrova 54
261 01 Příbram
www.unisec.cz

RAM SECURITY s. r. o.
Na Výhledu 139
250 66 Zdiby
www.security-cz.eu

ANIM plus – RS, s. r. o.
Areál TJ MEZ, 775 01
Vsetín – Ohrada
www.anim.cz

General Provider s.r.o.
Sídlo: Kodaňská 432/15
101 00 Praha 10
www.generalprovider.cz

SECURITY MONIT s.r.o.
Hoblíkova 548/6
613 00 Brno
www.security-monit.cz

APEurope s. r. o.
Kaprova 42/14
110 00 Praha 1
www.apeurope.cz

Security MCO s.r.o.
Struha 865
517 54 Vamberk
www.mco-security.cz

Trade Corporations s.r.o.
Mostecká 273/21
118 00 Praha 1
info@tcorp.cz

Solidita s.r.o.
Jeřábová 419
250 73 Radonice
www.solidita.cz

SEKURO & Group s.r.o.
Na Mlýnici 33/1a
702 00 Ostrava
www.sekuro.cz

CENTURION loss prevention a. s.
Kundratka 17/1944
180 82 Praha 8
www.centurionlp.cz

ABAS IPS Management s. r. o.
Jankovcova 1569/2c
170 00 Praha 7
www.abasco.cz

Preventa Service s.r.o.
Kutuzovova 547/13
703 00 Ostrava – Vítkovice
www.preventa.cz

OKO 69 s.r.o.
Březinova cesta 192/1
412 01 Litoměřice
www.oko69.cz

Česká pošta Security, s.r.o.
Sídlo: Politických vězňů 909/4
Nové Město, 110 00 Praha 1
pistek.roman@cpost.cz

ARES GROUP s.r.o.
Libušská 189/12
142 00 Praha 4
www.ares-group.cz

Stratia s.r.o.
Podolská 613/28
147 00 Praha 4
www.stratia.cz

Národní stálá konference o bezpečnosti (NSKB), z.s.
Chudenická 1059/30
102 00 Praha 10
www.nskb.cz

Pro Bank Security, a. s.
Václavské nám. 21
110 00 Praha 1
www.probank.cz

O.K. SHOOTING Security, s.r.o.
Záhradná 746/36
900 51 Zohor
Slovenská republika
www.sbs-shooting.sk

GADO s.r.o.
Heršpická 11b
639 00 Brno
www.gado.cz

Ing. Martin Neuschl
Šachetní 391
261 01 Příbram

INPOS SECURITY
Křížkový Újezdec 42
251 68 Kamenice
www.inpos.cz

PRIMM bezpečnostní služba s. r. o.
Kutnohorská 309
109 00 Praha 10
www.primm.cz

INCRISCO s.r.o.
Sádecká 400
252 30 Řevnice
info@incrisco.cz

3S security s.r.o.
Holušická 2253/1
148 00 Praha 4
www.3ssecurity.cz

Gatum Group, s.r.o.
Italská 2581/67
120 00 Praha 2
www.gatum.cz

ČVUT - Fakulta biomedicínského inženýrství
Sportovců 2311, Kladno
https://www.fbmi.cvut.cz/

ČASOPIS KOMORY PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČR
LEDEN - BŘEZEN/2025

BEZPEČNOST S PROFESIONÁLY

BEZPEČNOST VEŘEJNÝCH PROSTRANSTVÍ
WORKSHOP V POSLANECKÉ SNĚMOVNĚ PARLAMENTU ČR

SYSTÉM PROSTOROVÉHO ODPOSLECHU
HISTORIE A SOUČASNOST

NOVÝ ZÁKON O KYBERNETICKÉ BEZPEČNOSTI
CO ZNAMENÁ PRO POSKYTOVATELE SLUŽEB KOMERČNÍ BEZPEČNOSTI?

ISSN 2336-4793

WWW.KPKBCR.CZ

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI
ČESKÉ REPUBLIKY

BEZPEČNOST
S PROFESIONÁLY

Šéfredaktor
Mgr. Bc. Kateřina Poludová, DiS.

Jazyková spolupráce
PhDr. Alena Hasáková

Redakční rada
Ing. Václav Jahodář
Mgr. Bc. Kateřina Poludová, DiS.
Ivo Kolář
PhDr. Barbora Vegrichtová, Ph.D., MBA

Inzerce
kpkbcr@volny.cz

Nesignované fotografie a články
Redakce

Vydavatel
KPKB ČR, Vrážská 1562/24a, 153 00 Praha 5

Registrace
Bezpečnost s profesionály
MK ČR E 20140
ISSN 2336-4793

Tisk
Bittisk s r. o., B. Němcové 53, 746 01 Opava

Rozšiřování zdarma

Na zadních stranách obálky
členové KPKB ČR

OBSAH

ÚVODNÍ SLOVO

Vážení čtenáři,

zdá se, že letošní rok, do kterého jsme vstoupili velmi hekticky, nebude vůbec jednoduchý. Náročný bude zejména s ohledem na celosvětové změny pojící se s nástupem Donalda Trumpa do prezidentského úřadu v USA. Jeho postoj k válce na Ukrajině, názory na její možné ukončení, výhrady k fungování Evropské unie, zpochybňování stávajícího uspořádání NATO či další jeho zamýšlené politické a ekonomické kroky, to vše vnáší do již tak nepříliš hladce fungující evropské i naší domácí ekonomiky nejistotu a problémy.

Již teď jsou patrné některé důsledky – masové propouštění zaměstnanců, dramatické snižování výdajů, pokles odbytu zboží hlavně do zámoří a další. S tím souvisí i sociální nestabilita a negativní dopady na psychiku jedinců, jež nezřídka eskalují do násilných projevů vůči společnosti, systému či jedincům. Sílí projevy islámského radikalismu, stále častěji jsme svědky narůstající radikalizace a násilných projevů u mladistvých, kdy stoupá počet brutálních napadení, či dokonce vražd. Nedávné útoky ve školách, obchodních centrech a jinde jsou toho přímými důkazy.

Je zřejmé, že máme před sebou komplikovanou a zhoršující se bezpečnostní situaci, ať už z hlediska ochrany měkkých cílů či kritické infrastruktury, veřejného pořádku, zdraví a životů občanů. Nicméně navzdory výše zmíněným skutečnostem věřím, že budeme schopni všem bezpečnostním hrozbám současnosti stále účinněji čelit.

Jednou z viditelných aktivit, kterými se naše Komora snaží přispět ke zlepšování bezpečnosti v České republice, je pořádání vysoce specializovaných akcí pro širokou odbornou veřejnost. Pod záštitou poslance Roberta Králíčka připravujeme 10. dubna 2025 na půdě Poslanecké sněmovny Parlamentu ČR workshop na téma „Ochrana měkkých cílů – veřejná prostranství". Na ten naváže 12. června 2025 již tradiční konference „Ochrana měkkých cílů", která se uskuteční v Kongresovém centru CITY, Praha 4 Pankrác – rovněž jejím spolupořadatelem bude Komora podniků komerční bezpečnosti ČR. A jistě v této oblasti nezůstane jen u těchto dvou zajímavých akcí.

Jsme si velmi dobře vědomi, že narůstá potřeba vytvářet vhodné podmínky pro úspěšné a efektivní vykonávání všech bezpečnostních činností, tedy i našich komerčních, jak to je ve vyspělých zemích běžné a obvyklé. Nelze akceptovat ignoranci při zavádění bezpečnostních standardů a postupů jen z důvodu nedostatku finančních prostředků. Tyto prostředky se vždycky najdou, jen je smutné, že zpravidla až ve chvíli, kdy dojde k nějakému fatálnímu incidentu.

Navzdory všem chmurným myšlenkám, jež jsem výše zmínil, Vám ovšem přeji pozitivní mysl – ať Vám ji co nejvíce rozjasní vbrzku přicházející krásné jarní dny.

Ing. Václav Jahodář
prezident KPKB ČR

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI
ČESKÉ REPUBLIKY

PŘEDSTAVENÍ ČLENŮ NOVÉHO PREZIDIA KOMORY PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČR

Ing. Václav Jahodář
prezident

Vážení kolegové a kolegyně,

dovolím si Vám alespoň pár řádky přiblížit moji kariéru a svoje plány v KPKB ČR do budoucna.

Jsem absolventem Fakulty strojní ČVUT, obor jaderné elektrárny. Pracoval jsem na jaderné elektrárně Dukovany jako specialista spouštění jaderné části. Poté jsem se stal inspektorem jaderné bezpečnosti Státního dozoru nad jadernou bezpečností. Po demokratických změnách jsem se od roku 1990 začal podílet na vzniku a budování domácí zpravodajské služby (později BIS). Zde jsem se zabýval především bojem proti terorismu, nelegální migraci a zpravodajským službám cizích mocí. Byl jsem součástí vrcholného managementu služby.

Za dosažené výsledky mi byla udělena prezidentem Václavem Havlem medaile. V roce 2023 jsem obdržel plaketu za službu vlasti od ředitele BIS generála Ing. Michala Koudelky. Po skončení aktivní služby jsem se na MZV podílel na budování koncepce řešení krizových situací ambasád ČR v zahraničí. Následně od roku 2002 jsem pracoval ve Škoda auto jako vedoucí bezpečnosti a ochrany značky, což zahrnovalo jak otázky ochrany majetku a osob, ale i oblast ochrany informací, prototypů atd. ve všech zemích, kde Škoda auto má své závody.

Od roku 2008 pracuji ve společnosti Abas IPS Management s.r.o. na pozici ředitel obchodu a strategie. Od roku 2009 jsem členem KPKB ČR a aktivně se podílím na její činnosti. Osobně jsem přesvědčen , že právě naše Komora díky svému zaměření , vývoji a současnému obsazení má všechny předpoklady být tou správnou, kvalifikovanou a zejména objektivní autoritou, která je partnerem jak pro subjekty soukromého bezpečnostního podnikání, tak ale i pro státní a veřejnou správu a jiné instituce. Mojí snahou je dosažení lepších podmínek pro výkon soukromých bezpečnostních činností z pohledu legislativy, zlepšení podmínek ohodnocení těchto činností, možností zvyšování odbornosti a kvalifikace apod. Rovněž chci přispět k regeneraci tohoto odvětví tak, aby bylo veřejností a zejména odběrateli služeb vnímáno jako profesionální, plnohodnotná a respektovaná služba, která je partnerem adekvátním složkám státu, zejména pak IZS.

Libor Marada
1. viceprezident

Je mi 57 let. Vzděláním a původní profesí jsem chemik a pracoval jsem ve farmaceutickém průmyslu. Ale již od studií jsem současně pracoval ve společnosti SECURITY MONIT s.r.o., která je dnes členem Komory podniků komerční bezpečnosti České republiky.

Ve společnosti SECURITY MONIT s.r.o. pracuji na pozici obchodního ředitele. Kromě naší KPKB ČR aktivně působím v HOSPODÁŘSKÉ KOMOŘE České republiky, kde jsem členem představenstva Okresní hospodářské komory Brno - venkov. Jako hlavní cíl mého působení v obou komorách je snaha o kultivaci trhu soukromých bezpečnostních služeb, a především připomínkování legislativy, která naši činnost ovlivňuje. Tímto bych chtěl i v dalším období přispívat k činnosti naší KBKB ČR. Jinak jsem rozvedený, mám dva syny ve své péči a ve volném čase mne baví cestovat a sport, především lyžování.

Miroslav Slabý
viceprezident pro oblast soukromých bezpečnostních služeb

Je mi 48 let a v oblasti bezpečnosti mám dlouholetou praxi. V roce 1998 jsem spolu s kolegy založil bezpečnostní bezpečnostní agenturu OKO 69, s.r.o., kterou dodnes vlastním, řídím a jsem statutárním orgánem.

Čím mohu přispět KPKB ČR?

Za téměř třicet let praxe v komerční bezpečnosti znám snad veškerá úskalí, kte-

rá tento velmi důležitý obor má.

Pokud mám zmínit základní problémy tohoto oboru?

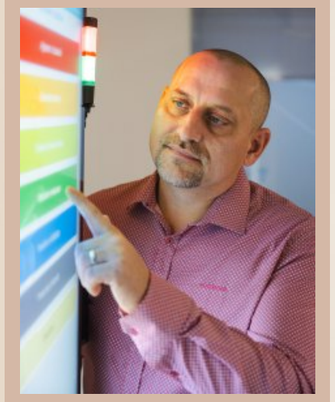
Minimální respekt vůči činnostem a práci soukromých bezpečnostních služeb a to jak ze stran běžných občanů, tak i potencionálních klientů.

Hitem dnešní doby je enormní tlak na co nejnižší cenu, bez ohledu na současné dění v zemi. Tím myslím migrační krizi, válku na Ukrajině, větší počet nepřizpůsobivých občanů páchající trestnou činnost, atd.

Dále určitě nemohu opomenout nedostatek pracovníků, kteří by chtěli u soukromých bezp. služeb pracovat.

Na závěr musím zmínit i problém v našich řadách, kdy dochází ke konkurenčnímu podhodnocování nabízených cen, za hranu ekonomické legální únosnosti.

Chtěl bych svými zkušenostmi a znalostmi v oboru, přispět k pozitivnímu vývoji komerční bezpečnosti a jejímu vnímání



Ing. Jan Burian
viceprezident pro oblast bezpečnostních technologií

Jan Burian vystudoval Fakultu elektrotechnickou ČVUT se zaměřením na telekomunikační a informační techniku. Od roku 2000 se aktivně pohybuje v telekomunikační branži.

Se svým týmem vyvinul moderní IT systémy pro call centra či pokročilé dispečerské systémy. Posledních 12 let se věnuje především vývoji a provozu bezpečnostních varovných systémů. Je ředitelem společnosti SAFE Technology SAFETE s.r.o., která vyvíjí a implementuje nejrozšířenější varovný systém v České republice, krizový informační a svolávací systém KISS.

Čím mohu přispět KPKB ČR a bezpečnostnímu oboru?

Z praxe víme, že jedním z největších problémů v krizových situacích je komunikace, konkrétně rychlé a přesné předávání informací o vzniku a vývoji dané události. Každá sekunda zpoždění a chyba v komunikaci může v důsledku vést ke značným škodám na majetku, či dokonce k ohrožení života osob. A právě to je moje téma. Informace o tom, jak komunikovat při krizové situaci a jak procesy ve firmě či organizaci automatizovat, jsem připraven konzultovat do nejmenšího detailu.

Mgr. Petr Smorádek, DiS.
člen prezidia

Po ukončení střední školy se zaměřením na podnikatelskou činnost jsem se rozhodl pro studium VOŠ TRIVIS, obor prevence kriminality.

Po řádném ukončení studia na TRIVIS jsem se rozhodl nejprve získat praktické zkušenosti v rámci soukromých bezpečnostních služeb (SBS) a postupně si zvyšovat vzdělání v o-boru.

Ve 22 letech, bezprostředně po ukončení školy, jsem proto začal pracovat u SBS Černí šerifové. Dalším mým působištěm byla firma ABL. Zde jsem pracoval na pozicích velitele směny a poté dispečera v obchodním centru DBK. Souběžně s prací pro ABL jsem absolvoval bakalářské studium v oboru sociálně právní činnost na Vysoké škole práv v Karlových Varech. V ABL jsem skončil po třech letech, kdy jsem dostal nabídku na pracovní pozici strážníka Městské policie v Mníšku pod Brdy. K městské policii jsem nastoupil v roce 2012. V roce 2016 jsem se stal zástupcem vedoucího MP a v roce 2018 jsem se stal vedoucím MP. Během zaměstnání jsem vystudoval magisterský obor Bezpečnostní studia na CEVRO institut Praha.

V roce 2023 jsem byl zvolen předsedou Svazu obecních a městských policií Středočeského kraje, kde jsem za své období prohloubil spolupráci městských a obecních policií Středočeského kraje mezi Krajským úřadem Středočeského kraje, Policií ČR Středočeského kraje a dalšími odbornými institucemi.

V následujících letech se chci aktivně podílet na pořádání konferencí a dalších odborných akcí. Dále se zaměřím na sebevzdělávání a dokončení postgraduálního studia.

Ing. Karel Hříbal, Csc.
člen prezidia

Vystudoval fakultu elektrotechniky ČVUT Praha, je kandidátem technických věd v oboru elektronika a vakuová technika.

Do roku 1991 pracoval v oboru výzkumu, vývoje a výroby elektronických systémů pro obranu a bezpečnost státu. Od roku 1991 stál v čele společnosti, která od počátku svého vzniku působila na trhu komerční bezpečnosti zejména v oblasti vývoje a výroby zabezpečovacích systémů a technických služeb pro ostrahu osob a majetku. Je technickým specialistou a bezpečnostním konzultantem významných privátních subjektů v ČR.

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI
ČESKÉ REPUBLIKY

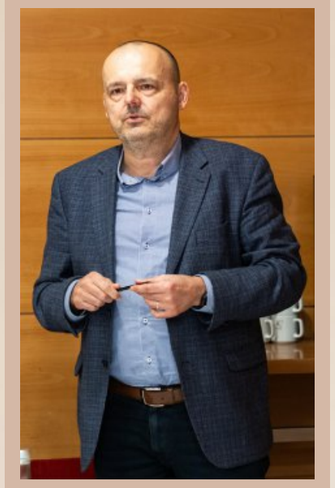
Ing. Daniel Vlček
člen prezidia

Ing. Daniel Vlček vystudoval Vysokou školu ekonomickou v Praze, kde získal titul v oboru Ekonomika a management. Již více než 15 let se pohybuje v oblasti bezpečnosti, strategického poradenství a moderních technologií pro veřejný i soukromý sektor.

Jako zakladatel a jednatel společnosti Gatum se zaměřuje na integrovanou bezpečnost, ochranu měkkých cílů a implementaci inovativních technologií, například pokročilé analytiky kamerových systémů či konceptů Safe City. Dále je jednatelem společností EnerSolutio a UnitX, které přinášejí řešení v oblasti energetiky a digitalizace.

V minulosti spolupracoval se zahraničními např. izraelskými nebo americkými start-upy v oblasti bezpečnosti, působil například jako národní koordinátor projektu 5G pro 5 měst při Ministerstvu pro místní rozvoj, kde řídil zavádění 5G technologií do vybraných českých měst. Je aktivním členem několika odborných a zájmových organizací včetně AFCEA, Komory podniků komerční bezpečnosti, Hospodářské komory a dalších. Svou komplexní expertizou se podílí na tvorbě strategií pro bezpečná a odolná města budoucnosti.

V rámci KPKB ČR se mohu aktivně zapojit do odborných diskusí, sdílet praktické zkušenosti z realizovaných projektů a přinášet nové pohledy na integraci moderních technologií do bezpečnostní praxe. Zároveň mohu přispět k propojování veřejného a soukromého sektoru, zejména v oblasti měkkých cílů a strategického plánování.



Ing. Jiří Giptner
člen prezidia

Mou ambicí je přispět ke kultivaci privátní bezpečnosti, a to zejména v těchto oblastech:

- Vytváření podmínek pro spolupráci nejen jednotlivých agentur, ale i profesních sdružení. Jak? Mluvit spolu, tupit hrany a hroty...
- Zreálnění očekávání a požadavků klientů a prosazení spravedlivé ceny a odpovídajícího zařazení osob se zdravotním postižením. Jak? Edukovat státní správu a samosprávu, klienty, odbornou veřejnost.

OSVČ (2020 - současnost)

Bezpečnostní poradenství. Vzdělávání a trénink. Nastavení a zajištění bezpečnosti. Řízení bezpečnostních rizik, opatření k jejich minimalizaci, řešení mimořádných situací. Interim security and sales management.

SECURITAS ČR s.r.o. (2010-2020) – Chief Risk Management Officer pro ČR a SK, pokurista společnosti

Sestavení a vedení pracovního týmu zabývajícího se řízením rizik. Nastavení pravidel, procesů a modulu pro evidenci, vyhodnocování a reporting interního auditu. Garant a osoba zodpovědná za průběh projektu Digitalizace, projektu GDPR, projektu Intranet, za každoroční revizi interních standardů, za implementaci politik mateřské společnosti do standardů v ČR a SK.

