



KPKB
KOMORA
PODNIKŮ
KOMERČNÍ
BEZPEČNOSTI
ČESKÉ REPUBLIKY

ČASOPIS KOMORY PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČR

1/2024

BEZPEČNOST

S PROFESIONÁLY

KONFERENCE OCHRANA MĚKKÝCH CÍLŮ

PROJEKTY K OCHRANĚ MĚKKÝCH CÍLŮ

KRIZOVÝ INFORMAČNÍ A SVOLÁVACÍ SYSTÉM KISS

ŘÍDICÍ A DOHLEDOVÁ CENTRA

ISSN 2336-4793



9 772336 479003

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 Vegrichová, Ph.D., MBA

Inzerce

sekretariat@kpkbcr.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

Autorská práva vykonává vydavatel, užití celku nebo částí, rozmnožování a šíření jakýmkoli způsobem je bez výslovného souhlasu vydavatele zakázáno.

Na zadních stranách obálky

členové KPKB ČR



ÚVODNÍ SLOVO

Vážení čtenáři,

dovolujeme si Vám představit další letošní číslo našeho časopisu Bezpečnost s profesionály, které je i tentokrát bohaté na řadu zajímavých odborných článků.

Především Vás ale chci pozvat na již osmý ročník naší tradiční konference Ochrana měkkých cílů 2024, která se letos uskuteční opět v kongresovém sále pražského hotelu Olšanka, a to 13. června 2024. Konferenci připravujeme s našimi partnery – asociací kyberbezpečnosti Afcea a Fakultou biomedicínského inženýrství ČVUT.

Tento rok jsme velmi potěšeni velkým zájmem o tuto prestižní akci, který je nepochybně odrazem zvýšené celospolečenské poptávky po bezpečnostních tématech, a to nejen tématu ochrany měkkých cílů. Velmi nás těší i podpora formou záštiti ze strany Hospodářské komory České republiky a jejího prezidenta Mgr. Zdeňka Zajíčka, Asociace krajů České republiky jménem jejího předsedy MUDr. Martina Kuby, záštiti předsedy Bezpečnostního výboru Poslanecké sněmovny parlamentu ČR pana PhDr. Pavla Žáčka, Ph.D., poslance Roberta Králíčka, předsedy Podvýboru pro Policii české republiky, obecní policie a bezpečnostní služby, a ředitele sekce komunikačních a informačních systémů Ministerstva obrany brigádního generála Ing. Petra Šnajdárka.

Účast na konferenci potvrdila řada zástupců firem a institucí zabývajících se bezpečnostní problematikou, a to jak z pozice návštěvníků posluchačů, tak aktivních účastníků, přednášejících na různá témata. Prezentovat se budou i členské firmy z KPKB ČR, se zaměřením na bezpečnostní technologie. Na konferenci bude distribuován i náš časopis Bezpečnost s profesionály. Jsme potěšeni, že tímto způsobem můžeme pomoci propagaci našich členů.

Více informací najdete na konferenčním webu www.ochranamekkychcilu.eu.

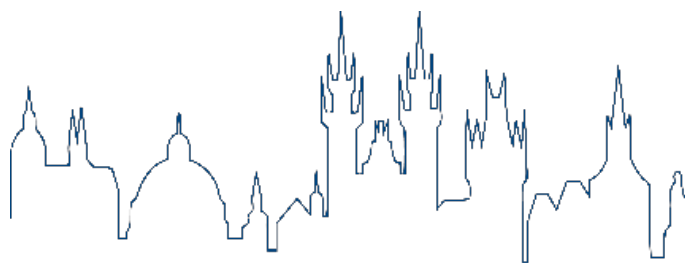
V nadcházejícím období nás čeká řada dalších aktuálních výzev souvisejících s problematikou bezpečnosti. Jsme však v Komoře přesvědčení, že se se všemi vypořádáme se ctí a ke spokojenosti všech zainteresovaných stran.

Do dalších měsíců Vám přeji hodně inspirativních zážitků, pracovních úspěchů i spokojenosti v osobním životě.