DORA Security a.s. (2002-2010) – Bezpečnostní ředitel, člen a předseda dozorčí rady

Vedení týmu zaměřeného zejména na supervizi, speciální služby a vnitřní bezpečnost. Podíl na vytvoření a implementaci Systému hodnocení kvality poskytovaných služeb, vedení projektu Ochrana informací a na základě jeho výsledků přenastavení souvisejících procesů ve společnosti. Vytvoření interní metodiky pro poskytování služby Inventura a služby Kontrola práce neschopných a jejich následné komerční poskytování.

Bezpečnostní složky České republiky (1991-2002)

Ing. Marek Hejduk
člen prezidia

Již od roku 2017 do současné doby pracuji jako bezpečnostní ředitel společnosti CD Cargo, předtím jsem více než dvacet let byl příslušníkem Policie České republiky a pracoval ve složkách Ministerstva vnitra ČR v bezpečnostní problematice.

V Komoře podniků komerční bezpečnosti České republiky, z.s., bych byl rád přínosem při tvorbě legislativních norem a koncepce využití soukromých bezpečnostních služeb v případech situací vyžadujících užití těchto složek pro potřeby státu.

WORKSHOP K BEZPEČNOSTI VEŘEJNÝCH PROSTRANSTVÍ V POSLANECKÉ SNĚMOVNĚ

Komora podniků komerční bezpečnosti ČR připravuje důležitý workshop v Poslanecké sněmovně, zaměřený na bezpečnost veřejných prostranství.

V reakci na nedávné události v Německu, Číně a Spojených státech, kde došlo k vražedným útokům na veřejných prostranstvích s použitím vozidel, střelných zbraní či nožů, se Komora podniků komerční bezpečnosti ČR rozhodla uspořádat odborný workshop věnovaný této problematice. Akce se uskuteční v Poslanecké sněmovně a bude se zabývat prevencí, ochranou a připraveností veřejného sektoru i odborné veřejnosti na tyto hrozby.

Klíčové informace o workshopu:

- **Téma:** Veřejná prostranství jako specifický typ měkkého cíle
- **Termín:** 10. duben 2025
- **Místo:** Poslanecká sněmovna ČR
- **Organizátor:** Komora podniků komerční bezpečnosti ČR
- **Záštita:** poslanec Robert Králíček
- **Kapacita:** cca 100 účastníků

Komora zahájila spolupráci se Svazem měst a obcí, oslovila Ministerstvo vnitra a další partnery s cílem zajistit širší odbornou účast.

Co workshop nabídne?

Workshop se zaměří na zvýšení bezpečnostního povědomí o specifikách veřejných prostranství jako měkkých cílů. Hlavní témata:

- Hrozby a rizika na veřejných prostranstvích (analýza trendů, typologie útoků, prevence a krizová komunikace).
- Metody posuzování bezpečnosti (standardizované postupy, právní rámec, zapojení veřejné správy a bezpečnostních složek).
- Praktické přístupy ke zvýšení odolnosti veřejných míst a ochraně obyvatelstva.
- Spolupráce mezi veřejným a soukromým sektorem v oblasti prevence a reakce na incidenty.

Propojení s červnovou konferencí Ochrana měkkých cílů

Téma bezpečnosti veřejných prostranství bude rovněž jedním z klíčových bodů červnové konference Ochrana měkkých cílů, kterou Komora podniků komerční bezpečnosti ČR spolupořádá. Výstupy z březnového workshopu poslouží jako základ pro hlubší diskusi a formulaci doporučení v této oblasti. Některé výstupy budou prezentovány ve speciálním panelu. Aktuální informace o konferenci najdete na webu: ochranamekkychcilu.cz

Proč se zúčastnit?

Workshop je určen především zaměstnancům měst a obcí, organizátorům veřejných akcí a odborníkům z oblasti bezpečnosti. Přinese cenné informace a praktické zkušenosti od předních expertů na ochranu měkkých cílů.

Komora podniků komerční bezpečnosti ČR, z.s., vyzývá všechny zájemce k účasti a k doporučení akce odborným partnerům či kolegům.

Pokud se chcete workshopu zúčastnit nebo jej doporučit dalším odborníkům, kontaktujte nás na e-mailu: sekretariat@kpkbcr.cz.

PaedDr. Martin Uher

Kontext tématu – několik vybraných událostí z posledních 10 let

Zde je uvedeno několik příkladů útoků na veřejná prostranství. Do výběru byly zařazeny útoky provedené podobně jako diskutovaný útok v Magdeburgu. Pokud by do výběru byly zařazeny i další vektory útoku, byl by seznam mnohonásobně delší.

1. ledna 2025, New Orleans: Muž najel pronajatým pickupem do davu lidí, nejméně 14 lidí mrtvých a desítky dalších zraněných.

20. prosince 2024, Magdeburg: Řidič najel autem do vánočního trhu, zemřelo 11 lidí, desítky zraněných.

24. listopadu 2024, Zhuhai: Řidič řádil se svým SUV v areálu sportovního centra, 35 mrtvých a 43 zraněných.

19. listopadu 2024, Dingcheng: Řidič zaútočil autem na studenty a rodiče před školou, 30 zraněných, vozidlo se naštěstí rozbilo a řidič nemohl v řádění pokračovat.

11. ledna 2023, Guangzhou: Řidič vjel cíleně do davu osob, 6 zabil, dalších 29 zranil.

8. června 2022, Berlín: Řidič najel autem do davu lidí, zabil učitelku a zranil 14 žáků.

21. listopadu 2021, Waukesha: Muž vjel autem do Christmas Parade, zabil 6 lidí a zranil dalších 62.

1. prosince 2020, Trevír: Řidič vjel na pěší zónu, zabil pět lidí včetně kojence, zranil dalších asi 20 chodců.

1. ledna 2019, Bottrop a Essen: Řidič najížděl autem do skupin lidí v Bottropu a Essenu, zranil pět osob a měl úmysl zabíjet dál.

12. září 2018, Mishui: Řidič SUV na náměstí zabil 15 osob a 43 dalších zranil.

23. dubna 2018, Toronto: Útočník najel dodávkou do chodců, vedlo to k úmrtí deseti lidí a zranění 16 dalších.

31. října 2017, New York: Útočník najel pronajatým pickupem na cyklostezku na Manhattanu, 8 lidí usmrtil a dalších 11 zranil.

7. srpna 2017, Barcelona: Útoky vozidly si vyžádaly 16 obětí a na 130 zraněných.

19. června 2017, Finsbury Park: Dodávka najela do skupiny osob, což vedlo k úmrtí jednoho člověka a ke zranění deseti dalších.

3. června 2017, London Bridge: Útok na London Bridge a Borough Market si vyžádal osm obětí a desítky zraněných.

7. dubna 2017, Stockholm: Útok nákladním autem si vyžádal pět mrtvých a 15 zraněných.

22. března 2017, Westminster: Útok u britského parlamentu v Londýně si vyžádal pět obětí a desítky zraněných.

8. ledna 2017, Jeruzalém: Útočník najel nákladním autem do skupiny vojáků, čtyři vojáky zabil a 15 dalších zranil.

19. prosince 2016, Berlín: Řidič s ukradeným kamionem najel do davu lidí na vánočním trhu v centru Berlína, zabil 2 lidi a zranil 50 dalších.

14. července 2016, Nice: Útok vozidlem během oslav státního svátku si vyžádal 86 obětí.

22. prosince 2014, Nantes: Útok na vánočním trhu si vyžádal dvě oběti a deset zraněných.

WWW.OCHRANAMEKKYCHCILU.EU

KPKB KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČESKÉ REPUBLIKY

OCHRANA MĚKKÝCH CÍLŮ

NOVÝ ZÁKON O KYBERNETICKÉ BEZPEČNOSTI

CO ZNAMENÁ PRO POSKYTOVATELE SLUŽEB KOMERČNÍ BEZPEČNOSTI?

Nový zákon o kybernetické bezpečnosti prošel ve sněmovně druhým čtením a dá se říci, že již klepe na dveře. V posledních měsících nabírá na intenzitě diskuse o tom, na koho vlastně dopadne.

Protože tento zákon transponuje evropskou směrnici NIS 2, která je navíc propojená s další směrnicí – CER (Critical Entities Resilience Directive – o odolnosti subjektů kritické infrastruktury), ovlivní společně činnost mnoha tisíců společností, mezi nimiž je i řada našich členů.

Jaký vliv bude mít tento zákon na členy Komory podniků komerční bezpečnosti, tedy poskytovatele fyzické ostrahy, vzdáleného dohledu, služeb převozu a dalších služeb?

S přijetím nového zákona se může kterýkoli člen Komory ocitnout v postavení dodavatele subjektu kritické infrastruktury nebo dodavatele (resp. významného dodavatele) povinné osoby podle zákona o kybernetické bezpečnosti. To znamená, že naši klienti, pokud budou spadat pod regulaci tohoto zákona, mohou ve smlouvách a zadávacích řízeních vyžadovat splnění specifických bezpečnostních požadavků.

Mezi nejdůležitější požadavky patří implementace technických a organizačních opatření, například v rozsahu definovaném zatím stále platným a rozvíjeným dokumentem Minimální bezpečnostní standard (MBS), který vydává Národní úřad pro kybernetickou a informační bezpečnost.

Vaše společnost tak může být vystavena nárokům na hlubší bezpečnostní školení personálu, auditům ze strany klientů nebo třetích stran, povinnosti implementovat opatření pro ochranu dat a systémů, řízení rizik, povinnosti penetračního testování a mnoha dalším.

Konkurenceschopnost a nové výzvy

Znamená to, že i když vaše společnost nespadá pod povinnou regulaci, neměli byste nová pravidla ignorovat. V praxi se totiž snadno můžete setkat (a někteří jste se již setkali) s tím, že nesplnění kybernetických standardů uzavře firmě dveře k zakázkám.

Již dnes se totiž objevují ve veřejných i soukromých tendrech podmínky na zabezpečení informačních a provozních systémů, které mohou omezit přístup na trh firmám, které nejsou připraveny.

Kybernetická bezpečnost se prostě stává konkurenční nutností. Proč? Co hrozí v případě jejího ignorování?

- **Vyloučení z tendrů** – některé veřejné zakázky vyžadují již dnes certifikace typu ISO 27001 nebo prokázání souladu s MBS.
- **Ztráta důvěry klientů** – subjekty kritické infrastruktury a povinné osoby budou preferovat dodavatele s prokazatelnou kybernetickou odolností.
- **Právní rizika** – ignorování smluvních požadavků na bezpečnost může vést k finančním postihům nebo žalobám.

Jak vám může pomoci Komora?

Komora podniků komerční bezpečnosti České republiky, z.s., si uvědomuje důležitost těchto změn, a proto připravuje workshop, který vám pomůže se v problematice zorientovat a připravit vaše společnosti na nové požadavky.

Na workshopu můžeme podle vašeho zájmu:

- Vysvětlit konkrétní povinnosti spojené s novou legislativou.
- Představit metodiky pro implementaci MBS a dalších norem.
- Nabídnout praktické rady pro přípravu na audity a jednání se zákazníky.

Chceme vědět, jak velký zájem mezi členy Komory o tuto problematiku je. Pokud se chcete workshopu zúčastnit jako posluchači nebo se aktivně zapojit do jeho tvorby, kontaktujte nás na e-mailu **sekretariat@kpkbcr.cz**.

Je načase připravit se a zajistit, aby vaše firma zůstala konkurenceschopná, v souladu s novými právními nebo smluvními požadavky.

PaedDr. Martin Uher

Oblasti opatření podle MBS:

Manažerská část

- Klasifikace a ochrana informací
- Řízení dodavatelů
- Řízení lidských zdrojů
- Řízení změn
- Řízení kontinuity činností
- Audit kybernetické bezpečnosti

Technická část

- Fyzická bezpečnost
- Řízení přístupů (registrace, autentizace, politika hesel)
- Ochrana před škodlivým kódem
- Kybernetické bezpečnostní události a incidenty
- Aplikační bezpečnost
- Kryptografické prostředky (šifrování disků, ukládání hesel)
- Zajištění dostupnosti informací (vysoká dostupnost, zálohování, SPOF)
- Bezpečnost cloudových služeb

OHLÉDNUTÍ ZA TRAGICKOU STŘELBOU NA FF UK

ROZHOVOR S JANEM BURIANEM

Uplynul více než rok od tragické události, která rezonovala celou Českou republikou. Jak vy jste vnímal první dny a týdny po této události?

Nejdřív jsem vnímal obrovský šok v celé společnosti. Málokdo si dovedl takovou událost v naší zemi představit. Slýchali jsme o útocích na školách v zahraničí, ale bylo to pro nás něco vzdáleného, něco, co se u nás nemůže stát. A najednou se to skutečně přihodilo – byla to realita, ne pouhé záběry z televize či na internetu.

Prvotní šok se následně rychle měnil na hledání případných viníků a hledání co nejrychlejších opatření. Často jsme četli rozbory, kdo co udělal, a naopak co kdo neudělal, co se mohlo udělat lépe. Psalo se o tom všude. V technických opatřeních, což je naše parketa, se začalo rychle spekulovat o detekčních rámech, zavírání veřejných budov, zákazech nadrozměrných zavazadel do škol a podobných nesmyslech. Často byla navrhována opatření, která nebylo možno realizovat nejen po finanční stránce, ale ani po stránce faktické či legislativní. Byla to doba, kdy se s nadsázkou 10 milionů hokejových trenérů změnilo během jednoho dne na 10 milionů specialistů na bezpečnost a krizové události. Kdekdo navrhoval kdeco, obvykle to ale byly úplné nesmysly.

A jak to vnímali odborníci jako jste vy?

Samozřejmě i pro nás to byl šok, ale ne tak velký jako pro širokou veřejnost. Útok z prosince 2023 na FF UK nebyl první v České republice. Paralelu vidíme v události z roku 2015 v Uherském Brodu (8 obětí aktivního střelce) a zejména v útoku ve FN Ostrava v roce 2019 (7 obětí aktivního střelce). Nemocnice jsou svým charakterem velmi podobné univerzitám. Jde o otevřené prostředí, kde se může pohybovat veřejnost vcelku bez omezení. Nelze je uzavřít, nelze kontrolovat každého, kdo přichází do budovy. Po útoku v Ostravě jsem viděl, že se mnoho věcí v ochraně měkkých cílů (OMC) v oblasti zdravotnictví posunulo výrazně dopředu. Zvýšila se spolupráce s Policií ČR, MŠMT poskytlo prostředky na školení zaměstnanců, cvičení a další opatření na zvýšení podpory OMC. Věci se posunuly výrazně kupředu a dnes mají nemocnice v této oblasti výrazný náskok. Pro srovnání náš varovný systém pro krizové situace KISS (Krizový Informační a Svolávací Systém) dnes používá více než 70 % velkých fakultních nemocnic. Používá se nejen v kapitole OMC, ale i pro spouštění traumatických plánů či na urgentních příjmech pro svolávání a informování lékařů a dalšího personálu. Pomáhá zachraňovat životy na denní bázi a to nás těší a motivuje k další práci.

Je možné přenést zkušenosti z nemocnic na univerzity?

Popravdě nejdříve jsem si myslel, že to tak skutečně bude. Ale ukázalo se, že akademická půda je trochu něco jiného než relativně centralizované zdravotnictví. Je zde více rozdílných názorů, jak danou situaci řešit, a větší autonomie jednotlivých univerzit. To přináší různorodost, která však ne vždy vede nejlepší a nejrychlejší cestou k cíli. Na druhou stranu vidím, zejména v poslední době, efektivní sdílení informací a zkušeností. Univerzity, které si už nějakou cestou v oblasti bezpečnosti prošly, poskytují informace ostatním, co je a co není efektivní, co se skutečně osvědčilo v praxi, co funguje. Zde vidím výrazný posun k lepšímu.

Co tedy opravdu funguje? Prozradíte nám to?

Samozřejmě, není to nic tajného. Bohužel nikdo z nás nemá okamžité řešení, po kterém tak volala veřejnost. Nic, co by se dalo udělat hned, a my bychom si mohli říct „hurá máme hotovo“. Bezpečnost je dlouhodobým procesem, který se dotýká všech oblastí v dané instituci. Musí se řešit organizační opatření, legislativní rámec, technická opatření a v neposlední řadě edukace, jak zaměstnanců, tak studentů. Nejdále jsou dnes ty univerzity, které s řešením bezpečnosti začaly již před několika lety. Malými krůčky se posouvaly kupředu, zapojovaly do bezpečnosti více personálu, pořizovaly technické prostředky, zapracovávaly legislativní rámec apod. Právě tyto univerzity dnes předávají své know-how ostatním. Co v praxi skutečně funguje, je to, že si stanovíte velké cíle, ale realizujete je po menších krůčcích, abyste do toho cíle reálně došli.

A kde vidíte slabá místa? Co naopak nefunguje?

Vrátím se k tomu, kde se nejčastěji pohybuji, a to jsou technologie. Hodně těžce nesu přístup některých firem, které si po prosinci 2023 uvědomily, že na oblast technologií pro bezpečnost půjde větší množství finančních prostředků než doposud, a ze dne na den předělaly své produkty a marketing na oblast „bezpečnost a OMC“. A to bez jakýchkoli zkušeností a referencí, což má pak výrazný vliv a dopad do praxe. Samozřejmě negativní.

Druhý a možná závažnější problém vidím v rozporu, co dnes moderní technologie umí, a na druhé straně kdo je obsluhuje a jakou má daná osoba odbornost. Pokud bych měl dát příklad, tak třeba kamerové bezpečnostní systémy s podporou AI technologie dnes umí rozpoznávat obličeje, nestandardní chování, držení zbraně a zvládají mnoho dalších, velmi moderních funkcí. Nezřídka se však stává, že k tomuto systému je přidělena obsluha ze strany externí bezpečnostní agentury, která tam, v souladu s kontraktem, dodá minimálně zaškoleného důchodce s minimální mzdou, bez jakýchkoliv IT znalostí. To je praxe, kterou potřebujeme změnit. A i my dodavatelé technologií musíme klást důraz na co nejjednodušší obsluhu, počítat s tím, že ne každý zaměstnanec je příznivec informačních technologií.

Můžeme společně nahlédnout na to, co se děje přímo při nějaké krizové situaci, a jak mohou pomoci technologie?

Pokud se podíváme již přímo na probíhající bezpečnostní incident, tak my řešíme něco, co označujeme jako tzv. DVI (Detekce, Varování a Informování).

Nejdříve musíte probíhající incident detekovat, rozpoznat, že se taková nechtěná věc děje. I v tomto mohou pomoci moderní technologie, jako jsou bezpečnostní kamerové systémy nebo například v poslední době velmi populární zvukové senzory, které dokážou rozpoznat střelbu, křik, rozbití skla a mnoho dalších událostí. Vedle technologií je ovšem stále nejčastějším „detektorem“ sám člověk. Osoba, která vidí či slyší, co se v místě děje.

Po „detekci“ následuje „varování“. Jedná se o co nejrychlejší předání informace osobám v nejbližším okolí daného incidentu, například v dané budově. Přesnost a rychlost doručení této informace je prioritou, která může pomoci minimalizovat škody na životech či majetku. Je třeba si uvědomit, že prvosledové hlídky a další složky IZS dorazí na místo incidentu v průměru za 10–15 minut od zahájení incidentu. Samozřejmě záleží na konkrétní lokalitě a daném městě. Ale ty první minuty jsou dobou, kdy se musíte ochránit sami, a měli byste vědět, jak se zachovat, o jaký typ incidentu se jedná. Máme provést evakuaci z budovy, nebo se naopak zabarikádovat? Přesně k tomuto rozhodnutí potřebujete být co nejrychleji a nejpřesněji informován o typu incidentu. To je parketa a úloha pro náš varovný systém KISS, který přenáší desítkám, stovkám, ba i tisícům osob v blízkosti incidentu konkrétní varování, a to různými komunikačními kanály (může volat, posílat SMS, odesílat sdělení na WhatsApp, na obrazovky v budově nebo do interního systému; dokáže komunikovat v různých jazycích).

Následné „informování“ slouží pro doplňování a distribuci průběžných informací o daném incidentu. Reálné události přinesly často stížnosti osob z blízkého okolí, že nevěděly, co se děje, jaká je povaha nebezpečí, zda už incident skončil apod. To se snažíme eliminovat průběžným doplňováním informací už v průběhu události i těsně po ní.

Říkal jste, že máme vědět, jak se zachovat pro danou konkrétní krizovou situaci. Vědí to i studenti a zaměstnanci univerzit?

Teoreticky to složité není. Používá se lety osvědčené pravidlo USB – Uteč, Schovej se, Bojuj. Tedy pokud můžeš, co nejrychleji uteč z místa incidentu. Pokud to není možné, tak se schovej nebo se zabarikáduj. A až poslední a nechtěnou volbou je bojuj s útočníkem. Zažil jsem případy, kdy do škol přišli rádoby experti a chtěli zaměstnance učit Krav Magu, jako přípravu na aktivního útočníka. Já sám jsem příznivcem bojových umění, ale daleko praktičtější je naučit dané osoby, kde jsou únikové cesty, kudy jinudy utéct, když to nepůjde po hlavní únikové cestě. Nebo jak se správně zabarikádovat ve třídě, jaké k tomu můžete použít pomůcky a jaká jsou pravidla pro odbarikádování. Tyto dovednosti je třeba se učit, a hlavně pak pravidelně trénovat.

Trénování a cvičení si mnozí z nás ještě pamatují z dob totality a nebyla to zrovna populární aktivita. Jak je to vnímáno dnes?

No možná to tenkrát nebyla populární aktivita, a i proto se od toho po revoluci do jisté míry upustilo. Nyní je však čas návratu. Bezpečnost kolem nás se bohužel zhoršuje. Válka v Evropě, klimatické změny, utečenecké vlny, negativní sociální sítě a mnoho dalších aspektů nám nedávají mnoho naděje, že se bezpečnostní situace u nás bude zlepšovat. Měli bychom na to být připraveni. Jak se říká, kdo je připraven, není překvapen. Cvičení navržených opatření je extrémně důležitá záležitost. Testujete a cvičíte nejen lidi, ale dokonce i samotné technologie.

Paradoxem je, že nejlépe při cvičeních na univerzitách fungují zahraniční studenti. Ti mají často návyky a disciplínu, kterou si nesou již ze základních a středních škol v zahraničí, kde jsou podobné věci běžné. Já pevně věřím, že i my v ČR začneme vnímat, že to děláme pro sebe a pro ochranu našich dětí, nejen jako povinnost, kterou nám někdo nařídil.

Redakce BsP
a Jan Burian
CEO společnosti
SAFE Technology SAFETE

Foto: Milan Maliček, Novinky

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČESKÉ REPUBLIKY

HISTORIE A SOUČASNOST KONSTRUKCE A POUŽÍVÁNÍ PASIVNÍCH A POLOPASIVNÍCH SYSTÉMŮ PROSTOROVÉHO ODPOSLECHU

1. ČÁST

Tento příspěvek je prvním z chystané série článků pojednávajících o technických prostředcích využívajících technické kanály k získávání důvěrných informací. Jde o problematiku značně rozsáhlou, tedy i tento první článek rozdělím do dvou částí.

Pojednává o jednom z několika druhů prostorového odposlechu rozhovorů. Jedná se o způsob, při kterém jsou nasazeny odposlechové přístroje označované v anglosaské literatuře jako Acoustic Reconnaissance Radar System (ARRS), tedy akustický průzkumný radarový systém. V ruskojazyčné literatuře se obvykle označuje jako Radiolokační systém akustické rozvědky (RLSAR).

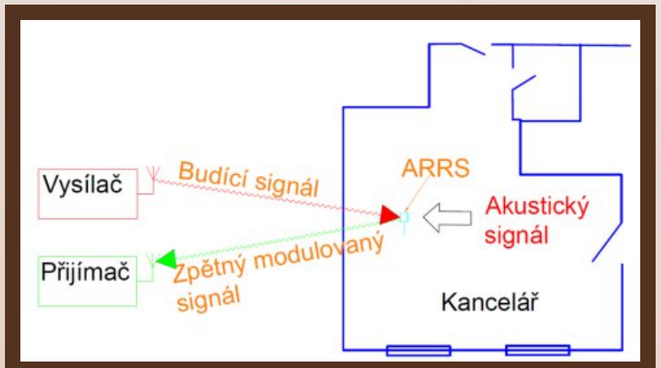
Jde o zařízení ovládaná vnějším vysílaným signálem (budící signál), která zpětně přenášejí akustickou informaci po radiovém kanálu. V případě nepřítomnosti budícího signálu je zařízení z hlediska odposlechu nefunkční, a není tudíž detekovatelné klasickými obrannými radiovými vyhledávacími metodami. Na obrázku 1 je principálně znázorněno použití prostředků ARRS.

Účelem prostorového odposlechu, podobně jako telefonního, resp. telekomunikačního, je získávání informací. Zařízení k tomu používaná se v odborné praxi zpravodajských služeb a policie nazývají již mnoho desítek let jako operativně technické prostředky (OTP), zpravodajsko technické prostředky (ZTP), operativní prostředky (OP) nebo jen prostorový odposlech. V běžné hantýrce též štěnice. Přestože označení „zpravodajsko technický prostředek" zahrnuje širší škálu speciální techniky, přidržím se v dalším textu označení ZTP.

Bohužel oblast zpravodajské techniky, která byla u nás čistě doménou orgánů zpravodajských služeb a policie, se po roce 1989 po vzoru západních zemí komercializovala a začala být nelegálně využívána v byznysu, politice apod. Článek se ovšem nezabývá právními aspekty legálního nebo nelegálního používání této techniky, ale pouze technickými aspekty v kontextu s historií, a to jen u jednoho druhu této techniky.

Na základě konstrukčního a obvodového řešení bych tyto přístroje osobně rozdělil na tři skupiny:

- pasivní (dále PAS), který je charakterizován čistě mechanickou konstrukcí;
- pasivní s elektronickými součástkami, ale bez napájecí baterie (dále PASE);
- polopasivní (používá se také název poloaktivní), který má na rozdíl od PASE i napájecí zdroj–baterii (dále PPASE).



Obr. 1, Princip používání prostředků ARRS k prostorovému odposlechu.[1]

Skupina ZTP PAS je charakterizována tím, že ke konstrukci zařízení nebyla použita žádná průmyslově vyrobená elektronická součástka (tranzistor, dioda, vypínač, kondenzátor, odpor atd.) a neobsahuje žádnou baterii coby napájecí zdroj. V technické komunitě se používá též označení „endovibrátory".

Základem konstrukce PAS je bezesporu revoluční vynález geniálního ruského inženýra L. S. Termena. Ten učinil svým revolučním objevem krok, kterým doslova změnil dějiny jedné oblasti zpravodajské techniky. Vynalezl endovibrátor coby pasivní odposlechový prostředek. Od té doby je z pohledu odposlechu možno skrýt do nějakého kancelářského předmětu nebo stavebního prvku v zájmovém místě nenápadnou, čistě mechanickou konstrukci a radiově vysílanou vlnou ji zvenčí (mimo objekt kde je ZTP nasazen), například i skrze zeď, aktivovat.

Z pohledu historie představuje tato skupina ZTP z hlediska přínosu pro zpravodajské služby skupinu velmi významnou, možná nejvýznamnější. Dopad touto cestou získaných informací na mezinárodní a politickou scénu své doby byl v mnoha ohledech zásadní.

Historie používání těchto systémů ve zpravodajských službách začala již po skončení 2. světové války a jako první na světě jej použila zpravodajská služba bývalého SSSR. Podle některých pramenů spadají počátky nasazení těchto pasivních ZTP do období již před rokem 1945.

Veřejně nejznámějším případem, který byl poprvé publikován počátkem 50. let (1952), je jeho nasazení sovětskou zpravodajskou službou k odposlechu kanceláře amerického velvyslance v Moskvě v srpnu 1945. Endovibrátor byl zabudován dovnitř emblému, který visel v moskevské kanceláři amerického velvyslance. Tento emblém předali 4. srpna 1945 sovětští Mladí pionýři W. Averellovi Harrimanovi, velvyslanci USA v Sovětském svazu, na výraz přátelství. Poté, co emblém prošel rutinní rentgenovou kontrolou, byl zavěšen za Harrimanův stůl v jeho kanceláři ve Spasově domě na Spasopeskovském náměstí č. 10 v Moskvě (oficiální rezidence velvyslanců USA v Sovětském svazu od roku 1934).

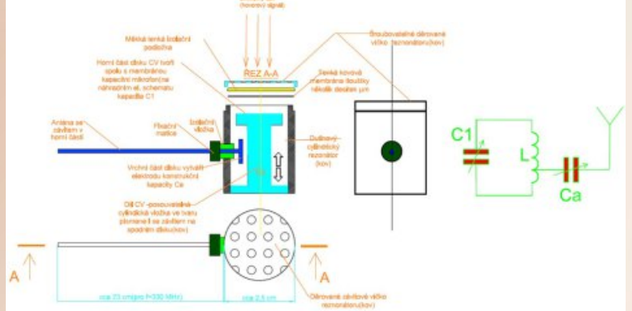
Po sedmi letech Američané endovibrátor odhalili a podrobili reverznímu inženýrství. Poměrně dlouhou dobu jim trvalo, než odhalili princip jeho fungování. Vyrobili jeho kopie, které jsou fyzicky vystaveny v Národním muzeu kryptologie (obr. 2), založeném americkou National Security Agency (NSA), spadající pod americké ministerstvo obrany. NSA je velmi významnou součástí zpravodajské komunity (Intelligence Community) jako nezávislá zpravodajská agentura, která se zabývá elektronickou rozvědkou (radioelektronickou nevyjímaje) a je zodpovědná za elektronické zpravodajství a obranu elektronických komunikací a sítí vlády USA.

O tom, že NSA má ve svém arzenálu tyto prostředky, se veřejnost dozvěděla po jejich odhalení, jež bylo učiněno Edwardem Snowdenem. Katalog ZTP, které jsou používány NSA, byl zařazen do série dokumentů, jež Edward Snowden zveřejnil v prosinci 2013 (Pokročilé síťové technologie – katalog ANT_NSA 3 – utajovaný dokument obsahující seznam ZTP, jež používá NSA). Jedná se o ZTP ze skupiny PPASE v již pokročilejších verzích, jak bude uvedeno dále.

Obr. 2, Fotografie kopií sovětského kamuflu endovibrátoru vyrobená v USA a vystavená v muzeu NSA. [2]

Technické dokumenty související s reverzním inženýrstvím endovibrátoru SSSR byly odtajněny v USA až v roce 2013, tedy po Snowdenově odhalení.

Stojí za zmínku, že existuje několik zajímavých skutečností spojených s tímto tématem, a pokud bude příležitost, pokusím se o nich napsat obšírněji. Z různých zdrojů lze načerpat konstrukční informace o endovibrátoru a na jejich základě vytvořit orientační nákres (obr. 3).



Obr. 3, Orientační nákres endovibrátoru a jeho náhradní elektrické schéma. [4]

Teoretický rozbor fungování endovibrátoru přesahuje rámec tohoto příspěvku. Pro alespoň jednoduché přiblížení lze konstatovat, že základem jeho fungování je modulace odraženého radiového (budícího) signálu akustickým signálem. Jedná se o cylindrický dutinový rezonátor, ve kterém přivedením energie budící elektromagnetické vlny vzniknou vysokofrekvenční rezonanční kmity. Na tenkou kovovou membránu působí akustický tlak z prostoru a vyvolává její pohyb v rytmu akustických kmitů. Ta tak funguje podobně jako kondenzátorový mikrofon a způsobuje změnu kapacity C1. To vyvolává změnu parametrů rezonančního systému a změnu odrazných vlastností antény, což vede k modulaci odraženého radiového signálu.

Z praktického hlediska jsou pro možnost srozumitelného poslechu akustické informace z endovibrátoru důležité dvě jeho vlastnosti:

- dobrá odrazivost pro budící signál;
- velikost změny rezonanční frekvence nebo činitele jakosti Q rezonátoru vyvolaná změnou ak. signálu.

Hlavní výhodou PAS je již zmíněná absence radioelektronických součástek a napájecích prvků. To umožňuje jejich výrobu jako suvenýrů, interiérových předmětů a podobně. Zároveň tento fakt ztěžuje možnost odhalení. Rovněž mohou být speciálně zvoleny geometrické rozměry prvků stavebních konstrukcí, tak aby posloužily ke vzniku endovibračního efektu. Další hlavní výhodou je naprostá anonymita subjektu, který získává hovorové informace, což zejména v komercializaci provádění těchto úkonů může hrát v současné době velkou roli.

Omezující vlastností PAS byly nízké hodnoty změny rezonanční frekvence nebo činitele jakosti Q rezonátoru. Tím byl omezován modulační koeficient odraženého signálu. Pro zajištění potřebné vzdálenosti mezi PAS a přijímačem, tak aby byla zachycená akustická informace srozumitelná, to následně vyvolávalo potřebu poměrně značně vysokého budícího výkonu. Další omezující vlastností PAS byl dále fakt plynoucí z fyzikální podstaty jevu, a sice to, že hlasovým signálem vzniklá modulace zpětně emitovaného signálu je prostou amplitudovou, eventuálně fázovou. To byly dvě hlavní vlastnosti, na které se soustředilo úsilí dalšího vývoje v této oblasti, protože představovaly hlavní demaskující vlastnosti tohoto typu ZTP při jejich nasazení. Poměrně vysoký výkon budícího signálu (desítky až stovky wattů) usnadňoval jeho zjištění a lokalizaci, zejména při nízkém obsazení radiového UHF pásma, na kterém probíhal provoz zařízení. Rovněž prostá amplitudová modulace zpětně emitovaného signálu mohla být relativně snadno zachycena i náhodným posluchačem.

Od poloviny 50. let 20. století se proto zpravodajské služby hlavních světových mocností zaměřily na vylepšování pasivních endovibračních radarů PAS. Když po odhalení jejich funkce (veřejně v roce 1952 USA) vymizel efekt překvapení, pracovalo se na jejich dalším rozvoji v utajení. Ten směřoval k odstraňování jejich hlavních slabin, jimiž byly:

1. nutnost vysokého výkonu budícího vysílače pro dosažení prakticky použitelné vzdálenosti v podmínkách reálného operativního nasazení;

2. prostá amplitudová modulace (AM) nosné frekvence zpětně emitovaného hlasového signálu.

V rámci zdokonalování vlastností zařadili vývojáři k PAS konvenční mikrofon, za nímž v obvodovém řetězci následoval nízkofrekvenční zesilovač a modulátor. Vznikla tak skupina ZTP označená v úvodu jako PASE. Tyto obvody bylo třeba napájet, k čemuž se využívala část energie vnějšího budícího signálu. Změnila se i konstrukce PAS části. Toto technické řešení umožnilo podstatně snížit výkon budícího signálu díky zvýšení modulačního indexu, a tím výrazně zvýšit dosah (vzdálenost ARRS–přijímač) jejich použití. Je dobré si připomenout, že v době do 70. let minulého století byla radiová pásma UHF (300 MHz–3 GHz) v civilním, průmyslovém a mediál-

ním využití ve srovnání s dnešní dobou jen poměrně řídce obsazena. Takže na rozdíl od současnosti bylo poměrně obtížné „schovat" se s provozem na těchto pásmech. Obsazenost radiových pásem se radikálně změnila zejména v posledních 20 letech.

Zařazení modulátoru umožnilo řešení i druhého slabého místa. Signály s prostou amplitudovou (AM), fázovou (PM) a frekvenční modulací (FM) byly dobře odhalitelné již tehdy existujícími měřicími a přijímacími přístroji, nehledě na speciálně vyráběné přijímače pro radiorozvědku. Pro vyřešení tohoto problému se postupně začaly zavádět různé maskovací techniky zpětně odraženého signálu. Maskování signálu obecně je technika, která se u profesionálních ZTP používala a používá pro skrytí obsahu zachyceného zvuku před náhodným nebo profesionálním posluchačem. Způsobuje, že pokud se běžným přijímačem naladíte na vysílaný signál, není možno slyšet jeho obsah.

Maskování se používá i dnes, např. u sériově vyráběných radiostanic za tím samým účelem. V některých případech se používají utajené modulační techniky, které překonají jakýkoli nekompatibilní odposlechový přijímač (pozn.: maskování není kryptování signálu, i když se tyto pojmy často nerozlišují). První aplikovanou technikou maskování bylo použití subnosných frekvencí a FM modulace. Postupně, s rozvojem modulačních technik, se začalo využívat pulsně polohové modulace (PPM), což spolu s vývojem digitalizace signálu umožňovalo další zdokonalování maskovacích technik s pozdějším následným přechodem ke kryptování přenášeného signálu.

Maskování však vyvolávalo nutnost použití dalších radioelektronických součástek, neboť se realizuje dalšími elektronickými obvody, které je nutno do pasivního prvku ARRS zabudovat. To na druhé straně zvyšuje možnosti jejich odhalení, například pomocí detektorů nelineárních přechodů.

Po určitou dobu se systémy PASE aktivně používaly, ale nejen Američané a Rusové si uvědomovali, že se tím nepodařilo zcela odstranit dvě hlavní, výše zmíněné demaskující vlastnosti ARRS.

Příkladem skupiny PASE může být řada těchto odposlechových prostředků, které si nechala CIA vyvíjet u holandské společnosti NRP (Nederlands Radar Proefstation). CIA navázala spolupráci s touto malou nizozemskou společností po odhalení sovětského endovibrátoru. To bylo a je plně v duchu politiky CIA – navazovat kontrakty pro speciální technické prostředky s malými společnostmi z důvodu možnosti lepšího utajení. Společnost NRP byla založena v roce 1947, tedy době, kdy skupina mladých, profesně nadaných inženýrů experimentovala s radiolokací 5. CIA oslovila společnost v roce 1952, záhy po zveřejnění odhalení nálezu sovětského endovibrátoru. NRP započala na základě kontraktu práci na vývoji projektu, který nesl označení Easy Chair (EC). Vztahy mezi CIA a NRP trvaly až do jejího administrativního zániku v roce 1994. V roce 1967 vznikla Laboratoř Christiana Huygense (CHL), která se v roce 1993 sloučila s NRP a pokračuje v činnosti pod názvem CHL Netherlands BV.

Prvním výsledkem spolupráce NRP s CIA bylo dodání zařízení označovaných jako EC1 pro CIA, a to v roce 1956. V dalším roce (1957) pak byla dokončena další verze pod označením EC MK 2 a o rok později (1958) verze EC MK 3. Tato verze již používala maskování pomocí subnosné frekvence a místo napájecího zdroje využívala k napájení část energie budícího vysílače.

Samotná vlastní odposlouchávací část se u EC1 skládala ze dvou dílů:

- anténní díl, který obsahoval diodu a dvě indukčnosti;
- díl se zesilovačem a mikrofonem, který se připojoval na anténní díl pájením nebo tenkou dvoulinkou na něco jako malou svorkovnici; délka připojovací dvoulinky mohla být i 10 m.

Další zařízení z řady EC měla již druhý díl zaintegrovaný do anténního dílu.

Ing. Karel Hříbal, Csc.

Obr. 4, Vysokofrekvenční část ZTP EC1. [6]

Obr. 5, Kompletní sestava ZTP EC1. [7]

Zdroje a poznámky:

1) Nákres autora článku.

2) HTTPS://EN.WIKIPEDIA.ORG/WIKI/THE_THING_(LISTENING_DEVICE)#/MEDIA/FILE:BUGGED-GREAT-SEAL-OPEN.JPG; HTTPS://COMMONS.WIKIMEDIA.ORG/WIKI/FILE:NSA_GREAT_SEAL_BUG.JPG.

3) NSA ANT CATALOG. HTTPS://WWW.EFF.ORG/FILES/2014/ 01/06/20131230-APPELBAUM-NSA_ANT_CATALOG.PDF.

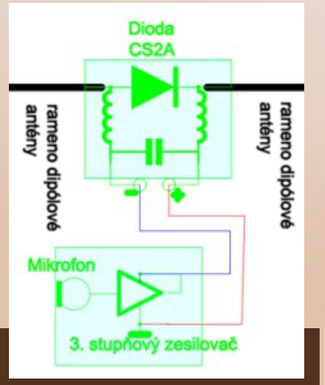
4) Nákres autora článku.

5) HTTPS://INTELNEWS.ORG/TAG/NEDERLANDS-RADAR-PROEFSTATION/ ; https://thecorrespondent.com/3789/Operation-Easy-Chair-or-how-a-little-company-in-Holland-helped-the-CIA-bug-the-Russians/116534484-2a3d7f11.

6) https://www.cryptomuseum.com/covert/bugs/ec/ec1/img/302546/019/full.jpg.