Ing. Václav Jahodář
prezident KPKB ČR

OBSAH

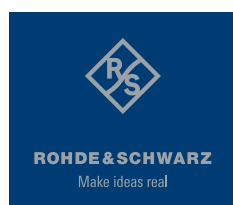
Ochrana měkkých cílů pozdávka	3
Projekty k ochraně měkkých cílů	4–6
Krizový informační a svolávací systém KISS	7–8
TEMPEST nezanedbávejte „blind spot“	9
Řídicí a dohledová centra klíčový pilíř každé společnosti	10
Dispečerská pracoviště Nowatron Elektronik, spol. s r.o.	11
Termokamery Hikvision jejich nepostradatelné využití v průmyslu	12–13
Budoucnost managementu v segmentu komerční bezpečnosti	14–15
Představení odborné publikace Dávida Dóményho	16
Bezpečnostní systém s mlhou	17–20
Reakce nebezpečnostního personálu	21
Setkání strážníků obecních policí ze střední Evropy v Olomouci	22–23
Psychologie výslechu dětí několik poznámek	24–25
Kroužek „Mladý strážník“ a další činnosti na poli prevence	26
Ochrana měkkých cílů detektivní ochrana sportovních a kulturních akcí	27–30
Hasičský záchranný sbor DPP návštěva Depa Hostivař	31



OCHRANA MĚKKÝCH CÍLŮ KONFERENCE

konference Ochrana měkkých cílů 2024

13. června 2024, Hotel Olšanka Praha



MBI

MEZINÁRODNÍ
BEZPEČNOSTNÍ
INSTITUT

NOWATRON®
ELEKTRONIK

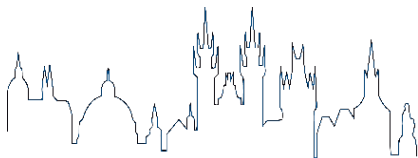
HIKVISION®

AXIS®
COMMUNICATIONS

VDT technology



www.ochranamekkychcilu.eu



PROGRAM

konference Ochrana měkkých cílů 2024

13. června 2024, Hotel Olšanka Praha

9:00 – 9:18

Slavnostní zahájení konference

BLOK 1 - PREVENCE

- řešení, koncepty, praxe

9:18 – 10:27

Mgr. Dalibor Smažinka
(Axis Communications, s.r.o.)

**Současná analýza obrazu a zvuku
v dohledovém systému**

Mgr. Filip Gundza
(Mezinárodní bezpečnostní institut, z.ú.)
Významné stavby: požární vs. bezpečnostní evakuace

Mgr. Veronika Fáberová
(Doverville, s.r.o.)

Těžko na cvičišti...aneb když se management přestane jen spoléhat a sám si vyzkouší, zda skutečně umí

Jaromír Průša (ASIS CZ, z.s.)
Útok na obchodní centrum - případová studie, doporučení pro oblast prevence

PŘESTÁVKA

BLOK 1A - PREVENCE

- metodika, standardy a regulace

10:42 – 11:49

pplk. prof. JUDr. Jana Šimonová, PhD
(Akademie Policejního sboru v Bratislavě)

Ochrana měkkých cílů na Slovensku: strategie, záměry a projekty

doc. Mgr. Oldřich Krulík, Ph.D.
(AMBIS vysoká škola, a.s.)
Dotační Program prevence kriminality: Projekty k ochraně měkkých cílů

Mgr. Robert Šťastný (Městský úřad Lysá nad Labem)
Teritoriální obrana jako efektivní pomocník při ochraně měkkých cílů

Mgr. et Mgr. Pavel Krčílek, Dis.
(Praha 11)

Měkké cíle pod ochranou aneb komparace bezpečnostních přístupů ČR a Velké Británie

brig. gen. Ing. Petr Šnajdárek
(Ministerstvo obrany ČR)
Platforma pro civilně vojenskou spolupráci pro zvládání krizí nevojenského a vojenského ohrožení

SPECIÁLNÍ HOSTÉ

11:49 – 12:27

Mgr. Josef Šlerka, Ph.D.
(Univerzita Karlova)
Deepfakes ve videoobsahu jako bezpečnostní hrozba

Mgr. Kateřina Lesch, Ph.D.
(EmbedIT s.r.o.)
Multimédia nejsou všechno – rozpoznávání deepfakes v textovém obsahu

OBĚD

BLOK 2 - DETEKCE - technika a lidé

13:24 – 14:45

Daniel Rážek (HIKVISION Czech s.r.o.)
Kamerové systémy v roli inteligentních detektorů

Petr Barták
(Nowatron Elektronik spol. s r.o.)
Dispečinky, velíny a dohledová centra a jejich význam pro bezchybnou detekci

Dr. Ing. Pavel Kotyk
(ROHDE & SCHWARZ – Praha, s.r.o.)
Průchodové 3D skenery – revoluce v kontrole osob