7) Výchozí obrázek – https://www.cryptomuseum.com/covert/bugs/ec/ec1/img/ec1_-pe.png, úprava a překlad popisů, vlastní nákres.

8) Nákres autora článku.



Obr. 6, Nejjednodušší variantu EC1 lze znázornit takto - orientační elektrické schéma ZTP EC1. [8]

Dioda CS2A plní funkci usměrnění. Signál z budícího vysílače je usměrněn, čímž vznikne napájecí napětí pro nf zesilovač. Signál z nf zesilovače ovlivňuje parametry antény a dochází k již zmíněné amplitudové modulaci zpětně emitovaného budícího signálu. Vzdálenost budícího vysílače a přijímače se pohybovala od 50 do 100 m, v závislosti na překážkách vyskytujících se v signálových cestách. Toto technické řešení umožnilo podstatně snížit výkon budícího signálu díky zvýšení modulačního indexu.

SPECIFIKA ZAJIŠŤOVÁNÍ MÍSTNÍCH ZÁLEŽITOSTÍ VEŘEJNÉHO POŘÁDKU V KONTEXTU

LETNÍCH OLYMPIJSKÝCH HER 2024

Předkládaný text přibližuje Letní olympijské hry 2024 (oficiálně Hry XXXIII. olympiády) v Paříži jako výrazný impulz k bezpečnostním úvahám a aktivitám, při vědomí obav z možného závažného narušení jejich průběhu.

Prudký vývoj bezpečnostních technologií, které byly v rámci Paříže přinejmenším dočasně využívány, byl jedněmi vnímán jako pozitivní trend, kdežto u dalších osob vzbuzoval vážné obavy.

Paříž a olympijské hry

Paříž hostila v roce 2024 olympijské hry sto let po obdobné akci pořádané roku 1924. Současné hry se konaly po překonání pandemie a na pozadí války na Ukrajině. V paměti Pařížanů ožívaly vzpomínky na islamisticky motivované incidenty poslední doby (Charlie Hebdo a Bataclan). Zapomenout nebylo možno ani na střety s policejními silami v Nanterre u Paříže 29. června 2023 a útok davu na radnici a dům starosty v L'Haÿ-les-Roses, kdy dav zhruba osmdesáti výtržníků nakonec dokázalo jen s vypětím všech sil zpacifikovat sedm městských strážníků. Není tedy divu, že v kontextu akce vyvstávaly obavy ohledně bezpečnosti a nepokojů.

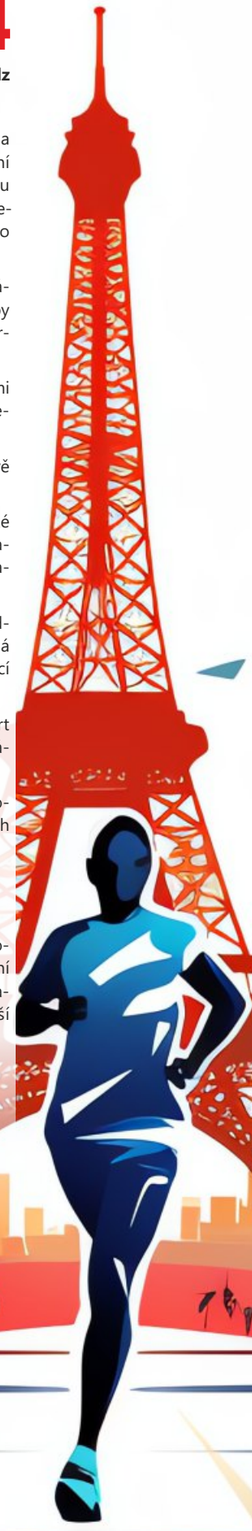
Na akci bylo prodáno okolo 10 milionů vstupenek, očekávala se účast 10 500 sportovců, a to během 18 dní soutěží. Vedení města i státu vnímalo olympiádu jako příležitost k uzdravení. Kladlo si za cíl ohromit publikum, počínaje nebývalým zahajovacím ceremoniálem 26. července 2024 pro více než půl milionu diváků. Sociální, etnické a politické tlaky však obraz sebevědomé Francie, který chtěli organizátoři her prezentovat, podkopávaly.

Důvody k obavám z možného bezpečnostního narušení akce byly zejména následující:

- Možnost islamisticky motivovaného teroristického útoku nebo výhrůžek takovým útokem.
- Teroristický útok v Krasnogorsku, který proběhl 22. března 2024, tedy pouhé čtyři měsíce před zahájením olympijských her – francouzská vláda po něm zvýšila stupeň bezpečnostního plánu Vigipirate na nejvyšší úroveň.
- Chaotické finále Ligy mistrů mezi Liverpoolem a Realem Madrid v Paříži v roce 2022, kdy se před stadionem nedařilo regulovat tisíce neukázněných fanoušků obou týmů a policejní složky nebyly schopny účinně a nekonfliktně zasáhnout (došlo k použití slzného plynu) – vzpomínka na tuto událost ve francouzské společnosti dosud nevyprchala.
- Kybernetické incidenty ve vztahu k akci – jejich počet se předpokládal desetinásobně větší než při Letních olympijských hrách v Tokiu 2021. Pro připomenutí: při Zimních olympijských hrách v Pchjongčchangu 2018 byl použit počítačový virus nazvaný „Olympic Destroyer".
- Předpokládaná vysoká koncentrace osob, jejichž přímým zájmem nemusela být vždy jen účast na jednotlivých sportovních utkáních, ale celou událost pojímaly jako důvod k oslavám.
- Eventualita nezvládnutého davového chování, například v případě poplašné zprávy. Některé akce se konaly často přímo ve městě, v blízkosti ikonických turistických atrakcí, nikoli na specializovaných sportovištích.
- Možné incidenty ohledně přítomnosti sportovců z Ruské federace a Běloruska či střety se sportovci s Ukrajiny, respektive šířeji pojaté incidenty mezi podporovateli a odpůrci Ruské federace (a její války na Ukrajině) – viz například ubodání sportovců z Ukrajiny v Německu v únoru 2024. V prostředí Ruské federace byla akce ostatně označena jako „festival rusofobie".
- Možné sociální nepokoje – olympiádu se mohly pokusit využít osoby protestující proti důchodové reformě ve Francii.
- Možné střety veřejnosti s policejními složkami v Paříži nebo v obcích v jejím okolí (obyvatelstvo suburbií).
- Možnost stávky ve veřejné dopravě v aglomeraci.
- Eventualita zhoršení pandemické situace v době her (ať již by se jednalo o koronavirus či jinou vysoce nakažlivou chorobu).
- Dopad akce na prodej drog a nabídku prostituce v aglomeraci (zvýšená nabídka i poptávka a vlna související kriminality).
- Dopady vysokých teplot na komfort a zdraví účastníků – sportovců i diváků.
- Znepokojivé vyšetřování protikorupční policie ohledně některých souvisejících veřejných zakázek.

Očekávání a obavy

Paříž sama sebe definovala jako testovací polygon pro nový model pořádání olympijských her. Hry byly přímo označeny za inkluzivnější, ekologičtější



a v neposlední řadě i lacinější, než bývá zvykem (včetně využívání stávajících nebo dočasných sportovišť namísto budování nových). Avizované náklady se uváděly ve výši okolo 8,8 miliardy eur, což bylo asi o 40 % méně, než kolik stály hry v Tokiu v roce 2021. Hry se doslova snažily lépe přizpůsobit svému místu konání, nikoli naopak. Jediná sportoviště, která byla nově postavena, byla centrum vodních sportů a lezecké stěny. Obojí se nachází na severovýchodních předměstích, kde sportoviště celkově chyběla (po skončení her byla zařízení předána místním organizacím pro práci s mládeží).

Policejně-bezpečnostní síly v této souvislosti avizovaly určité silné stránky nebo zaváděná či připravovaná opatření ke zvládnutí situace:

Rok 2023 – například akce okolo státního svátku v červenci, mistrovství světa v ragby v září a říjnu, akce spojené s Vánocemi a oslavami konce roku – to vše byly svého druhu generální zkoušky na bezpečnostní zajištění olympiády. Policejně bezpečnostní síly v této zkoušce obstály (zejména s ohledem na řízení davů a boj proti delikvenci).

Vláda, předseda organizačního výboru her v Paříži 2024 a starostka Paříže podepsali bezpečnostní protokol, obsahující detaily plánování akce s ohledem na bezpečnost (obavy z terorismu, útoky dronů s výbušninami a další rizika pro davy).

Celkem bylo v období olympiády v Paříži denně k dispozici 30 000 až 45 000 příslušníků policejně bezpečnostních sil, tedy pěti- až desetinásobek běžného stavu (pro srovnání: londýnská korunovace Karla III. představovala angažmá pro zhruba 13 000 policistů). Počítalo se i s využitím personálu soukromých bezpečnostních služeb.

Vstupenky, a to i na akce, které byly zdarma, byly navázány na registraci na jméno. I to mělo pravděpodobnost bezpečnostních incidentů omezit.

V březnu 2023 schválil francouzský parlament pro dohled nad olympiádou zavedení kamerového dohledu s využitím umělé inteligence. Francie tak byla rychlejší než celounijní procesy hledání právního rámce ve vztahu k umělé inteligenci. Nasazení nejmodernějších technologií může zachraňovat lidské životy. Související obavy bylo však třeba vnímat jako důvodné a silné, při vědomí obav z narušení základních lidských práv a svobod.

Další obavy, že by sběr dat získaných kamerami byl svěřen soukromé společnosti, byly bezpředmětné – stejně jako názor, že policejní drony ponesou zbraně pro střelbu do davu.

Kamery umístěné v ulicích či na dronech v reálném čase sledovaly dění. Nové technologie využívaly software k analýze snímků zachycených kamerami v reálném čase. Umělá inteligence dokáže velmi rychle (v reálném čase) identifikovat opuštěné zavazadlo, podezřelé vozidlo, oheň, hluk, nebo prudkou změnu v chování davu. Počty těchto kamer v aglomeraci byly navýšeny o „několik stovek". Další zařízení tohoto typu byla mobilní, včetně zařízení umístěných na dronech.

Kritika postupu a opatření

Kritika souvisejících opatření byla založena například na následujících výhradách:

- Boj s drogami, bezdomovectvím, nelegálními trhovci, prostitucí a kriminalitou obecně spočíval pouze v dočasném vytlačení souvisejících osob (dealerů, narkomanů atd.) z nejvíce viditelných míst (sportovní areál Porte de la Chapelle, náměstí Forceval, břehy Seiny, veřejné parky a další). Dokonce i některá již existující zavedená zařízení pro narkomany, provozovaná asociacemi Gaïa-Paris a Aurore, byla přemístěna na okraj metropole.
- Represe zcela dominovala nad prevencí.
- O nějakém komplexním sociálně-zdravotním programu nemohla být v této oblasti řeč.
- Velice riskantní byly ceremoniály a sportovní akce na hladině Seiny, která byla pro tento účel po mnoha letech vyčištěna. V případě úspěchu to měly být dechberoucí scenérie – ale v případě jakéhokoli problému mohlo snadno dojít k tragédii, která by celé hry znevěrohodnila.
- Řada nasazených policistů a dalšího bezpečnostního personálu byla stažena z celé země – šlo tedy o osoby bez místní znalosti.
- Koncentrace policejně-bezpečnostních aktivit na dobu olympiády znamenala, že dovolené a přesčasy bezpečnostního personálu budou muset být vybírány ve zbytku roku, v důsledku čehož mohou bezpečnostní standardy po akci v Paříži i jinde ve Francii skokově poklesnout.
- Odhodlaného útočníka – jakým byl například vjezd nákladního automobilu do osob na promenádě v roce 2016 v Nice – je tak jako tak nesnadné zastavit.
- Nasazené technologie nebyly schopny rozeznávat obličeje zájmových osob (absence této funkce byla některými mluvčími vnímána jako pozitivum).
- Některé kamery byly naopak schopny vyhodnocovat algoritmus chůze konkrétní osoby, což bylo některými kritiky vnímáno jako potenciálně zneužitelné.

Kritici tak olympiádu v Paříži vnímali spíše jako předehru či laboratoř budování „policejního státu" v evropském/unijním měřítku – jako něco, čeho se bude po skončení akce „škoda zbavovat". Související právní rámec byl koneckonců v platnosti „do konce roku 2024".

Stěžejní bezpečnostní proměnné

Stěžejní aktuální bezpečnostní výzvy, které s fungováním pařížské aglomerace souvisely, ale i nadále souvisí, lze nejenom s ohledem na olympijské hry identifikovat následujícím způsobem:

• Řízení davů a dopravy

S očekávaným nárůstem pohybu osob ve městě je třeba řídit davové situace a dopravní toky. To zahrnuje plánování a implementaci účinných opatření pro zajištění plynulosti dopravy a minimalizaci mimořádných událostí.

• Prevence terorismu

Akce, během kterých dochází k velké koncentraci osob (mezi něž patří i olympijské hry) představují obecně potenciální cíl pro teroristické útoky a jiné kriminální aktivity. Všechny zainteresované bezpečnostní složky v této souvislosti musí provádět rozsáhlá preventivní bezpečnostní opatření.

• Prevence kriminality a ochrana veřejného pořádku

V případě velkého množství návštěvníků a mnoha akcí spojených s olympijskými hrami je nutno zajistit dodržování veřejného pořádku a řešit případné incidenty či konflikty v městském prostředí.

• Bezpečnostní hrozby spojené s technologiemi

S rozvojem technologií a digitalizace může aglomerace čelit novým bezpečnostním hrozbám, jako jsou kybernetické útoky nebo zneužití informačních technologií ke kriminálním účelům. Zajištění kybernetické bezpečnosti je proto klíčovou prioritou.

Ve vztahu k uvedeným eventualitám bylo, je a bude třeba připravit adekvátní plány a strategie a investovat do příslušných technologií a vybavení.

Kudy dál?

Odborná nadstavba pro bezpečnostní zajištění pařížských olympijských her zahrnovala několik klíčových oblastí a technologií, které pomohly zlepšit účinnost bezpečnostních opatření. V této souvislosti stojí za úvahu shrnout oblasti, které budou i v budoucnu vyžadovat při řízení akcí za účasti velkého množství osob náležitou pozornost:

• Zapojení technologických inovací

Využití nových technologií, jako jsou umělá inteligence a strojové učení, může přispět k posílení bezpečnosti jako celku.

• Analýza dat a prediktivní modelování

Využití pokročilých analýz dat a prediktivního modelování umožňuje identifikovat potenciální hrozby a předvídat možné bezpečnostní události. Může se jednat o použití sofistikovaných algoritmů na analýzu dat z různých zdrojů (včetně sociálních médií, veřejných záznamů a dalších zdrojů) pro identifikaci a predikci rizikových situací. Tímto způsobem mohou být zdroje lépe přiděleny a rozhodnutí přijímána rychleji.

• Řízení informací a komunikace

Integrované systémy řízení informací a komunikace umožňují městské policii efektivně sdílet informace mezi jednotlivými bezpečnostními složkami a dalšími organizacemi zapojenými do zajištění olympijských her. To zlepšuje koordinaci a rychlou reakci na události.

• Biometrická identifikace

Systémy biometrické identifikace, jako jsou rozpoznávání obličeje nebo otisků prstů, mohou pomoci identifikovat podezřelé osoby a monitorovat pohyb lidí během olympijských her. Tímto způsobem lze zvýšit bezpečnost na klíčových místech a v prostorách konání událostí.

• Monitorování veřejného prostoru

Použití pokročilých systémů videonahrávání a analýzy videa umožňuje monitorovat veřejné prostory a identifikovat potenciálně podezřelé aktivity. To poskytuje policejním složkám cenné informace pro prevenci a řešení bezpečnostních incidentů.

• Robotika a drony

Využití robotických systémů a dronů může pomoci provádět průzkum a monitorování oblastí s omezeným přístupem. Tím se zvyšuje schopnost reagovat na mimořádné události a poskytovat pomoc tam, kde je to potřeba.

• Systémy podpory rychlé reakce a koordinace

Vytvoření efektivního systému pro rychlou reakci na bezpečnostní incidenty, který zahrnuje koordinaci mezi národní policií, městskou policií, hasiči, záchrannými službami a dalšími relevantními organizacemi.

• Vzdělávání a osvěta ve vztahu k veřejnosti

Jádrem úsilí je propagace osvědčených postupů pro informování veřejnosti o možných rizicích a opatřeních, která mohou přijmout.

doc. Mgr. Oldřich KRULÍK, Ph.D.
Katedra bezpečnostního managementu,
Vysoká škola AMBIS, Praha,
odbor centrální analytiky Úřadu služby kriminální policie a vyšetřování Policie ČR

PhDr. Milan POLÍVKA
Katedra bezpečnostního managementu,
Vysoká škola AMBIS, Praha,
bezpečnostní odbor Ministerstva vnitra ČR

Mgr. Petr KLÍMA, MPA
Katedra bezpečnostního managementu,
Vysoká škola AMBIS, Praha,
odbor prevence kriminality Ministerstva vnitra ČR

SPOLEČENSKÁ ODPOVĚDNOST A ETICKÉ KONCEPCE UPLATNITELNÉ V PROSTŘEDÍ MALÝCH A STŘEDNÍCH FIREM V KONTEXTU VLIVŮ A DOPADŮ PANDEMIE COVID-19

Ve svém odborném článku, i s ohledem na svoji manažerskou praxi, se chci zaměřit na důležitou a stále aktuální problematiku společenské odpovědnosti a etických koncepcí v prostředí malých i středních firem. Vzhledem k rozsahu zpracované problematiky jsem článek rozdělil na tři na sebe navazující části, další dvě budou otištěny v následujících číslech tohoto časopisu.

Jako manažer v soukromé bezpečnostní firmě chci zdůraznit stále patrné vlivy a dopady pandemie COVID-19, které ovlivnily nejenom chování a požadavky zaměstnanců, ale také samotnou manažerskou práci. Hlavně je nutno zmínit větší požadavky na rovnováhu osobního a pracovního života zaměstnanců, kterou musí v malých a středních firmách respektovat i manažeři.

Dopady pandemie COVID-19 podtrhují i v segmentu české komerční bezpečnosti potřebu dynamičtějšího modelu řízení talentů a práce s nimi. Manažeři i vedoucí zaměstnanci v oblasti lidských zdrojů mohou růstu soukromých bezpečnostních firem pomoci tím, že se budou zaměřovat na identitu, agilitu a škálovatelnost jednotlivých pracovních míst v organizacích těchto firem.

Ve firemních segmentech představují dopady pandemie COVID-19 hluboké a okamžité změny ve fungování jejich organizace v úrovni řízení, v interakci a práci jednotlivých zaměstnanců i pracovních týmů. Během posledních dvou let docházelo u řízení lidských zdrojů často k přechodu na práci na dálku (online), k dynamickému přerozdělování zdrojů a zrychlené digitalizaci a automatizaci činností a procesů, které mají uspokojit měnící se potřeby zaměstnanců v prostředí nejenom soukromých bezpečnostních firem.

Organizace malých a středních firem se s výzvami i příležitostmi tohoto krizového období v zásadě vyrovnaly a soukromé bezpečnostní firmy byly v roce 2022 opětovně schopny dosahovat dílčích růstových aktivit. Tento trend pokračoval i v období let 2023–2024.

Růstové řízení malých a středních firem již ale není možné realizovat podle starých pravidel hierarchie, která řeší uniformitu, byrokracii a kontrolu. Tyto přístupy již nejsou efektivní. V této souvislosti musí nastoupit model, který bude pružnější a bude reagovat efektivnějším způsobem. Takový model bude postaven na čtyřech vzájemně propojených trendech, kterými **jsou větší propojení, bezprecedentní automatizace, nižší transakční náklady a demografické změny.**

To jsou pilíře modelu, které jsou relevantní i pro prostředí soukromých bezpečnostních firem. Pro zavedení organizace budoucnosti by manažeři lidských zdrojů a další vedoucí zaměstnanci měli přijmout nové základní principy organizace malých a středních firem podporující růst. Nově vznikající modely jsou kreativní, přizpůsobivé a flexibilní.