Ing. Jan Burian
(SAFE Technology SAFETE, s.r.o.)
Automatizované systémy pro distribuci varování a informací při mimořádné události

Dr. Ing. Pavel Kotyk
(ROHDE & SCHWARZ – Praha, s.r.o.)
Kybernetická bezpečnost v kontextu ochrany měkkých cílů – případová studie

PŘESTÁVKA

BLOK 3 - REAKCE VČETNĚ KAZUISTIKY A PŘÍPADOVÝCH PREZENTACÍ

15:00 – 16:26

mjr. Ing. Zdeněk Orel (Policie ČR)
Složky IZS na místě násilného útoku na měkký cíl

Ing. Václav Fišer
(ZZS Jihomoravského kraje)
Připravenost zdravotnictví... černá labuť bezpečnosti?

PhDr. Martin Klika, MBA DBA
(Městská policie Litvínov)
Činnosti a význam městské a obecní policie při ochraně měkkých cílů

Mgr. David Rožek, MBA (Synergia)
Zaměstnanec měkkého cíle - přírodní first responder

Panelová diskuze

16:26 – 16:36

Závěrečná slova

Dotazy pro vystupující můžete pokládat v systému sli.do. Stačí naskenovat tento QR kód.



Vaše zpětná vazba je pro nás důležitá. Prosíme o vyplnění krátkého dotazníku.



Změna programu vyhrazena.

REAKCE NEBEZPEČNOSTNÍHO PERSONÁLU

V souladu s metodou DDRM (Deter, Detect React, Mitigate) se v bezpečnostní komunitě obvykle převážně zabýváme nastavením procesů pro bezpečnostní pracovníky, nejružnější reakční týmy, výjezdové skupiny PCO a další, řekněme více či méně bezpečnostně zainteresované osoby s rozličnou kvalifikací i zkušenostmi.

U všech výše zmíněných subjektů předpokládáme, že mají osvojené základní obecné bezpečnostní postupy, návyky a že krizové situace dokáží odbavit převážně profesionálně. Pokud jsou takoví pracovníci přítomni při vzniku krizové události, očekává se od nich, že budou reagovat jako první, předpokládá se jejich iniciativa a vedení ostatních přítomných zaměstnanců nebo náhodně přítomných osob. Jak už je ale obvyklé, při vzniku krizových událostí bývá člověk, který je odborně proškolený a kompetentní reagovat, málokdy nablízku.

V případě vzniku krizové události na pracovišti s veřejným přístupem – v typickém měkkém cíli, kde jsou přítomni i osoby z řad širší veřejnosti – se očekává, že je to právě personál, který by měl v případě nepřítomnosti profesionálů zareagovat na vzniklou krizi jako první. Personál, který můžeme označit termínem „nebezpečnostní“ (není v oblasti bezpečnosti profesionálem). Očekává se primárně jeho iniciativa, okamžitá reakce na situaci a řízení nutných činností. V lidech je podvědomě zakořeněno vnímání odpovědnosti druhých za svěřený provoz. Nelze tudíž při koncepci bezpečnostních opatření pominout žádné zaměstnance, kteří se pohybují ve veřejné zóně, jsou apriori v kontaktu s veřejností a statisticky jsou tak často první, kteří se s krizovou událostí setkají.

Řeč je o zaměstnancích či pověřených osobách (nebezpečnostních pracovnících), jejichž primárním úkolem a pracovní povinností není řešení krizových situací, přesto je třeba, aby byli na takové situace připraveni. Analogicky můžeme tuto skutečnost srovnat se schopností poskytnutí první pomoci, kdy se očekává, že ji může poskytnout

kdokoli, aniž by musel být školeným zdravotníkem, natož záchranářem či lékařem. Srovnání snese tento ilustrativní příklad i v očekáváních. Jak v případě poskytnutí první pomoci, tak v případě ochrany bezpečnosti jde primárně o zjištění základní definice a atributů nastalé situace – o prvotní rozhodnutí, které zabrání pokračování škodlivého následku či jeho eskalaci, potažmo vzniku dalších škod. Krizové situace vyžadují, pokud možno, zapojení okolních osob do spolupráce, rychlý kontakt s profesionály, aktivaci bezpečnostních opatření a následnou spolupráci s IZS.

Jak při první pomoci, tak při ochraně ohrožené bezpečnosti jde cca o prvních 20 minut, ne-li dobu kratší (v závislosti na nastavených bezpečnostních postupech), v níž je třeba situaci základem odbavit s cílem zabránit jejímu zhoršení, eskalaci, případně vzniku dalších škod. Podmínkou přípravy pracovníků na krizovou situaci je, že se musí jednat o soubor obecně použitelných a současně jednoduchých pravidel, která není obtížné pochopit a realizovat.

Nelze se však spoléhat jen na teorii. Současně je třeba krizové situace důkladně cvičit na modelových situacích. Takové cvičení je i z didaktického hlediska mnohem účinnější než pouhá teorie. Pro další zvýšení přirozenosti i zájmu pracovníků je dobré takové cvičení modelovat na scénáře, které jsou realistické pro konkrétní pracovní prostředí a vycházejí nejen ze zkušeností dotyčných pracovníků, ale i například z analýzy rizik. Současně je velmi přínosné, když se reálné cvičení uskutečňuje přímo v prostorách pracoviště a za okolností, které jsou realistické, neboť tak si účastníci školení dokáží

snadněji osvojit popisované návyky. A také pro lektora bude snazší popisovat přímo na pracovišti u konkrétních situací, jak účelně využít a skloubit znalosti, dostupný materiál, pomůcky a typologii prostor.

Součástí bezpečnostních opatření bývají v dnešní době jednoduché definice kategorií zaměstnanců, u kterých je definováno, jak často a jak intenzivní školení mají na konkrétních pracovištích absolvovat. Je však třeba mít na paměti, že školení je jedním, nikoli jediným nástrojem, jak začleňovat nebezpečnostní personál do řešení krizí.

Dalšími aspekty jsou prevence, možnost sdílet chyby i úspěchy při řešení bezpečnostních událostí, pravidelné seznamování pracovníků s přijatými a měněnými opatřeními a požadavky na jejich reakci na provozní úrovni. Důležité je pak být pracovníkům k dispozici na denní bázi, vnímat jejich podněty, dotazy a připomínky a reagovat na ně.

Pouze souborem takto přijatých opatření a dodržováním zásady jednoduchosti lze dosáhnout vyššího bezpečnostního povědomí u všech nebezpečnostních pracovníků a udržet jejich zájem o téma bezpečnosti a bezpečnostních postupů.

Mgr. David Rožek, CPP®

Company representative
Certified Protection Professional
Board Certified in Security Management

PROJEKTY K OCHRANĚ MĚKKÝCH CÍLŮ

JAKO SOUČÁST DOTAČNÍHO PROGRAMU PREVENCE KRIMINALITY V ČESKÉ REPUBLICE PRO ROKY 2018–2022

Jedná se o výstup, vypracovaný pro potřeby projektu (veřejné zakázky) „Měření úspěšnosti programů a projektů prevence kriminality“ [VC20232026014], realizovaného v rámci „Programu bezpečnostního výzkumu pro potřeby státu 2022–2027“.

Mezi lety 2018 až 2022 bylo v rámci dotačního Programu prevence kriminality v České republice podáno celkem 11 projektů týkajících se problematiky ochrany měkkých cílů. Všechny tyto žádosti uspěly, což svědčí o dů-

ležitosti uvedené problematiky, nejen optikou Ministerstva vnitra České republiky. Příjemci podpory byly u tohoto typu projektů vždy kraj nebo krajské město. V rámci příspěvku je sledováno, jaké bylo konkrétní zaměření někte-

rých těchto projektů a jejich praktické dopady. Sledován je i způsob, kterým byly související výsledky prezentovány a zda v této souvislosti došlo k nějaké širší využitelné odezvě.

Rok	Žadatel	Název projektu	Přidělená dotace
2018	Středočeský kraj	Středočeský kraj – Ozbrojený útočník ve škole	352 000 Kč
2018	Středočeský kraj	Středočeský kraj – Informační a vzdělávací kampaň na ochranu měkkých cílů	390 000 Kč
2018	Liberecký kraj	Liberecký kraj – Informační a vzdělávací kampaň na ochranu měkkých cílů pro rok 2018	150 000 Kč
2018	Pardubický kraj	Pardubický kraj – Informační a vzdělávací kampaň na ochranu měkkých cílů pro rok 2018	57 000 Kč
2018	Jihočeský kraj	Jihočeský kraj – Informační kampaň k ochraně měkkých cílů	240 000 Kč
2018	Jihočeský kraj	Jihočeský kraj – Ozbrojený útočník ve škole, III. – závěrečná etapa	735 000 Kč
2018	Olomoucký kraj	Olomoucký kraj – Informační a vzdělávací kampaň k ochraně měkkých cílů	150 000 Kč
2018	Plzeň	Plzeň – Informační kampaň na ochranu měkkých cílů pro rok 2018	30 000 Kč
2018	Karlovarský kraj	Karlovarský kraj – Informační a vzdělávací kampaň k ochraně měkkých cílů	120 000 Kč
2018	Ostrava	Ostrava – Informační seminář k problematice měkkých cílů	30 000 Kč
2022	Plzeň	Plzeň – Nasazení SED: detektorů střelby, panických výkřiků a tříštění skla – 2022	550 000 Kč

Přehled projektů týkajících se ochrany měkkých cílů, podpořených mezi lety 2018 až 2022 prostředky z dotačního Programu prevence kriminality v České republice.