Firemní účel pohání odvážné obchodní činnosti a procesy v souladu s funkčními strategiemi firem. Z hierarchie se stávají sítě pracovních týmů. Z konkurentů se stávají spolupracující subjekty v ekosystému. Malé a střední soukromé bezpečnostní firmy tak mohou participovat na zajištění menších zakázek z velkého celku zakázky, který řeší velká soukromá bezpečnostní firma. A jednotlivé soukromé bezpečnostní firmy se stávají lidštějšími – inspirujícími, spolupracujícími a zaměřenými na vytváření smysluplných a příjemných zkušeností zaměstnanců. Tyto skutečnosti jsou relevantní i v kontextu zavádění CSR (Corporate Social Responsibility – volně přeloženo: firemní společenská odpovědnost) do prostředí malých a středních soukromých bezpečnostních firem v ČR.

Například společnost McKinsey každoročně provádí výzkum, jak mohou firmy v obecné rovině nejlépe organizovat budoucnost a dosahovat růstu i vyšší konkurenceschopnosti a ziskovosti. Probíhající experimenty naznačují, že firmy připravené na budoucnost mají tři společné charakteristiky – **vědí, co jsou a za čím si stojí, fungují s fixací na rychlost, flexibilitu a jednoduchost a rostou díky škálování své schopnosti učit se a inovovat.**

Personální oddělení může tuto transformaci podpořit tím, že usnadní pozitivní změny v těchto třech klíčových oblastech, a také devíti imperativy, které z nich vycházejí. Obecně je možno uvést, že firmy, které vykonávají svou činnost s ohledem na stanovené strategické cíle, mají lepší předpoklady pro vytvoření významné a dlouhodobé přidané hodnoty, což může následně vést k vyšší finanční výkonnosti, větší angažovanosti zaměstnanců a vyšší důvěře zákazníků.

Vlastníci a manažeři malých a středních podniků mají obecně zásadní roli při zajišťování toho, aby organizace těchto firem naplňovaly svůj účel a stanovené firemní hodnoty. HR může formulovat a modelovat žádoucí individuální myšlení a chování spojené se strategickým účelem firem tím, že identifikuje „momenty, na kterých záleží" ve firemní kultuře dané firmy a promítne účel do souboru norem a chování vedení a zaměstnanců ve vztahu k jednotlivým segmentům zákazníků. Personální oddělení takové malé a střední firmy může také zajistit jasné změny v činnostech a procesech náboru a budování schopností tím, že určí charakteristiky „cílevědomého a efektivního" zaměstnance a zakotví tyto atributy v rámci náboru, rozvoje a plánování nástupnictví.

...VĚDÍ, CO JSOU A ZA ČÍM SI STOJÍ, FUNGUJÍ S FIXACÍ NA RYCHLOST, FLEXIBILITU A JEDNODUCHOST A ROSTOU DÍKY ŠKÁLOVÁNÍ SVÉ SCHOPNOSTI UČIT SE A INOVOVAT.

Personální oddělení může také začlenit metriky zaměřené na účel do rozhodování o odměňování a výkonnosti, které mohou významně podporovat růst každé soukromé bezpečnostní firmy, a to včetně pravidel a nastavení poskytování zpětné vazby. V poslední době se do těchto metrik pustily malé a střední firmy napříč odvětvími včetně segmentu komerční bezpečnosti.

Organizace malých a středních firem, které dokáží přerozdělovat talenty v souladu se svými strategickými plány i stanovenými strategickými cíli, mají více než dvakrát vyšší pravděpodobnost, že dosáhnou lepších výsledků než jejich kolegové. Aby bylo možné propojit talent s hodnotou, měli by být nejlepší talenty přesunuty na klíčové pozice, které vytvářejí hodnotu. To znamená opustit či minimálně aktualizovat tradiční přístupy, kdy jsou kritické role a talenty zaměnitelné a založené na hierarchii.

Dosazení nejlepších zaměstnanců do pracovních pozic představujících nejdůležitější role vyžaduje disciplinovaný pohled na to, kde organizace malých a středních firem skutečně vytváří hodnotu a jak k tomu přispívají špičkové talenty. Tyto kulturní priority jsou jádrem hodnotových programů i soukromých bezpečnostních firem. Role potřebné k tomu, aby se tyto priority proměnily v hodnotu, často souvisejí s výzkumem a vývojem a jsou obsazeny talentovanými, kreativními lidmi. Aby bylo možné tento posun uskutečnit, mělo by řízení lidských zdrojů důsledně řídit talenty vybudováním analytické kapacity, která bude vytěžovat data za účelem najímání, rozvoje a udržení nejlepších zaměstnanců pro konkrétní soukromou bezpečnostní firmu v segmentu komerční bezpečnosti.

Obchodní partneři HR, kteří tyto personální potřeby formulují výkonnému managementu, by se měli považovat za interní poskytovatele služeb, kteří zajišťují vysokou návratnost investic do lidského kapitálu. Aby například zapojili vedoucí zaměstnance do pravidelné kontroly talentů, mohou vytvořit poloautomatické datové panely, jež sledují nejdůležitější ukazatele pro kritické role. Je tak důležitá spolupráce jednotlivých relevantních zainteresovaných stran, ale také technické a technologické inovace

Malé a střední firmy mají již zřejmě dostatek empirických zkušeností i dat, které potvrzují, že lepší zkušenosti zaměstnanců znamenají lepší hospodářské výsledky. Úspěšné organizace malých a středních firem spolupracují se svými zaměstnanci na vytváření personalizovaných, autentických a motivujících zážitků, které využívají účel, aby posílily výkonnost jednotlivců, pracovních týmů i oddělení jednotlivých firem v rámci segmentu komerční bezpečnosti.

Týmy i oddělení lidských zdrojů hrají při formování zaměstnanecké zkušenosti klíčovou úlohu. Malé a střední firmy, v nichž personální oddělení usnadňuje vytváření pozitivních zkušeností zaměstnanců, vykazují 1,3krát vyšší pravděpodobnost, že budou vykazovat lepší výkonnost organizace, ukázal výzkum společnosti McKinsey v letech 2022 a 2023. To se stalo ještě důležitějším v průběhu pandemie COVID-19, kdy se organizace firem pracujících na budování týmové morálky a pozitivního myšlení snažily udržet konkurenceschopnost, ziskovost i přidanou hodnotu.

Personální oddělení v malé a střední firmě by mělo usnadňovat a koordinovat zkušenosti zaměstnanců. Organizace firem to mohou podpořit tím, že pomohou personálnímu oddělení se rozvíjet a posílí schopnosti této funkce tak, aby se stala zdrojem pozitivní zaměstnanecké zkušenosti. Pozitivní firemní kultura je základem, na kterém se buduje výjimečná finanční výkonnost, konkurenceschopnost i růst malých a středních firem.

Soukromé bezpečnostní firmy se špičkovou firemní kulturou, měřeno indexem organizačního zdraví společnosti McKinsey, dosahují výnosů pro akcionáře o 60 % vyšších, než je tomu u běžných malých a středních firem. Změna firemní kultury by měla být řízena vedením i manažery, s jasným a dobře viditelným vedením shora, a její provedení by mělo být důsledné a kon-

1. ČÁST

KPKB KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČESKÉ REPUBLIKY

zistentní. Takové firmy mají více než pětkrát vyšší pravděpodobnost úspěšné transformace, pokud byli vedoucí zaměstnanci vzorem pro změny chování, které požadovali po svých zaměstnancích.

Agilita organizace dané malé a střední firmy zvyšuje výkonnost a spokojenost zaměstnanců. Personální oddělení může být nápomocné při posunu organizace od tradiční hierarchie k inovativní znalosti organizace, jež poskytuje talenty a zdroje souboru zmocněných malých pracovních týmů. Pomáhá jim plnit jejich poslání a působí jako společná vůdčí entita. K tomu, aby byla taková transformace úspěšná, měla by se dotýkat všech aspektů organizace, konkrétně **lidských zdrojů, procesů, strategie, struktury a technologií, jež jsou rozhodné pro růst malé a střední firmy.** Oddělení lidských zdrojů může pomoci vytvořit iteraktivní přístup tím, že vytvoří základní prvky procesu řízení lidí, včetně nových kariérních cest pro agilní pracovní týmy, přepracovaného řízení výkonnosti a budování konkurenční schopnosti.

Protože se mnoho pracovních rolí stává nesourodými a proměnlivými, bude i český trh práce stále více definován z hlediska dovedností jednotlivých zaměstnanců. Zrychlující se tempo technologických změn rozšiřuje mezery v dovednostech, které se stávají běžnějšími a rychleji vznikají. Aby všechny organizace přežily a plnily své strategické cíle, budou muset v příštích deseti letech rekvalifikovat a zvyšovat kvalifikaci značné části své pracovní síly. Tento trend je možno označit za faktor rozvoje a růstu dané firmy.

V průzkumu, který společnost McKinsey provedla s globálními vedoucími zaměstnanci v roce 2022 na téma postpandemické pracovní síly, uvedla více než třetina respondentů, že jejich organizace nejsou připraveny řešit nedostatky v dovednostech, jež prohlubuje automatizace a digitalizace. Přechod na digitalizaci se během pandemie COVID-19 zrychlil – až 85 % firem různých velikostí a významu v celoevropském měřítku zrychlilo tempo své digitalizace, a to včetně 48 % nárůstu digitalizace zákaznických kanálů. S ohledem na uvedené trendy a potřeby přesunu dovedností má strategie a plánování pracovních sil jasné obchodní i marketingové opodstatnění.

Oddělení lidských zdrojů by v tomto ohledu mělo být strategickým partnerem malých i středních firem tím, že zajistí, aby byly k dispozici ty správné talenty, které umožní realizovat hlavní cíle v souladu s korporátní strategií. Oddělení lidských zdrojů může také řídit plánování pracovních sil tím, že přezkoumá, jak převratné trendy ovlivňují zaměstnance, určí budoucí klíčové schopnosti a posoudí, jak se nabídka a poptávka vztahují k budoucím nedostatkům v dovednostech.

Přechod k zaměření na dovednosti vyžaduje také inovativní vyhledávání zdrojů, aby se vyhovělo specifickým potřebám pracovní činnosti, a změnu toho, které role musí jednotlivé firmy zajišťovat tradičními pozicemi na plný úvazek a které mohou být vykonávány dočasnými zaměstnanci nebo smluvními partnery.

Dopady pandemie COVID-19 upozornily na význam rychlého rozhodování, protože mnoho organizací muselo postupovat výrazně rychleji, než původně předpokládaly. Personální oddělení může pomoci s pevným rozhodováním tím, že umožní zaměstnancům riskovat v kultuře, která je za to odměňuje. Malé a střední firmy v současné době experimentují s nejrůznějšími přístupy ke zlepšení způsobu řízení výkonnosti.

Podle globálního průzkumu společnosti McKinsey je možno konstatovat, že řízení výkonu nemělo pozitivní vliv na výkonnost zaměstnanců nebo organizace. Přitom je možno identifikovat tři postupy, které zvyšují šanci, že systém řízení výkonnosti pozitivně ovlivní výkonnost zaměstnanců – **koučování vedoucích zaměstnanců, propojení cílů zaměstnanců s odbornými pracovními pozicemi a diferencované odměňování.** Personální oddělení hraje důležitou roli při zavádění těchto postupů do řízení výkonnosti tím, že podporuje proces stanovování cílů, odděluje diskusi o odměňování a rozvoji, investuje do budování schopností manažerů a zavádí technologie a analytiku pro zjednodušení činností a procesů řízení výkonnosti. Všechny tyto skutečnosti též vedou k budoucímu růstu u malých a středních firem.

Obecně je možno uvést, že jedním z nejpodstatnějších znaků prosperující soukromé bezpečnostní firmy je silný a trvalý růst tržeb. V posledních deseti letech se přitom růst některých firem vlivem globální finanční krize zpomalil. Při opětovném růstu cen komodit a energií v roce 2022 a 2023 a současných dopadech války na Ukrajině je stále nutné opětovně podporovat malé a střední firmy v jednotlivých segmentech trhu v jejich růstu.

Aby se vlastníci a manažeři firem dokázali těmto trendům postavit, musí se řídit uceleným strategickým plánem růstu, který se skládá ze tří základních prvků: **inovativních podnikatelských aspirací a doprovodného myšlení, správných nástrojů začleněných do organizace a jasných cest v podobě uceleného souboru růstových iniciativ v prostředí konkrétní malé a střední firmy v segmentu komerční bezpečnosti.**

KOUČOVÁNÍ VEDOUCÍCH ZAMĚSTNANCŮ, PROPOJENÍ CÍLŮ ZAMĚSTNANCŮ S ODBORNÝMI PRACOVNÍMI POZICEMI A DIFERENCOVANÉ ODMĚŇOVÁNÍ

Typická střední firma obecně rostla v průběhu deseti let předcházejících epidemii COVID-19 tempem na úrovni 2,8 % ročně; pouze jedna z osmi společností v evropském měřítku zaznamenala tempo růstu vyšší než 10 % ročně. Takto rostoucí byly zejména inovativní technologické firmy, které poskytovaly produkty založené na AI a dalších prvcích konceptu Průmysl 4.0.

Výzkumy i analytické studie ve firemní praxi opětovně potvrdily, že růst tržeb je rozhodujícím faktorem výkonnosti jednotlivých firem. Pět procentních bodů příjmů ročně navíc koreluje s dalšími třemi až čtyřmi procentními body celkové výnosnosti pro relevantní zainteresované strany. Zdravý růst firmy je obecně také těžké udržet.

Pro pochopení toho, jak se organizace jednotlivých firem mohou pokusit tyto překážky překonat, lze analyzovat jednotlivé segmenty trhu, včetně komerční bezpečnosti, a externí i interní faktory. Přitom jedním z hlavních předpokladů růstu firmy na trhu je jeho konkurenční výhoda. V segmentu komerční bezpečnosti je možné tuto skutečnost rozvíjet u ziskových a dynamických produktů a bezpečnostních zakázek. Důležité jsou též technické a technologické inovace v podnikatelské činnosti jednotlivých firem.

Zásadní je rovněž kvalita poskytovaných produktů a služeb v segmentu českého stavebnictví. Podnik se musí zaměřit na růst tam, kde u něj existuje specifická konkurenční výhoda, například v kvalifikovaných lidských zdrojích a podobně. Firma také může významněji rozvíjet svoji podnikatelskou činnost na regionální úrovni než usilovat o zakázky na celostátní úrovni. Na evropský či globální trh je možno vstoupit pouze v případě, že existuje mezinárodně přenositelná konkurenční výhoda dané firmy i z hlediska produktů či služeb. Je také v pořádku zmenšit okruh podnikatelských aktivit, pokud jsou činnosti takové firmy stále ziskové.

Vysoká návratnost investovaného kapitálu (ve zkratce ROI) svědčí o obchodním modelu dané firmy poháněném konkurenční výhodou. Společnosti, které dosahují vyšší návratnosti, přitahují a rozdělují více kapitálu, což je příznivý cyklus, který jim umožňuje rychlejší růst a dosahování ještě vyšší finanční návratnosti. Některé firmy se ve snaze o růst zřeknou na určitou dobu svých zisků, zatímco mnohem typičtějším a praktičtějším přístupem je vytvoření individualizovaného obchodního modelu a jeho následné rozšíření z lokální a regionální úrovně na národní a mezinárodní úroveň.

Překonání růstu v odvětví českého segmentu komerční bezpečnosti znamená silný obchodní model generující specifickou konkurenční výhodu, kterou kapitálové trhy odměňují, ať už v rychle nebo pomalu rostoucím odvětví. Tímto může být i komerční bezpečnost v ČR. Navíc firmy, kterým se podaří získat podíl na trhu od konkurence, pravděpodobně překonají očekávání růstu promítnutá do ceny svých produktů a služeb a v konečném důsledku to pro ně představuje vyšší ziskovost i další potencionální růst.

Při vytváření strategie růstu vybrané firmy je často první otázkou, která napadne vlastníka či manažera: „Odkud by měl růst dané firmy pocházet?" Primárně je nutno sledovat význam zdravé hlavní činnosti a obecně je možno uvést, že je nepravděpodobné, aby daná firma mohla dosáhnout ihned silného růstu, pokud její hlavní činnost dostatečně neprosperuje.

U některých organizací to může vyžadovat zásadní změnu provozního modelu. Bude i nutno identifikovat produkty a služby s růstovým potenciálem na stávajících nebo nových trzích a přesunout do nich zdroje ze stagnujících segmentů. Firmám s rychle rostoucími hlavními obory podnikání může expanze do nových oblastí pomoci umístit jejich portfolia před budoucími vývojovými trendy. Firmy, jejichž hlavní činnosti rostou pomalu, mohou naopak využít sousedních činností k vyrovnání pomalého růstu v jiných oblastech.

PhDr. Mgr. Dávid Dömény, MBA, DBA

PŘI VYTVÁŘENÍ STRATEGIE RŮSTU VYBRANÉ FIRMY JE ČASTO PRVNÍ OTÁZKOU, KTERÁ NAPADNE VLASTNÍKA ČI MANAŽERA: „ODKUD BY MĚL RŮST DANÉ FIRMY POCHÁZET?"

Seznam odborných zdrojů

ČERVENÝ, R.; FICBAUER, J.; HANZELKOVÁ, A.; KEŘKOVSKÝ, M. 2014. Business plán – krok za krokem. 1. vyd. Praha: C. H. Beck, 230 s. ISBN 978-80-7400-511-4.

HORVÁTOVÁ, P.; BLÁHA, J. ET AL. 2016. Řízení lidských zdrojů. Nové trendy. Praha: Management Press. ISBN 978-80-7261-430-1.

KEŘKOVSKÝ, M.; HANZELKOVÁ, A.; VYKYPĚL, O. 2017. Strategické řízení. Teorie pro praxi. 3. vyd. Praha: C. H. Beck, 256 s. ISBN 978-80-7400-637-1.

KOL. AUTORŮ. 2022. IPSOS CSR & reputation research report. Dostupné na: https://www.ipsos.com/cs-cz/ipsos-csr-reputation-research.

KOL. AUTORŮ. The Business Case for Corporate Social Responsibility. 2021. [online]. Harvard Law School CSR. Dostupné z: https://corpgov.law.harvard.edu/2011/06/26/the-business-case-for-corporate-social-responsibility/.

KOL. AUTORŮ. 2021. Human resources development as an element of sustainable HRM – with the focus on production engineers [online]. USA: PMC. Dostupné z: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7470767/.

KOL. AUTORŮ. 2021. The Four Elements Of Strategic Business Development [online]. USA: Forbes. Dostupné z: https://www.forbes.com/sites/forbescommunicationscouncil/2020/03/09/the-four-elements-of-strategic-businessdevelopment-/?sh=7123485f7f90

KOL. AUTORŮ. 2022. Company analysis: determiningstrategic capability [online]. Strategic Change. Dostupné z: https://onlinelibrary.wiley.com/doi/pdf/10.1002/jsc.568

LYNCH, R. 2018. Strategic Management. Pearson Education Limited, 704 s. ISBN 9781292211404.

MCKINSEY AND COMPANY. 2022. Social Responsibility. Dostupné online: https://www.mckinsey.com/about-us/social-responsibility

MCKINSEY AND COMPANY. 2023. Social Responsibility. Dostupné online: https://www.mckinsey.com/about-us/social-responsibility

TŘI AKTUÁLNÍ OTÁZKY K BEZPEČNOSTI KAMEROVÝCH SYSTÉMŮ

Mgr. Bc. Milan Bláha, LL.M.
lektor FES ÚSII Univerzity Pardubice

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČESKÉ REPUBLIKY

1. JAKÉ TECHNICKÉ NÁSTROJE LZE VYUŽÍT PRO AUTOMATIZACI SPRÁVY KAMEROVÝCH ZÁZNAMŮ A JEJICH BEZPEČNÉ UCHOVÁVÁNÍ V SOULADU S POŽADAVKY GDPR?

Pro automatizaci správy kamerových záznamů a jejich bezpečné uchovávání v souladu s požadavky GDPR lze využít technické nástroje kybernetické bezpečnosti, které lze uplatnit u všech dalších informačních systémů správce, jako jsou například:

EDR

Platforma EDR zaznamenává a vzdáleně ukládá chování koncových bodů na systémové úrovni. Poté je analyzuje, aby odhalila veškerou podezřelou aktivitu a nabídla různé možnosti reakce a obrany.

XDR

Rozšířená detekce a odezva je jednotná platforma pro bezpečnostní incidenty, která využívá umělou inteligenci a automatizaci. Poskytuje organizacím holistický a efektivní způsob ochrany před pokročilými kybernetickými útoky a navrhuje reakce na ně.