Z přehledu je zřejmé, že ve sledovaném období byl nejvíce významný rok 2018, nicméně projekty tohoto druhu začaly být aktuální již daleko dříve, přinejmenším po tragickém útoku ve škole ve Žďáru nad Sázavou v říjnu 2014. U některých žadatelů se tak jednalo o pokračování starších aktivit. V konkrétních případech byla aktivita rozdělena na problematiku ochrany školských za-

řízení a ochranu „ostatních“ typů měkkých cílů (míst velké koncentrace osob). Další aktivity pak probíhají mimo dotační systém prevence kriminality nebo se týkají let 2023 a 2024, proto je tento přehled nepostihuje. Problematika přitom byla, respektive je do určité míry tradiční náplní činnosti některých společností, delší dobu se specializujících na poradenství v oblasti

ochrany míst velké koncentrace osob (Doverville, F.S.C. – Bezpečnostní poradenství, případně dalších), které své zapojení do projektů na úrovni krajů nebo krajských měst vnímají jako sítěžejní referenci pro své další podnikání.

Středočeský kraj – Informační a vzdělávací kampaň na ochranu měkkých cílů, 2018

Středočeský kraj realizoval projekt v roce 2018 ve spolupráci s Krajským ředitelstvím policie Středočeského kraje a Vzdělávacím institutem Středočeského kraje. V pozici přednášejících byli experti z Krajského úřadu, ale i Ministerstva vnitra České republiky a Asociace bezpečná škola. V průběhu přednášek, kterých bylo celkem 13 (viz Harmonogram akcí Středočeského

kraje), zazněly i zmínky o útocích v zahraničí. Tyto zkušenosti pak byly využity ve formě doporučení a instruktážních videí, včetně konceptu „Uteč – Skryj se – Bojuj“. Nechybělo ani seznámení s normou ČSN 73 44 00 / Prevence kriminality – řízení bezpečnosti při plánování, realizaci a užívání škol a školských zařízení a s bezpečnostními audity dle této normy.

Semináře byly určeny především pro zástupce samospráv, zástupce zřizovatelů a personál škol a školských zařízení, správce budov a veřejných prostranství, organizátory akcí pořádaných na veřejných prostranstvích, policisty, strážníky a zástupce dalších složek integrovaného záchranného systému.

Termín	Místo	Tematické zaměření
10. 9. 2018	Praha (budova krajského úřadu)	Povědomí o ochraně měkkých cílů, její důležitosti a smyslu
17. 9. 2018	Benešov	Úvod do problematiky ochrany měkkých cílů
18. 9. 2018	Nymburk	Úvod do problematiky ochrany měkkých cílů
20. 9. 2018	Rakovník	Úvod do problematiky ochrany měkkých cílů
1. 10. 2018	Mladá Boleslav	Pořádání kulturních, sportovních a dalších akcí
2. 10. 2018	Říčany	Úvod do problematiky ochrany měkkých cílů
4. 10. 2018	Příbram	Úvod do problematiky ochrany měkkých cílů
9. 10. 2018	Praha	Bezpečnostní analýza měkkého cíle
11. 10. 2018	Beroun	Úvod do problematiky ochrany měkkých cílů
16. 10. 2018	Praha	Pořádání kulturních, sportovních a dalších akcí
6. 11. 2018	Praha	Bezpečnost škol a školských zařízení
13. 11. 2018	Mělník	Veřejné budovy a veřejná prostranství
15. 11. 2018	Kladno	Pořádání kulturních, sportovních a dalších akcí

Harmonogram akcí Středočeského kraje, rok 2018.