IDS

Systém pro odhalení průniku je v informatice obranný systém, který monitoruje síťový provoz a snaží se odhalit podezřelé aktivity.

IPS

Systém prevence průniku je označení zařízení, jehož úkolem je sledovat případnou škodlivou činnost operačního systému, rozpoznat ji, zaznamenávat o ní informace, blokovat a také ji nahlásit. IPS k detekci využívá odhalení protokolových anomálií, provozních anomálií a stavovou detekci značek. IPS může být použito v rámci celé sítě nebo jen operačního systému.

IDR

Detekce a reakce na identitu – jedná se o technologii a procesy, které se zaměřují na detekci a reakci na hrozby spojené s identitami a přístupy uživatelů v IT systémech. IDR řešení pomáhají správcům identifikovat a reagovat na anomálie, které mohou indikovat neoprávněný přístup nebo zneužití identity, což je klíčové pro ochranu citlivých dat a prevenci bezpečnostních incidentů.

DLP

Software na kontrolu kopírování dat. SW pro prevenci ztráty dat detekuje potenciální narušení dat/přenosy exfiltrace dat a předchází jim sledováním, zjišťováním a blokováním citlivých dat při používání, v pohybu i v klidu.

Mezi hlavní aktivity pro zvýšení ochrany osobních údajů a kybernetické bezpečnosti lze uvést i další nástroje:

- nástroj pro řízení přístupových oprávnění,
- nástroj pro ochranu integrity komunikačních sítí,
- nástroj pro zajišťování úrovně dostupnosti informací,
- nástroj pro ochranu před škodlivým kódem,
- kryptografické prostředky.

2. JAKÉ PROBLÉMY LZE SPATŘOVAT V IMPLEMENTACI A DODRŽOVÁNÍ GDPR U MALÝCH FIREM (SPRÁVCŮ MENŠÍCH KAMEROVÝCH SYSTÉMŮ), KTERÉ NEMAJÍ DOSTATEK PERSONÁLNÍCH NEBO FINANČNÍCH ZDROJŮ?

Hlavní problém při implementaci a dodržování GDPR v malých zdravotnických zařízeních vidím v náročnosti na splnění všech požadavků uvedených v GDPR a popsaných v příslušné metodice úřadu ÚOOÚ.

Základním „kamenem úrazu" jsou právní znalosti legislativy (zejména GDPR, občanský zákoník, zákoník práce). GDPR není jediným právním předpisem, který se vztahuje na ochranu osobních údajů (jedná se přece jen o obecné nařízení). Znalost právních základů, účelů zpracování a zásad zpracování osobních údajů je u kamerových systémů zásadní.

V praktické rovině je to pak zajištění školení a tvorba povinné dokumentace (evidence kamer, provozní kniha, interní předpis k ochraně osobních údajů v kamerovém systému, test proporcionality neboli balanční test, záznamy o činnostech zpracování, informace o zpracování osobních údajů – bezpečnostní tabulky a informace na webových stránkách).

Bez pomoci odborníka na problematiku kamerových systémů, včetně znalostí GDPR a dalších předpisů, se tato zařízení jen stěží obejdou. Pokud zdravotnická zařízení nemohou takového odborníka zaměstnat, je třeba si jej nasmlouvat (za podmínky uzavření zpracovatelské smlouvy dle čl. 28 GDPR).

Většinou však chybí vůle správců kamerových systémů vůbec něco změnit. Kontroly dozorového úřadu nejsou prováděny v takové míře, aby správci kamerových systémů cítili nějaký tlak (přes vysoké pokuty do 10 mil. Kč dle zákona č. 110/2019 Sb., o zpracování osobních údajů). Snad jen možná stížnost subjektu údajů k dozorovému orgánu může přispět k nápravě současného stavu.

Finanční zdroje jsou vždy omezené, bez ohledu na velikost zdravotnického zařízení. Z technického hlediska lze ušetřit na počtu kamer, ovšem zpravidla je to vždy na úkor bezpečnosti. Počet kamer a jejich rozmístění se odvíjí od vypracovaného bezpečnostního auditu. Ve výjimečných případech lze kamery nahradit atrapami, ovšem zaměstnanci o nich musí být informováni. Jinak by mohl být instalací atrapy kamerového systému porušen zákoník práce (§ 302, písm. c) zák. č. 262/2006 Sb., konkrétně povinnost „vytvářet příznivé pracovní podmínky a zajišťovat bezpečnost a ochranu zdraví při práci").

V případě absence bezpečnostního auditu, kdy je instalace plně ponechána na dodavatelské firmě, se lze v praxi setkat i s tím, že kamera není umístěna tam, kde by to bylo z bezpečnostního hlediska žádoucí, ale tam, kam technik např. snadno, s minimální námahou dosáhne.

3. JAKÝM KONKRÉTNÍM ZPŮSOBEM LZE ZVÝŠIT ZABEZPEČENÍ KAMEROVÝCH SYSTÉMŮ PROTI POTENCIÁLNÍM KYBERNETICKÝM HROZBÁM?

Zabezpečení kamerových systémů lze zvýšit přijetím vhodných technických a organizačních opatření dle čl. 32 GDPR, včetně případných opatření dle předpisů o kybernetické bezpečnosti, jako jsou například:

a) Kontrola přístupu do prostor a zařízení

Opatření zabraňující přístupu neoprávněných osob k systémům zpracování údajů, kterými jsou osobní údaje zpracovávány nebo využívány – kamerový systém, EZS, EKV, klíčový režim, interní předpisy.

b) Řízení přístupu k systémům

Datové nosiče jsou spravovány podle určeného procesu (ochrana proti hrozbám).

K nosičům dat mohou přistupovat pouze oprávněné osoby. Bezpečné a zabezpečené heslo. Vhodné nastavení monitorů (prohlížečů).

c) Řízení přístupu k údajům

Opatření, která zajistí, aby osoby oprávněné k používání systému zpracování údajů měly přístup pouze k údajům, ke kterým mají přístupové právo, a aby osobní údaje nebylo možné po uskladnění, v průběhu zpracování nebo používání číst, kopírovat, upravovat nebo odstraňovat bez povolení – přístupové heslo do prohlížeče kamerového systému určené oprávněným osobám.

d) Řízení přenosu

Opatření, která zajistí, aby osobní údaje nebylo možno číst, kopírovat, upravovat nebo odstraňovat bez povolení během elektronického přenosu nebo během jejich přepravy nebo ukládání na datové nosiče a aby bylo možné zkontrolovat a zjistit, na které subjekty se přenos osobních údajů prostřednictvím zařízení pro přenos údajů vztahuje – šifrování přenosu dat.

e) Řízení zpracování dat

Školení a kontrola oprávněných osob, mlčenlivost zaměstnanců, logování přístupu, vedení dokumentace.

f) Řízení dostupnosti

Opatření k zajištění ochrany osobních údajů před náhodným zničením nebo ztrátou – záložní systém elektřiny, zálohování dat, postup při mimořádných událostech, nastavení automatických aktualizací SW na koncových zařízeních.

PŘELOMOVÁ KAMPAŇ ZKRATKY

SPOLEČNÝ PROJEKT ČESKÉ ASOCIACE POJIŠŤOVEN (ČAP) A POLICIE ČR

Během čtyř měsíců významně změnila postoj Čechů k problematice drog. Ukázaly to rozsáhlé průzkumy společnosti STEM/MARK. Kampaň propojila odborníky, umělce, média, preventisty, policii i státní správu s cílem snížit rizika spojená s užíváním návykových látek.

Osvětová kampaň, která zahrnovala seriál Adikts, dokumentární cyklus Česko na drogách a minipořady upozorňující na závažná fakta spojená s užíváním drog, podle průzkumu oslovila takřka každého obyvatele České republiky ve věku nad 15 let. V rámci kampaně byly vysílány také televizní spoty upozorňující na nebezpečí spojená s užitím drog za volantem a součástí byla i rozsáhlá PR komunikace a masivní debata na sociálních sítích.

Kampaň tak zanechala výraznou stopu v postojích obyvatel k užívání nelegálních drog. Průzkumy před hlavní částí kampaně, během ní a po ní ukázaly, že více než polovina lidí si všimla zintenzivnění komunikace na téma užívání drog a dalších návykových látek. Více než 80 % lidí ve věku 15–54 let zaznamenalo obecně intenzivnější komunikaci o nebezpečnosti drog, nebo dokonce některý z konkrétních formátů kampaně.

Odborné diskuze podporují důležitost kampaně

Zkratky přinesly podle výzkumů zásadní proměnu v postojích občanů k drogám. Kampaň upozorňovala na to, že drogy jsou zkratky a mohou vést do slepé uličky. Šest z deseti lidí vidí v drogách zkratky a podíl těch, kteří drogy považují za berličku, roste. Došlo ale také k výraznému snížení počtu lidí, kteří upřednostňují impulzivní životní styl. Asociace drog s nebezpečím, rizikem a obavami se v důsledku kampaně zvýšila.

„V českém prostředí unikátní a formátově velkorysá kampaň vzbudila žádoucí pozornost a rozproudila debatu o vnímání závislostního chování a přístupu k němu v kontextu doby a formou, která nemoralizuje, ale klade otázky a nasvěcuje jej z mnoha netradičních názorových úhlů jako reálný společenský fenomén, který nemá černobílá řešení," uvádí ředitel Národní protidrogové centrály služby kriminální policie a vyšetřování brig. gen. PhDr. Jakub Frydrych.

Podstatné změny v postojích k drogové problematice

Podle předkampaňového průzkumu neměla téměř polovina české populace o drogách dostatek informací a ani o ně nejevila zájem. V tomto ohledu zaznamenala ČAP velmi pozitivní dopad, vzrostla informovanost a snížil se podíl lidí, kteří se o téma nezajímají. Navíc více než třetina lidí zná název Zkratky nebo zaregistrovala kampaň, která o drogách jako o „zkratkách" mluví. Z konkrétních formátů byly nejčastěji zaznamenány reklamní spoty a seriál Adikts.

Kampaň také pozitivně rezonovala mezi lidmi napříč věkem i vzděláním. Nejvíce ohroženou skupinu představují mladí lidé, na které také Zkratky cílily, a ti z nich, kteří se s kampaní ztotožnili, uvažují nyní o drogách mnohem zodpovědněji. Průzkum také potvrdil, že u nezletilých jsou hlavními zdroji informací škola a sociální sítě a u mladých dospělých pak spíše filmy a seriály. I z tohoto důvodu se potvrdila správnost taktiky a většina respondentů považovala kampaň za srozumitelnou, užitečnou a originální s motivací zamyslet se nad individuálními i celospolečenskými dopady

Zaměření na mládež: moderní metody vzdělávání a osvěty

„Podle mého názoru byla kampaň moderní a atraktivní, rozpoutala i odbornou a laickou diskusi a vyvolala kontroverze," vysvětluje odborník na vzdělávání a inovace ve výuce Petr Chára. „Určitě je dobře, že vznikl také hraný high-end seriál, který je pojat v duchu současných světových seriálů pro mladé a který je digitálně dostupný. Je zřejmé, že klasické besedy a pasivní přijímání informací už nejsou pro dnešní mládež atraktivní a neplní svůj účel. Kombinace otevřené komunikace, atraktivního digitálního obsahu, příběhů z reálného života a interaktivních forem výuky může být naopak velmi efektivní a zábavná," pokračuje dále Chára.

Průzkum, který byl proveden za účelem zjištění názorů na seriál Adikts, jeho vyznění a vnímání z pohledu mladých diváků, tedy generace Z, ukázal, že seriál je vnímán jako vhodná součást osvětové kampaně. Je natočený dostatečně poutavě pro binge-watching, má zajímavě vykreslené charaktery, vzbudil zájem a rozpoutal diskusi. O uživatelích drog a drogách obecně vypráví realistickým a věrohodným způsobem, ale zároveň obsahuje i dostatek nepříjemných momentů, které upozorňují na škodlivost drog, jako agresi, změny chování a vedlejší účinky. Z dalších součástí kampaně jsou nejlépe hodnoceny minipořady, které jsou považovány za úderné, graficky pěkné a informačně zajímavé.

„Naším hlavním cílem bylo oslovit mladé lidi tam, kde tráví nejvíce času – tedy na sociálních sítích a online. Zvolili jsme inovativní mediální mix, který se ukázal jako velmi efektivní. Kampaň zasáhla mnohem širší publikum, než jsme očekávali. Čtyři z pěti lidí ve věku 15–54 let zaznamenali zvýšenou komunikaci o tomto tématu nebo se setkali s některým z našich formátů. Nejvíce nás těší, že jsme trefili správný tón u mladých lidí. Výsledky potvrzují, že nástroje, které jsme zvolili, jsou skutečně účinné a kampaň má pozitivní ohlas a plní svůj účel," uvádí Milada Veselá, vedoucí Oddělení komunikace a vzdělávání.

WWW.DROGYJSOUZKRATKY.CZ

KPKB KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČESKÉ REPUBLIKY

DATA Z VÝZKUMU BĚHEM KAMPANĚ ZKRATKY

- Více než polovina lidí si všimla zintenzivnění komunikace na téma užívání drog a dalších návykových látek.
- Více než 80 % lidí ve věku 15-54 let zaznamenalo obecně intenzivnější komunikaci nebezpečnosti drog, nebo dokonce některý z konkrétních formátů kampaně.
- Více než třetina lidí zná název kampaně Zkratky nebo zaznamenali kampaň, která o drogách jako o „zkratkách" mluví.
- Z konkrétních formátů byly nejčastěji zaznamenány reklamní spoty a seriál Adikts. Během kampaně vzrostla také informovanost o tématu a snížil se podíl lidí, kteří se o téma nezajímají.
- Kampaň také pozitivně rezonovala mezi lidmi napříč věkem i vzděláním. U skupiny 15 až 17 let narostly negativní asociace s drogou, a ti z nich, kteří se s kampaní ztotožnili, uvažují o drogách mnohem zodpovědněji.

Zdroj: Česká asociace pojišťoven https://www.opojisteni.cz/pojistny-trh/cap-zkratky-zmenily-postoje-cechu-k-drogam-a-vyrazne-zvysily-informovanost/c:28103/#_ftn1

SHRNUTÍ ZÁSADNÍCH DAT Z OBLASTI DROG A ZÁVISLOSTÍ

Zde je souhrnný seznam zásadních dat k drogové tematice. Data jsou čerpána z výzkumu agentury STEM/MARK 2023 pro Českou asociaci pojišťoven, který byl realizován v termínu 1.-7. června 2023 na reprezentativním vzorku české populace ve věku 15-54 let. Dále je čerpáno ze Zprávy Národního monitorovacího střediska pro drogy a závislosti z roku 2023 a dále z datové analýzy Portálu nehod Policie České republiky. Data jsou pro lepší přehlednost rozdělena do tematických bloků.

OBECNÁ DATA

51,5 % české populace drogy striktně odmítá, 48,5 % k nim má poněkud benevolentnější postoj. [1]

43 % lidí přiznalo zkušenost s konopím, mezi mladistvými to bylo 27 %. Zkušenost s tvrdou drogou přiznalo 18 % populace, u mladistvých to bylo 10 %.[2]

Tvrdé drogy podle vlastních slov občas užívá každý desátý mladistvý.[3]

- Problematické užívání psychoaktivních léků má 1,3–1,5 mil. osob.
- Intenzivních uživatelů konopných látek je 350–465 tis. osob.

Užití v obecné populaci 15-64 let v roce 2022: [4]

Jakákoliv nelegální droga	47,4 %
Konopné látky	43,2 %
Extáze (MDMA)	8,9 %
Halucinogenní houby	8,2 %
Kratom	7,7 %
LSD	5,4 %
Kokain	5,3 %

Na celou populaci ČR ve věku 15+ let je v ČR odhadem 1,35 mil. osob vykazujících známky rizikového užívání psychoaktivních léků, v tom odhadem 430 tis. mužů a 900 tis. žen.

Sedativa a hypnotika užívá rizikově odhadem 1,1 mil. osob, v tom 310 tis. mužů a 780 tis. žen.[5] Opioidní analgetika nadužívá odhadem 550 tis. osob, v tom 220 tis. mužů a 330 tis. žen . Lidé užívajících drogy (pervitin a opioidy) rizikově je 44–46 tis .[6]

UŽÍVÁNÍ DROG MEZI MLADISTVÝMI

24 % 16letých studentů užilo v posledních 12 měsících nelegální drogu, (23 % užilo konopné látky, 3,5 % sedativa bez předpisu, 3,3 % těkavé látky, 2,6 % extázi, 1,1 % halucinogenní houby, 1,9 % LSD či jiné halucinogeny a přibližně 1 % kokain či pervitin).[7]

Spotřeba drog u mladistvých v roce 2022 byla poměrově:

Konopí	21,2 %
Kratom	4,4 %
Extáze (MDMA)	2,0 %
Halucinogenní houby	2,1 %
LSD	1,7 %
Pervitin[8]	1,0 %

DĚTI A RODIČE

- 59 % rodičů si myslí, že jejich děti mají o návykových látkách lepší přehled než oni. Čím starší děti lidé mají, tím spíše si myslí, že jejich děti drogám rozumějí lépe než oni sami.[9]
- 4 z 5 rodičů si myslí, že vědí, s čím se v oblasti návykových látek jejich děti mohou setkat.
- Ti ostatní se o to příliš nestarají, protože svým dětem věří, což zmiňuje 76 % z nich.[10]

PREVENCE A OSVĚTA

V návykových látkách se lidé dobře orientují pouze v problematice kolem alkoholu, v drogách se nevyznají. Polovina lidí si uvědomuje, že o drogách nemá dostatek informací. Naprostá většina z nich o ně ale ani nejeví zájem. Jen 6 % lidí uvádí, že informace jsou obtížně dostupné, a proto se cítí být neinformováni. Ostatní si na jejich nedostatek nestěžují. Více informací o drogách by uvítali mladiství. Osvětu v oblasti řízení pod vlivem omamných látek považuje za dostatečnou cca třetina populace.[11]

Osvěta o drogách by měla být součástí školní výuky, míní 46 % lidí.[12]

Za nejlepší informační kanály pro informování široké veřejnosti o drogové problematice jsou kromě škol filmová zpracování, dokumenty a seriály, což zmiňuje 33 % lidí. 23 % osob považuje za vhodné osvětové kampaně, 19 % různé veřejné debaty. Lidé se shovívavým postojem k drogám, na které by různé osvětové kampaně měly cílit především, o ně ale nejeví téměř žádný zájem. Masová média vč. internetu považují za vhodný informační kanál o tomto tématu tři čtvrtiny populace.[13]

ŘÍZENÍ POD VLIVEM

Jen třetina lidí si myslí, že je osvěta v otázce drog za volantem dostatečná. Řízení pod vlivem omamných látek Češi považují za poměrně závažný problém. Pro 72 % lidí je to skutečně zásadní problém na našich silnicích, jen 5 % populace to považuje za problém okrajový.[14]

Obecné statistiky z Portálu nehod PČR za období 2010-2022:

70 818 - počet nehod s přítomností alkoholu/drog (u řidiče nebo chodce nebo v různých kombinacích)

18 641 - (26,32 %) nehody s přítomností alkoholu/drog, při kterých byl přítomen spolujezdec.[15]

Hlavní příčiny nehod s přítomností alkoholu/drog v krvi řidiče:

Nejčastější příčinou u nehod s přítomností alkoholu či drog je způsob jízdy, ten tvoří téměř 56 %. Z toho se např. 11 645 řidičů plně nevěnovalo řízení vozidla, 10 316 nezvládlo řízení vozidla, 3 489 případů byla jízda po nesprávné straně vozovky a u více než 3 000 bylo nesprávné otáčení či couvání. Druhou nejčastější příčinou je rychlost (např. nepřizpůsobení rychlosti technickému stavu vozovky, nepřizpůsobení rychlosti vlastnostem vozidla a nákladu), tato příčina tvoří až 30 % nehod pod vlivem.[16]

Pokud se zaměříme pouze na hlavní příčiny nehod podle věku, rychlost hraje výraznější roli u řidičů ve věku 18 až 38 let. Pokud se zaměříme na nejčastější příčiny nehod s přítomností pouze drog, zde se nejvíc vyskytuje nepřizpůsobení rychlosti technickému stavu vozovky.[17]

Tzv. fenomén discocrash[18]

- **70 818** - celkový počet nehod s přítomností alkoholu/drog
- z toho **18 641** je nehod, při kterých byl přítomen spolujezdec, tedy **26,32 %** nehod
- věk spolujezdců při těchto nehodách je nejčastěji 18 až 24 let (více než **6 000** nehod)
- **jedná se o ukázkový příklad situace tzv. discocrash**, tedy kdy mladí lidé jedou společně z nějaké akce s alkoholem / drogami v krvi
- tuto situaci potvrzuje i počet nehod v pozdních hodinách, neboť u této věkové kategorie jsou to nejčastěji večerní hodiny mezi 22.00 hodinou večer a 1:00 hodinou ranní. Více se nehody dějí v letních měsících (cesty z diskoték), nejvíce nehodovým dnem je sobota

Věkové rozložení zaviněných nehod s přítomností drog:

Drogy za volantem jsou doménou mladých, i těch úplně nejmladších řidičů, kteří drogy často kombinují i s alkoholem. Alarmující je i fakt, že je sem zahrnuta skupina od 15 do 17 let (tvoří sice minimální procento, ale vyskytují se zde) a celkových 57 % se týká lidí ve věku 18-31 let, tedy více než polovina. V kombinaci alkohol a drogy se tento poměr ještě zvyšuje na celkem 62 % lidí ve věku 18-31 let.[19]

Zranění:

Téměř 6 % nehod s přítomností drog končí těžkými zraněními či úmrtím někoho z posádky vozidla, obdobné procento (5 %) těžkého zranění či úmrtí je v kombinaci alkohol i drogy.