Liberecký kraj – Informační a vzdělávací kampaň na ochranu měkkých cílů pro rok 2018 a navazující aktivity

Jádrem naplňování projektu byla pětice seminářů, konaných v multimediálním sále krajského úřadu v Liberci. Přednášky byly určeny především pro zástupce obcí, bezpečnostní manažery a manažery prevence kriminality, vedoucí a další pracovníky objektů označitelných jako měkké cíle, pro policisty a strážníky. Přednášejícími byli primárně experti ze společnosti Doverville, kladoucí dle vlastních vyjádření důraz na praktickou využitelnost sdělovaných poselství. Harmonogram akcí byl následující:

- Ochrana měkkých cílů – Úvodní informace, 24. IX. 2018.
- Ochrana měkkých cílů – Veřejné budovy a prostranství, 8. X. 2018
- Ochrana měkkých cílů – Eventová bezpečnost (pořádání kulturních, sportovních, společenských akcí), 15. X. 2018.
- Ochrana měkkých cílů – Specifika outdoorových eventů, 22. X. 2018.
- Vyhodnocení ohroženosti měkkého cíle (bezpečnostní analýza, určení priorit), 5. XI. 2018.

Nebyla to však zdaleka poslední činnost kraje ve sledované oblasti. V letech 2019 až 2021 využil kraj dotační titul Ministerstva vnitra České republiky „Ochrana a zabezpečení škol a školských zařízení jako měkkých cílů“. Z dotací bylo vynaloženo přibližně 3,5 milionu korun, zapojilo se 16 škol a školských zařízení zřizovaných Libereckým krajem. Vzděláváním prošlo přes 300 pedagogických i nepedagogických zaměstnanců.

Ve spolupráci s Policií České republiky probíhá v kraji dvakrát do roka cvičení na téma útok aktivního střelce (například na středních školách v Turnově, Frýdlantu, České Lípě a Jablonci nad Nisou).

Po skončení dotačního titulu uskutečnil krajský odbor školství vlastní projekt pro systematické proškolení dalších škol zřizovaných krajem, včetně metodických návodů k použití ve smyslu strategie „Uteč – Skryj se – Bojuj!“. Další součástí procesu je dotační program „Ochrana škol jako možných měkkých cílů“, který alokuje 5 milionů Kč na opatření vedoucí k větší bezpečnosti škol jako měkkých cílů, stanovení bezpečnostních priorit, vytvoření funkčního systému ochrany a nastavení prováděných bezpečnostních opatření.

Dotaci (do výše 50 % způsobilých výdajů, minimálně se jedná o 25 000 Kč, maximálně o 100 000 Kč) mohou využít obce jako zřizovatelé škol a také privátní sektor či církev zřizující základní školu. Prostředky mohou využít zřizovatelé i na vzdělávací a výcvikové akce pro pedagogické i nepedagogické pracovníky či na vytvoření metodických plánů.

V neposlední řadě se pak jedná, počínaje rokem 2024, o zpracování a revize bezpečnostních plánů škol a školských zařízení, teoretická školení, semináře pro zaměstnance a praktická cvičení se zaměřením na útok na měkký cíl. Dodavatelem těchto služeb (kdy cena nepřekročí 2 295 370 Kč) se stala opět společnost Doverville.

- Cílovou skupinou tohoto projektu jsou školy a školská zařízení zřizované Libereckým krajem (většina středních škol v regionu, pedagogicko-psychologické poradny, speciální pedagogická centra, dětské domovy a základní školy speciální).
- Pro rok 2024 bylo avizováno 20 nových bezpečnostních plánů a 10 revizí plánů stávajících. V plánu je na rok 2024 také 10 cvičení.

Projekt počítá rovněž se dvěma semináři a jedním rozsáhlým součinnostním cvičením s Policií České republiky.

Jihočeský kraj – Ozbrojený útočník ve škole, III. – závěrečná etapa

Preventivní projekt „Ozbrojený útočník ve škole“ byl v rámci kraje zahájen roku 2016. Projekt je vnímán jako komplexní soubor preventivních opatření, jejichž hlavním cílem je snížení pravděpodobnosti výskytu ozbrojeného útočníka ve školním prostředí, zvýšení schopnosti personálu školy na tuto situaci účinně a správně reagovat a zmírnit tak možné negativní dopady útoku.

Do realizace souvisejících činností je zapojen krajský úřad, krajské ředitelství policie a zdravotnická záchraná služba. Projekt je finančně podporován všemi partnery projektu, včetně Ministerstva vnitra České republiky. Projekt od počátku realizoval stabilní tým policejních a záchranářských specialistů a záchranářů za koordinace manažerky prevence kriminality Krajského úřadu Jihočeského kraje.

Za roky 2016 až 2018 se do projektu se zapojilo 34 škol, přičemž bylo proškolen 2 453 zaměstnanců škol. Do aktivit projektu se navíc zapojilo dalších 646 osob. V rámci projektu se také podařilo uspořádat konference a odborná setkání na téma „Bezpečná škola“.

Konkrétně rok 2018 byl ve znamení prezentace série instruktážních filmů, určených primárně policistům a pracovníkům základních a středních škol v rámci kraje. Filmy přizpůsobily celosvětově uznávaný koncept „Uteč – Skryj se – Bojuj!“ tuzemskému prostředí. Ve filmech vystupují žáci základních a středních škol v rámci kraje (Základní škola Bezdravská České Budějovice a Obchodní akademie v Písku) a jsou tematicky koncipovány do pěti samostatných dílů. Jako příklad dobré praxe byla související metodika ve druhé polovině roku 2018 nabídnuta i ostatním krajským ředitelstvím policie v České republice. V rámci souvisejících aktivit došlo rovněž k vytvoření informačních a osvětových materiálů pro zaměstnance škol ve formátu karet a souhrnného informačního lepořela. Samostatným výstupem projektu je i daleko šířeji využitelná metodika „První pomoc při útoku“.

V roce 2018 navázali realizátoři projektu rovněž spoluprací s kolegy ze Slovenska, Rakouska a Německa. Získali tak hodnotné praktické zkušenosti z realizace obdobných preventivních akcí v zahraničí, které zúročili v metodických filmech.

Ambicí projektů bylo a je proškolení personálu, respektive žáků všech jiho-

českých škol v horizontu několika let. V rámci jednotlivých okresů vznikly školící mikrotýmy. Pro konkrétní školu to zahrnuje jak bezpečnostní audit a školení laické první pomoci, tak nácvik chování při útoku s modelovými situacemi – stejně jako závěrečný debriefing u kulatého stolu.

Plzeň – Nasazení SED (Sound Event Detektorů): detektorů střelby, panických výkřiků a tříštění skla

V roce 2021 byl prostřednictvím Správy informačních technologií města Plzně realizován pilotní projekt nasazení a testování detektorů střelby, panických výkřiků a tříštění skla.

V prosinci 2022 získalo město dotaci na jejich další rozšíření. Detektory tohoto typu zvyšují pravděpodobnost dopadení pachatele trestného činu a tím napomáhají snížení kriminality.

Jak prokázal pilotní projekt na Americké ulici, detektory jsou s velmi vysokou mírou spolehlivosti schopné zaznamenat například rozbití výlohy vandaly či zloději.

Město Plzeň avizovalo v rámci projektu nasazení dalších 25 kusů senzorů v lokalitách určených na základě analýzy provedené Městskou policií Plzeň, Policií České republiky a krizovým řízením města. Senzory byly integrovány do prostředí bezpečnostního dispečinku (platforma iVISEC), aby obsluha byla v reálném čase upozorněna na incident, mohla ho ověřit a případně k události přijmout potřebná opatření.

Shrnutí a doporučení

Téma ochrany měkkých cílů bylo a zůstává silným motivem kampaní na úrovni krajů a větších (krajských) měst, přičemž zdaleka ne všechny související aktivity jsou financovány po linii Ministerstva vnitra České republiky. Rovněž sledované období let 2018 až 2022 představuje jen výše souvisejících aktivit a je třeba vnímat kroky, které mu předcházely a které na něj v současnosti navazují.

Obecně je přitom vhodné, aby výsledky projektů byly běžně dostupné, aby nedocházelo k opakování úspěšných i méně úspěšných procesů nebo vytváření obdobných výstupů (videa, letáky, karty). Rovněž „Evropská síť prevence kriminality“ požaduje, aby výsledky, a to nejen nejlepší praxe, byly co nejdříve k dispozici – a tato priorita je nyní přenášena i do prostředí České republiky. Je tedy politováníhodné, že některé výstupy z výše uvedených projektů nejsou vždy intuitivně k nalezení a je třeba je skládat z dílčích podkladů, nebo ne-

jsou v otevřených zdrojích k dispozici vůbec.

doc. Mgr. Oldřich Krulík, Ph.D.

Vysoká škola AMBIS
Mezinárodní bezpečnostní institut, z. s.