ÚMRTÍ A ZRANĚNÍ

- 14–15 tis. případů hospitalizací je ročně hlášeno pro úraz pod vlivem návykových látek
- **16–18 tis.** úmrtí je ročně způsobeno kouřením tabáku
- **6–7 tis.** úmrtí je ročně způsobeno pitím alkoholu
- **64 lidí** v r. 2021 zemřelo v důsledku smrtelných předávkování
- **150** případů úmrtí bylo identifikováno pod vlivem nelegálních drog a psychoaktivních léků z jiných příčin než předávkování, z toho nejvíce v důsledku nemocí, nehod a sebevražd.[20]

Rizikové formy závislostního chování mezi dospělými[21]	
Denní kuřáci	**1,5–2,1 mil.**
Denní konzumenti alkoholu	**800–980 tis.**
Rizikové pití alkoholu	**1,5–1,7 mil.**
z toho ve vysokém riziku (tzv. škodlivé pití)	**800–980 tis.**
Problematické užívání psychoaktivních léků	**1,3–1,5 mil.**
Intenzivní uživatelé konopných látek	**350–465 tis.**
z toho ve vysokém riziku	**160–250 tis.**
Lidé užívající drogy (pervitin a opioidy) rizikově	**44–46 tis.**
uživatelé pervitinu	**34–35 tis.**
uživatelé opioidů	**10–11 tis.**
lidé užívající drogy injekčně	**40–41 tis.**
Osoby v riziku problémového hraní	**170–220 tis.**
z toho ve vysokém riziku	**91–120 tis.**
Osoby v riziku digitální závislosti	**375–510 tis.**
z toho ve vysokém riziku	**90–160 tis.**

1) Výzkum agentury STEM/MARK pro ČAP 2023, reprezentativní vzorek české populace 15-54 let, termín sběru dat červen 2023.

2) Výzkum agentury STEM/MARK pro ČAP 2023, reprezentativní vzorek české populace 15-54 let, termín sběru dat červen 2023.

3) Výzkum agentury STEM/MARK pro ČAP 2023, reprezentativní vzorek české populace 15-54 let, termín sběru dat červen 2023.

4) Zpráva o nelegálních drogách v České republice 2023. Národní monitorovací středisko pro drogy a závislosti.

5) Zpráva o problematickém užívání psychoaktivních léků v České republice 2023. Národní monitorovací středisko pro drogy a závislosti.

6) Zpráva o nelegálních drogách v České republice 2023. Národní monitorovací středisko pro drogy a závislosti.

7) Národní monitorovací středisko pro drogy a závislosti. Přehled situace. Příloha k tiskové zprávě 15. 5. 2023.

8) Zpráva o nelegálních drogách v České republice 2023. Národní monitorovací středisko pro drogy a závislosti.

9) Výzkum agentury STEM/MARK pro ČAP 2023, reprezentativní vzorek české populace 15-54 let, termín sběru dat červen 2023.

10) Výzkum agentury STEM/MARK pro ČAP 2023, reprezentativní vzorek české populace 15-54 let, termín sběru dat červen 2023.

11) Výzkum agentury STEM/MARK pro ČAP 2023, reprezentativní vzorek české populace 15-54 let, termín sběru dat červen 2023.

12) Výzkum agentury STEM/MARK pro ČAP 2023, reprezentativní vzorek české populace 15-54 let, termín sběru dat červen 2023.

13) Výzkum agentury STEM/MARK pro ČAP 2023, reprezentativní vzorek české populace 15-54 let, termín sběru dat červen 2023.

14) Výzkum agentury STEM/MARK pro ČAP 2023, reprezentativní vzorek české populace 15-54 let, termín sběru dat červen 2023.

15) Analýza dat z Portálu nehod PČR za období 2010-2022.

16) Analýza dat z Portálu nehod PČR za období 2010-2022.

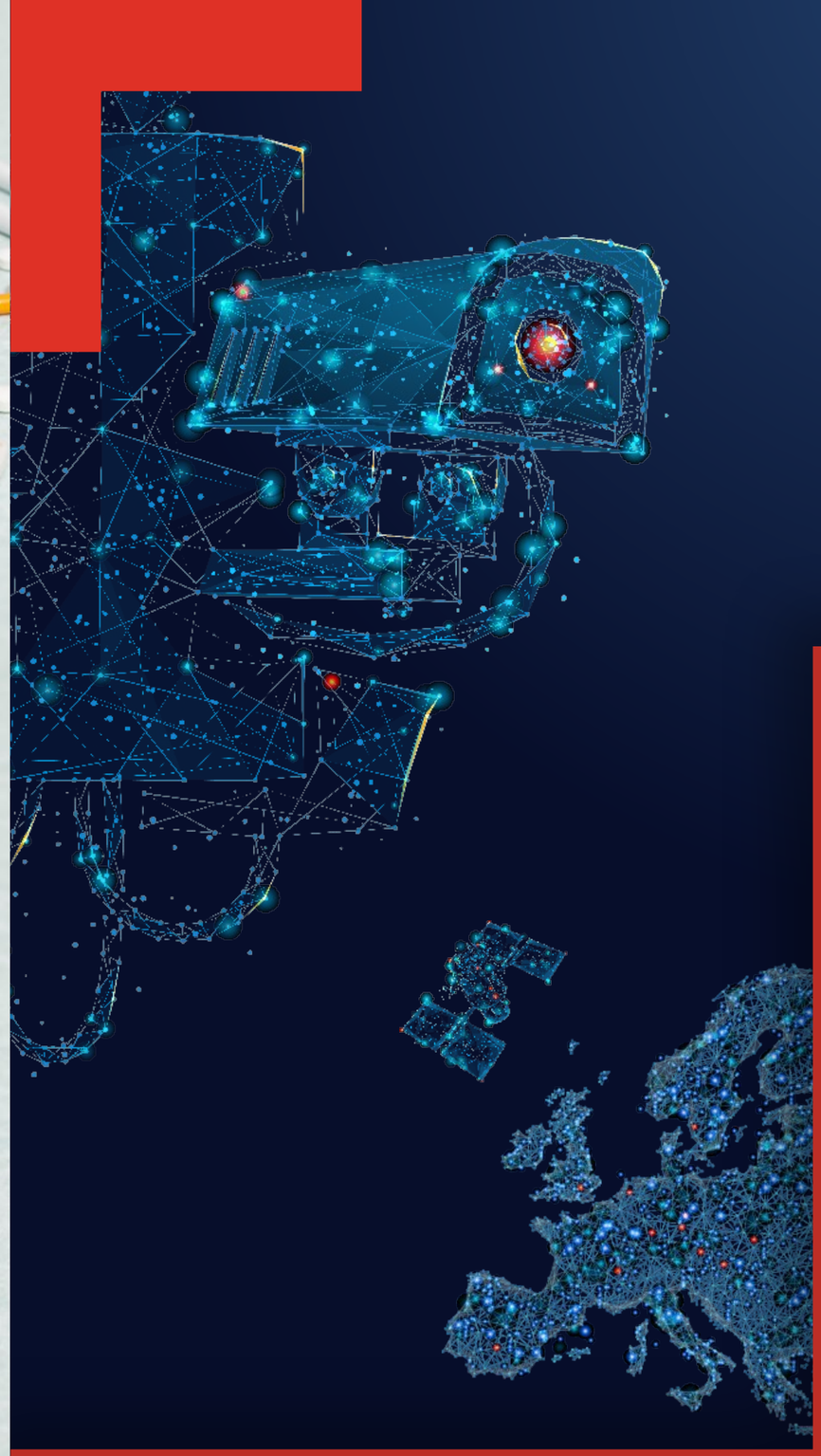
17) Analýza dat z Portálu nehod PČR za období 2010-2022.

18) Analýza dat z Portálu nehod PČR za období 2010-2022.

19) Analýza dat z Portálu nehod PČR za období 2010-2022.

20) Národní monitorovací středisko pro drogy a závislosti. Přehled situace. Příloha k tiskové zprávě 15. 5. 2023.

21) Národní monitorovací středisko pro drogy a závislosti. Přehled situace. Příloha k tiskové zprávě 15. 5. 2023.



S KÝM (NE)SPOLUPRACOVAT?

Jednoduchá otázka, ale těžká odpověď. Každý z nás nosí v hlavě představu ideálního partnera jak pro práci, tak pro život. Naše vize se však mnohdy naplňují jen obtížně. Aplikovanou částí psychologie je manažerská psychologie. Snaží se dát na otázku položenou v názvu co nejkomplexnější odpověď. Všechny typy, které uvádí, mají v sobě něco, co se nám může líbit, a co ne. Lidská typologie je složitá, proto uvedeme pro laickou veřejnost alespoň některé, poměrně srozumitelné příklady typů pracovníků – čtenář může posoudit sám.

IDEOVÝ TYP – řídí se ve svém životě ideály, které jsou pochopitelné pouze pro něj. Vše jim podřizuje, nezáleží mu na jinak smýšlejících lidech, na obsahu či produktivitě práce. Jsou-li jeho ideály pracovně pozitivní, může z něj být dobrý parťák pro spolupráci. Negativním příkladem jsou pak např. sabotéři, či rasisté nebo xenofobové, kteří odmítají vše, co pochází odjinud než z domova, neuznávají informace z ciziny.

SOCIÁLNÍ TYP – preferuje ve svém životě nade vše sociální vztahy. Nezáleží mu na obsahu a výsledku práce, na první místo klade pokojné vztahy s lidmi, upřednostňuje vzájemné sympatie a kvalitní sociální klima. To je jistě chvályhodné, v pracovním kolektivu však nesmí být potlačena produktivita práce na úkor sociálních vztahů. Může to pak mimo jiné způsobit, že toleruje i neschopného spolupracovníka jen proto, aby se z hlediska sociálních vztahů cítil komfortně.

ČINNOSTNÍ TYP – má zcela jasno, kterou činnost chce vykonávat. Nezajímá ho výdělek, pracovní doba, sociální prostředí. Jeho hlavní prioritou je činnost, které se chce věnovat. Jedná se hlavně o individualisty, které enormně zajímá jejich práce, bez ohledu na ostatní faktory. Své činnosti jsou ochotni téměř vše obětovat. Jsou z nich kvalitní a často výkonní pracovníci, ale spolupráce s nimi není jednoduchá, neboť si hledí primárně toho svého, bez ohledu na ostatní. Patří sem např. počítačoví specialisté, někteří architekti a vesměs pracovníci v technických profesích. Určitě nelze tyto pracovníky hledat v sociálních oblastech, které vyžadují nutnou kooperaci.

VĚČNÝ CESTOVATEL – je na svém pracovišti obtížně k sehnání. Věčně někde pobíhá, často svou nenadálou přítomností obtěžuje ostatní, ale sám si to nejspíš neuvědomuje. Má radost, když se může podílet na řešení věcí, které mu nepřísluší, a udělovat rady a moudra tam, kde o ně nikdo nestojí. Je schopen jakýchkoli výmluv, jen aby se nemusel zdržovat na svém pracovišti a podávat odpovídající pracovní výkon.

DETAILISTA – toho nezajímá výslednost činnosti jako celku, zajímá ho detail, např. dostatek papíru, na který ale nic kloudného nenapíše, ořezané tužky, přesně srovnané věci na psacím stole nebo dokonale upravený zevnějšek s příslušným výrazem tváře. Tomuto jedinci však zcela uniká podstata jeho práce, a pokud se nejedná o detaily, které zajímají jen jeho, např. o barevně rozlišenou, jinak ale bezobsažnou zprávu, kterou sám vytvořil, nejeví zájem o spolupráci s ostatními.

AGRESOR – je cholerický typ, jehož první reakcí je emoční afekt vzteku a otevřené naštvanosti. V komunikaci a jejím způsobu si nebere servítky. Máme-li na něj pracovní požadavek, okamžitě v něm najde negativa a odmítne jej. Jeho prvotní vzteklá reakce sice po chvíli zpravidla odezní, brzy ji však vystřídá vztek nový. Je-li tento pracovník ve svém oboru odborníkem a máme-li trpělivost snášet napjatou atmosféru, kterou kolem sebe šíří, může pracovní povinnosti plnit kvalitně. Jeho okolí je však jeho věčnými vzteklými afekty většinou otráveno.

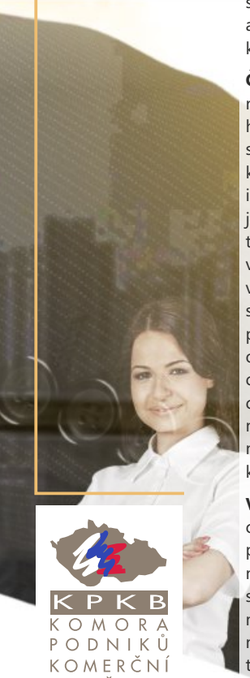
PARTICIPATIVNÍ TYP – participaci obecně vymezujeme jako schopnost spolupráce s ostatními, spolupodílnictví. Je to záležitost velmi chvályhodná a vítaná. V případě typu pracovníka se však jedná o jedince, který není schopen (jak v životě, tak v práci) samostatně fungovat. Nutně potřebuje k sobě někoho, kdo jej bude ujišťovat a chválit jeho pracovní i životní rozhodnutí. Tento typ je velmi unavující, nutí ostatní, kteří mají své povinnosti, k ohledům na sebe. Při počátečním zaučování takto fungovat může, po nějaké době se však musí osamostatnit.

AUTORITÁŘ – chce mít za každou cenu autoritu a respekt, stát zřetelně v čele. Rád rozhoduje a organizuje, aniž by přijímal zodpovědnost. Při spolupráci s ostatními přebírá vůdčí roli, snaží se řídit ostatní, sám však přitom mnohdy není kvalitním a spolehlivým odborníkem. Převezme-li však autoritář za svá rozhodnutí i odpovídající míru zodpovědnosti, je díky svým organizačním schopnostem vhodným typem pro řešení nenadálých, časově náročných a nepopulárních úkolů.

SOUHLASNÝ TYP – je spolupracovníky často označován jako „přikyvovač". Je to jedinec, který není schopen otevřeně říct svůj názor, často odlišný od názorů ostatních. Díky tomuto charakterovému defektu bývá oblíben u některých nadřízených prosazujících nevhodné pracovní změny, protože jim vždy i bez svých opodstatněných námitek vše odsouhlasí. Při vhodně zvolené argumentaci je tento pracovník snadno manipulovatelný a lze jej většinou bez problémů nasměrovat tam, kam je potřeba.

VĚČNÝ NEGATIVISTA (a kritik) – na všem hledá chyby a to, co se v práci podaří, neguje. V žádném případě nepřináší do pracovního týmu nic nového, přínosného. Vytváří nepříjemnou atmosféru, spolupracovníci se mu v očekávání jeho negativních a kritických komentářů vyhýbají. Při kontaktu s novými a nezkušenými pracovníky jednoznačně sráží jejich pozitivní pracovní motivaci, nikdy nikoho za nic nepochválí.

KONSTRUKTIVNÍ TYP – lze jej hodnotit pozitivně. Je-li ve své činnosti odborníkem, zřetelně vnímá klady a nedostatky pracovního procesu a přináší realizovatelné návrhy na jeho zkvalitnění. V krajním případě však může působit kontraproduktivně – když jeví snahu vše radikálně změnit, aniž bere zřetel na zaběhnutý existující pracovní režim. Má-li ovšem tento typ dostatek možností, dokáže se ukáznit a metodou postupných kroků realizovat své cíle a zkvalitnit jak pracovní efektivitu, tak prostředí.



Existuje ještě poměrně velké množství pracovních typů. Využitelnost pracovní typologie je však závislá na druhu vykonávané činnosti, na konkrétním pracovním prostředí, a hlavně na motivaci lidí v pracovním kolektivu.

Většina lidí má nějakou svou psychickou libůstku, zvláštnost, která se promítá, mnohdy nevědomky, do jejich životů, a vzbuzuje u jiných lidí pobavení, humor, nebo je naopak odrazuje a je jim na závadu.

Manažerská psychologie uvádí i další zajímavé typy pracovníků, např.:

- **„typ člověka, který se neustále diví"** – udivuje jej jeho život, děti i jejich výchova či práce; přestože byl mnohokrát seznámen s podstatou své činnosti, pořád je jí udiven;

- **„astrální typ"** – nedá dopustit na horoskopy a příslušná měsíční znamení; neustále se podle nich řídí a vše podle nich vysvětluje, často však bývá mimo realitu;

- **„příliš drahý experimentátor"** – je v podstatě „pracovní fantasta" – přečetl si někde něco o nových pracovních metodách, často podivných a nereálných, a pokouší se je aplikovat do pracovní činnosti – tam však většinou za vysokou cenu lidských sil i finančních investic selžou;

- **„tvrdý logik"** – prahne po přísně logickém zdůvodnění všeho, co dělá – nehodí se pro práci, která vyžaduje kreativitu, opovrhuje tvůrčím přístupem, považuje jej za zbytečný;

- **„studijní typ"** – má někdy podobu „věčného studenta", ani ten se do tvůrčích činností příliš nehodí; studovat a zdokonalovat se je jistě chvályhodné, nicméně v krajní podobě tento typ nestuduje kvůli sobě, ale proto, aby své okolí udivoval nově získanými informacemi; jeho pracovní produktivita je nízká, neboť vyžaduje stálé zohledňování svého studia.

Mgr. Zoja Kalivodová, CSc.
sociální psycholožka

SPOLEČENSKÁ ODPOVĚDNOST TROCHU JINAK ANEB ZDRAVOTNÍ HENDIKEP NEMUSÍ BÝT LIMITEM

V nejrůznějších debatách na téma společenské odpovědnosti často postrádám další, dle mého velmi důležitý pilíř, totiž lidskost a vzájemné pochopení.

V bezpečnostních službách dnes pracuje stále více lidí se zdravotním hendikepem. Pokud jim zaměstnavatel ve spolupráci s klientem zajistí odpovídající pracovní prostředí a vhodnou pracovní náplň, ani výrazné zdravotní omezení nemusí být překážkou. Důkazem toho je příběh paní Dany.

Ve 13 letech spadla ze stromu a poranila si páteř. Od té doby se pohybuje na invalidním vozíku. Přesto se dokázala vyučit zlatnicí, vyzkoušela si práci montážní dělnice i zaměstnání na call centru – to je vzhledem k jejímu hendikepu obdivuhodné.

Dnes je už několik měsíců součástí týmu IBIS GROUP. Díky pochopení svých nadřízených, zejména paní Ilony Ganibegovičové a pana Petra Jaroše, díky vstřícnosti Ascorium Mladá Boleslav, konkrétně pana Pavla Mudry a pana ředitele Pavla Vokurky, našla stabilní zaměstnání. Pracuje sice na zkrácený úvazek, ale je platným a přínosným členem týmu.

Paní Dana říká: „Když opravdu chcete, vyrovnáte se s každou překážkou." A dokazuje to nejen svou pracovní pílí, ale i tím, že je šťastnou maminkou pětiletého syna.

Mám pocit, že v honbě za ukazateli všeho druhu na tu již zmiňovanou lidskost a pochopení občas zapomínáme.

Tímto článkem chci povzbudit všechny, kteří v životě neměli jen samé štěstí, zároveň bych si ale přál, aby se stal rovněž inspirací pro zaměstnavatele.

Ing. Jiří Giptner

DETEKTIVNÍ OCHRANA SPORTOVNÍCH, KULTURNÍCH A SPOLEČENSKÝCH AKCÍ

OCHRANA MĚKKÝCH CÍLŮ

Před započetím realizace detektivního průzkumu je třeba vytěžit a získat informace z otevřených zdrojů. To umožňuje přistoupit k vlastnímu průzkumu se znalostí věci.

Za otevřené zdroje informací považujeme všechny typy veřejných médií, jako jsou rozhlas, televize, internet (ANOPRES, ČTK apod.). Všechny tyto zdroje nám mohou poskytnout relevantní informace, ale také informace zkreslené či dezinformace. Patří sem ať již volně dostupné nebo placené databáze, rejstříky, evidence apod.

Je třeba si uvědomit, že činnost detektiva v závadovém prostředí je rizikovou záležitostí. Proto je nutné připravit vhodnou a kvalitní legendu, která detektiva či detektiva-zpravodajce kryje a chrání před napadením ze strany členů závadové skupiny.

Detektivní průzkum v souvislosti se sportovními, kulturními nebo společenskými akcemi se realizuje:

Před konáním zmíněných akcí

Se zaměřením na vytipování případných organizátorů a potencionálních účastníků narušování režimových, organizačních akcí a případných výtržností, kdy tyto jsou připravovány v souvislosti s konáním akce.

V rámci konání zmíněných akcí

Se zaměřeném na vytipování narušitelů organizačních a režimových opatření a výtržníků. V případě, že již k narušení či výtržnosti dojde, dokumentování organizátorů a dalších účastníků nepokojů.

Po skončení zmíněných akcí

Stejně jako v průběhu akce, tak i po skončení akce je třeba dokumentovat pokračující narušování bezpečnosti a veřejného pořádku.

Detektiv či detektiv-zpravodajec se pro realizaci detektivního průzkumu v rámci zajišťování bezpečnosti a veřejného pořádku v souvislosti se sportovními, kulturními nebo společenskými akcemi infiltruje do předpokládaného závadového prostředí (například mezi fotbalové fanoušky fotbalového klubu, s nímž se má konat utkání). K této infiltraci může dojít před konáním akce, v rámci konání akce, případně i po jejím skončení.

Metody detektivní práce:

a) Osobní pátrání jako základ detektivního průzkumu

Detektivní průzkum začíná zpravidla realizací metody detektivního osobního pátrání. V rámci prováděného detektivního průzkumu je detektivní osobní pátrání velmi významnou metodou. Pomocí ní provádí detektiv průzkum zájmového prostředí, získává potřebný přehled o situaci a potřebné informace o probíhajícím dění, získává osobní a místní znalost. Pozor! Tuto metodu nelze zaměňovat s formou otevřeného detektivního pátrání. Svou činnost kryje legendou a mnohdy i dezinformacemi.

V průběhu detektivního průzkumu detektiv-zpravodajec využívá i dalších metod, například metody detektivního pozorování apod.

b) Detektivní vytěžování jako součást osobního pátrání v rámci detektivního průzkumu

Na detektivní osobní pátrání, v jehož rámci detektiv získá osobní a místní znalost a další bezpečnostní informace, navazuje zpravidla metoda detektivního vytěžování.

Vytěžování provádí detektiv s využitím detektivní legendy, aby zajistil své vlastní krytí v závadovém prostředí a aby zakryl svůj zájem, jehož cílem je získat informace o připravovaných výtržnostech, jejich organizátorech a osobách, které se výtržností na sportovní, kulturní nebo společenské akci mají zúčastnit. Vytěžování provádí případně již v průběhu sportovní, kulturní nebo společenské akce, kdy k jejímu narušování dochází, zjišťuje, kdo se případných výtržností účastní a kdo je organizuje. Při vytěžování se detektiv zaměřuje na osoby:

- které mohou poskytnout informace o potencionálních organizátorech či potencionálních účastnících, narušitelích veřejného pořádku a bezpečnosti, o režimových, organizačních a dalších bezpečnostních opatřeních;
- které představují potencionální účastníky narušování veřejného pořádku a bezpečnosti – zde detektiv či detektiv-zpravodajec, krytý vhodnou legendou, může využívat i detektivní zpravodajskou metodu dez-

1

2

informace, s cílem rozložit závadovou skupinu narušitelů, narušit její jednotu;

- které jsou potencionálními organizátory narušování veřejného pořádku a bezpečnosti; zde je perfektní neprůstřelná legenda ke krytí detektiva či detektiva-zpravodajce a jeho zájmu obzvlášť důležitá; v těchto případech jsou v rámci vytěžování zpravidla infiltrovány dezinformace.

c) Využití metody informačního proniknutí v procesu realizace detektivního průzkumu

V případě, že se jedná o opakované sportovní (např. riziková fotbalová utkání), kulturní nebo společenské akce, je vhodné v závadovém prostředí (prostředí, z něhož se rekrutují narušitelé těchto akcí) vybudovat lidské informační zdroje. Jde o metodu detektivního informačního proniknutí, jejímž cílem je infiltrovat informátora především mezi organizátory. To pak umožňuje získat relevantní kvalitní informace k připravovaným narušením veřejného pořádku a bezpečnosti těchto akcí. Informace jsou tak získávány s jistým předstihem, což umožňuje připravit potřebná bezpečnostní opatření. Získat informátora (lidský informační zdroj) je však záležitost dlouhodobější a účelná zejména při opakujících se akcích.

Lidské informační zdroje (informátory) je v těchto případech vhodné budovat jako poziční, tedy přímo v prostředí závadové skupiny (např. fanoušků tropících výtržnosti) a na delší dobu.

d) Dokumentování informací, informací o důkazech a důkazů z procesu detektivního průzkumu

V průběhu celého detektivního průzkumu je důležité dokumentovat získané informace a v řadě případů je i legalizovat. Přichází v úvahu především:

- audiodokumentace
- fotodokumentace
- videodokumentace

V současné době pro všechny tyto druhy dokumentace může posloužit mobilní telefon. Důležité je přitom zabezpečit ve vhodný okamžik odeslání zadokumentovaných informací na svůj počítač umístěný mimo prostor průzkumu a mimo možný dosah některé osoby závadové skupiny, případně na chráněný počítač detektivní kanceláře. Jde o to, aby se zadokumentované informace nedostaly do rukou kterékoliv osoby závadové skupiny.

e) Třídění a analýza informací, informací o důkazech a důkazů z procesu detektivního průzkumu

Třídění informací o důkazech a důkazů a jejich následná analýza prolíná celým procesem detektivního průzkumu. Třídění a analýzu můžeme rozdělit na:

- **počáteční** – jedná se o třídění a analýzu informací získaných z otevřených zdrojů;
- **průběžnou** – jde o třídění a analýzu informací, informací o důkazech a důkazů probíhající de facto nepřetržitě, v celém průběhu detektivního průzkumu;
- **závěrečnou** – jde již o vysoce kvalifikované třídění a vysoce odborně prováděnou analýzu po skočení detektivního průzkumu, s cílem získat z množiny informací, informací o důkazech a důkazů relevantní informace v podobě závěrečné zprávy, ať už ústní nebo písemné, doprovázené případně audiodokumentací, fotodokumentací či videodokumentací.

Jedná se o bezpečnostní analýzu[3], která představuje základní bezpečnostní činnost. Její výsledky jsou základním a nezbytným předpokladem následné bezpečnostní prognózy – předpokládaného vývoje průběhu sportovní, kulturní nebo společenské akce.

Analýza představuje techniku a metodu sloužící k získání relevantních informací – poznatků k dané problematice. To, co bezpečnostní analýzu vymezuje a specifikuje, je problém formulovaný vymezeným cílem, jehož má být dosaženo.

f) Bezpečnostní prognóza[4] vývoje průběhu sportovní, kulturní nebo společenské akce

Prognóza průběhu a vývoje sportovní, kulturní nebo společenské akce je výsledným produktem detektivního průzkumu.

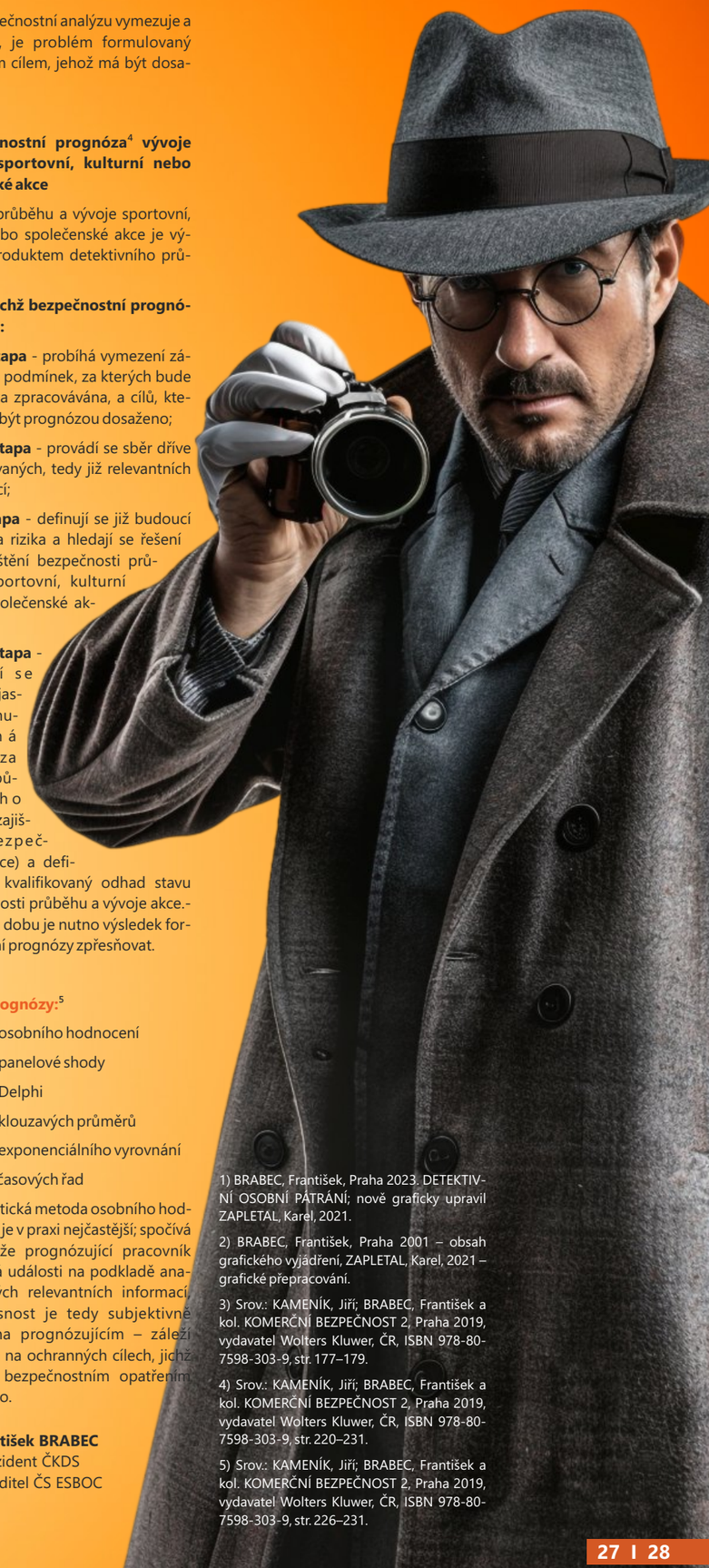
Etapy, v nichž bezpečnostní prognóza probíhá:

- **první etapa** - probíhá vymezení základních podmínek, za kterých bude prognóza zpracovávána, a cílů, kterých má být prognózou dosaženo;
- **druhá etapa** - provádí se sběr dříve analyzovaných, tedy již relevantních informací;
- **třetí etapa** - definují se již budoucí hrozby a rizika a hledají se řešení pro zajištění bezpečnosti průběhu sportovní, kulturní nebo společenské akce.
- **čtvrtá etapa** - vytváří se vlastní, jasně formulovaná prognóza podle původního zadání (zajištění bezpečnosti akce) a definuje se kvalifikovaný odhad stavu bezpečnosti průběhu a vývoje akce.- Po celou dobu je nutno výsledek formulování prognózy zpřesňovat.

Metody prognózy:[5]

- metoda osobního hodnocení
- metoda panelové shody
- metoda Delphi
- metoda klouzavých průměrů
- metoda exponenciálního vyrovnání
- modely časových řad
- prognostická metoda osobního hodnocení – je v praxi nejčastější; spočívá v tom, že prognózující pracovník předvídá události na podkladě analyzovaných relevantních informací, její přesnost je tedy subjektivně ovlivněna prognózujícím – záleží zejména na ochranných cílech, jichž má být bezpečnostním opatřením dosaženo.

JUDr. František BRABEC
čestný prezident ČKDS
výkonný ředitel ČS ESBOC



1) BRABEC, František, Praha 2023. DETEKTIVNÍ OSOBNÍ PÁTRÁNÍ; nově graficky upravil ZAPLETAL, Karel, 2021.

2) BRABEC, František, Praha 2001 – obsah grafického vyjádření, ZAPLETAL, Karel, 2021 – grafické přepracování.

3) Srov.: KAMENÍK, Jiří; BRABEC, František a kol. KOMERČNÍ BEZPEČNOST 2, Praha 2019, vydavatel Wolters Kluwer, ČR, ISBN 978-80-7598-303-9, str. 177–179.

4) Srov.: KAMENÍK, Jiří; BRABEC, František a kol. KOMERČNÍ BEZPEČNOST 2, Praha 2019, vydavatel Wolters Kluwer, ČR, ISBN 978-80-7598-303-9, str. 220–231.

5) Srov.: KAMENÍK, Jiří; BRABEC, František a kol. KOMERČNÍ BEZPEČNOST 2, Praha 2019, vydavatel Wolters Kluwer, ČR, ISBN 978-80-7598-303-9, str. 226–231.

DO OLOMOUCE SE OPĚT SJEDOU ČEŠTÍ, POLŠTÍ A SLOVENŠTÍ STRÁŽNÍCI

PRAVIDELNĚ SE ZDE KONÁ JEJICH NEJVĚTŠÍ STŘEDOEVROPSKÉ SETKÁNÍ

Již IX. Mezinárodní konference obecních policií se uskuteční ve dnech 26. – 28. 3. 2025 na Právnické fakultě Univerzity Palackého v Olomouci. Ojedinělé a největší mezinárodní setkání obecních a městských policií ve střední Evropě bude ve znamení řady novinek a radikálních programových změn.

Podle hlavního organizátora, společnosti FT Technologies, určitě zůstane zachován koncept dvou konferenčních dnů, kterým bude předcházet neformální uvítací večeře. Také se uskuteční tradiční doprovodné aktivity, tedy středeční pracovní setkání zástupců profesních organizací českých a slovenských strážníků, nebo čtvrteční doprovodný program určený rovněž pro širokou veřejnost, v němž dostává prostor neziskový sektor a dobrovolnické aktivity.

„Upustili jsme ale od tradičního večerního doprovodného programu v závěru prvního konferenčního dne. Není tajemstvím, že místo něj připravujeme pozměněnou podobu neformálního setkání, abychom ještě více zdůraznili určitý status společenské události, kterou naše konference má. Ale především, zásadní změny dozná samotný koncept denního programu," podotýká manažer konference Pavel Boháč. Hodlají se ještě více zaměřit na konkrétní témata, která rezonují ve společnosti, trápí obce a města, respektive ty, kteří dohlíží na bezpečnost ve veřejném prostoru, tedy strážníky obecních a městských policií. V programu konference, který již nebude rozdělen na dosavadní programové bloky, se tak pilotně hned dvakrát objeví nová diskuzní a prezentační platforma nazvaná „ÚHEL POHLEDU".

„Spočívá v moderátorkou řízené diskusi několika odborníků z různých institucí na konkrétní téma, kteří se k němu budou vyjadřovat ze své odbornosti, reagovat na své diskusní kolegy, popřípadě názory a dotazy z auditoria," vysvětluje Boháč. Podle něj lze očekávat, že zazní různé postřehy, možná i odlišné názory, tedy se potvrdí fakt, že lze na danou problematiku nahlížet z různých úhlů pohledu. „Ten formát debaty se nám osvědčil u našeho Expert Dialogu, zkusíme tedy některé jeho prvky přenést do programu konference," doplňuje s vírou, že auditorium takováto výjimečná debata zaujme a program obohatí.

Také proto si organizátoři dali obzvláště záležet při hledání témat a především těch, kteří by k nim mohli poutavě hovořit. Jedním z témat bude „psychosociální klima ve společnosti" v kontextu psychické odolnosti populace, nárůstu agrese, sociálně patologických jevů a z toho plynoucích důsledků na bezpečnost ve veřejném prostoru. Tím druhým pak „bezdomovectví, sociální izolace a vyloučení" v kontextu práce s lidmi bez domova, problematiky sociálního bydlení, programů v sociálně vyloučených lokalitách, rizik spojených se zhoršující se ekonomickou situací, kumulace agenturních zaměstnanců v některých regionech a z toho všeho plynoucích důsledků zhoršení bezpečnosti situace. Podle Boháče to však neznamená, že by zcela upustili od tradičních formátů přednášek a prezentací, i ty dostanou svůj prostor. „Posluchači se tak mohou těšit na vlastní prezentace strážníků a jejich zkušeností. Zajímavé určitě budou postřehy z povodní, vzájemného vzdělávání, práce s lidmi bez domova či realizací preventivních programů pro různé věkové kategorie," vyjmenovává jen některé z nich. Je tak zřejmé, že se opět podaří vytvořit v programu zajímavý a výjimečný mix přednášek a přednášejících.

„Kdo se účastní naší konference pravidelně, jistě zaregistroval, že roste počet institucí, které se na programu podílí. Stále přitom zůstává zachován již zmíněný akcent na prezentace obecních a městských policií a v neposlední řadě zde máme aktivity, které činí naši konferenci v jistém ohledu výjimečnou," shrnuje dosavadní programové schéma Boháč s dovětkem, že díky avizovaným změnám by se počet vystupujících měl ještě navýšit. Jako vždy, detailní program bude publikován počátkem března na konferenčních stránkách.

V kombinaci s tradičním nadstandardním konferenčním servisem a nezapomenutelnou atmosférou, kterou každoročně toto mezinárodní setkání provází, a snad tomu bude i tentokrát, se dá očekávat, že půjde opět o vydařený ročník. Navíc organizátoři věří, že tak jako v uplynulých letech se ještě před plánovaným ukončením registrace na konferenci naplní kapacita auditoria stanovená na 250 účastníků. „Takže rozhodně není vhodné s přihlášením na konferenci otálet," uzavírá Boháč.

IX. Mezinárodní konference obecních policií (26. - 28. 3. 2025, Olomouc) je ojedinělé a největší mezinárodní setkání obecních a městských policií ve střední Evropě. Jedná se nejen o společenskou událost, ale především o ojedinělou platformu pro osobní setkávání a výměnu zkušeností. Její součástí je také bohatý doprovodný program. Auditorium tvoří nejen zástupci obecních a městských policií, ale také statní správy, samospráv, integrovaného záchranného systému a bezpečnostních sborů, exekutivy, akademické sféry a dalších subjektů a organizací včetně neziskového sektoru a dobrovolnických aktivit. Hlavním organizátorem je společnost FT Technologies a.s., která je považována za středoevropského lídra trhu v oblasti poskytování informačních technologií pro obecní a městské policie. Spoluorganizátorem je Právnická fakulta Univerzity Palackého Olomouc. Hlavním partnerem je společnost Hedurio s.r.o. Konferenci podporují profesní organizace strážníků z České republiky, Slovenska a Polska. Významná je podpora ze strany Ministerstva vnitra České republiky, Ministerstva vnitra Slovenské republiky, Olomouckého kraje a statutárního města Olomouc, přičemž na zdárné realizaci spolupracuje a konferenci podporuje řada dalších subjektů a partnerů. Jedním z nich je od roku 2018 také **časopis Bezpečnost s profesionály – mediální partner konference.**