Použité zdroje pro další informace

Středočeský kraj:

Středočeský kraj pokračuje v projektu zaměřeném na bezpečnost škol. Bezpečný Středočeský kraj, 2017, 2018. <https://bezpecny.stredoceskykraj.cz/aktuality/stredocesky-kraj-pokracuje-projektu-zamerenem-bezpecnost-skol/>

Ozbrojený útočník ve škole – Středočeský kraj. Prevence kriminality, 5. III. 2019. <https://prevence-kriminality.cz/ozbrojeny-utocnik-ve-skole-stredocesky-kraj/>

O první seminář na ochranu měkkých cílů byl velký zájem. Asociace „Bezpečná škola“, 11. IX. 2018. <https://www.asociacebezpecnaskola.cz/2018/09/11/o-prvni-seminar-na-ochranu-mekkych-cilu-byl-velky-zajem/>

Středočeský kraj zahajuje „Informační a vzdělávací kampaň na ochranu měkkých cílů“. Bytová správa Ministerstva vnitra České republiky, 2018. <https://www.mvcr.cz/bsmv/clanek/stredocesky-kraj-zahajuje-informacni-a-vzdelavaci-kampan-na-ochranu-mekkych-cilu.aspx>

Vzdělávací institut Středočeského kraje. <https://visk.cz/>

Liberecký kraj:

TRDLA, Filip. Kraj pokračuje v ochraně měkkých cílů, pomůže v prevenci i tvorbě bezpečnostních plánů. Liberecký kraj, 6. III. 2024. <https://www.mvcr.cz/bsmv/clanek/stredocesky-kraj-zahajuje-informacni-a-vzdelavaci-kampan-na-ochranu-mekkych-cilu.aspx>

Jihočeský kraj:

Uteč – Skryj se – Bojuj. Jihočeský kraj; Policie České republiky; Youtube, 2018, 2019. <https://www.youtube.com/watch?v=FT29KA-lpuM>

HOCKE, David. Ozbrojený útočník ve škole - projekt prevence útoku ve školním prostředí má novinku. Jihočeský kraj, 20. III. 2019. <https://www.kraj-jihocesky.cz/cs/ozbrojeny-utocnik-ve-skole-projekt-prevence-utoku-ve-skolnim-prostredi-ma-novinku>

Projekt Ozbrojený útočník ve škole - metodické filmy. Policie České republiky – krajské ředitelství policie Jihočeského kraje, 2018. <https://www.policie.cz/clanek/projekt-ozbrojeny-utocnik-ve-skole-metodicke-filmy.aspx>

Ozbrojený útočník ve škole. Sociální portál Jihočeského kraje. <https://socialniportal.kraj-jihocesky.cz/financujeme/projekty/ozbrojeny-utocnik-ve-skole>
Jihočeský kraj spouští web k projektu „Ozbrojený útočník ve škole“. Ministerstvo vnitra České republiky. <https://www.mvcr.cz/chh/docDetail.aspx?docid=22088121&docType=ART>

Plzeň

Pro bezpečnost občanů: Plzeň rozšiřuje použití detektorů střelby, panických výkřiků a tříštění skla. Smart city v praxi, 8. XII. 2022. https://www.smartcitypraxi.cz/zajimave_projekty_505.php

KRIZOVÝ INFORMAČNÍ A SVOLÁVACÍ SYSTÉM KISS

Společnost SAFE Technology SAFETE, s.r.o., přichází na trh s novou dimenzí bezpečnosti do nemocnic, škol, veřejných institucí i výrobních podniků. Jakou roli hraje v ochraně měkkých cílů?

Krizový informační a svolávací systém (KISS) dnes představuje komunikační řešení pro monitoring, svolávání i informování osob. Je hojně využíván ve zdravotnictví a rozšiřuje se také na veřejných institucích, ve školách nebo výrobních podnicích. Tam všude platí za ceněného pomocníka pro systematické, rychlé a spolehlivé oslovení při krizích, jako je např. aktivace traumatických plánů, svolávání krizových týmů nebo informování o hrozícím nebezpečí (např. aktivní střelec, únik chemických látek aj.).

Využíván je ale rovněž pro distribuci běžných informací větším skupinám příjemců, ke svolávání na plánované porady či sledování zpětné vazby. KISS může fungovat i jako aktivní systém zabezpečující ochranu měkkých cílů při útoku v prostorách jakéhokoli zařízení. Při napadení či hrozícím nebezpečí informuje KISS personál o aktuální situaci, je schopen dle geografické polohy upozornit příchozí a zabránit tak vstupu dalších osob do potencionálně nebezpečných prostor.

cizích osob, proto jsou z hlediska ochrany měkkých cílů velmi zranitelné a vyžadují zvýšenou ochranu. Samostatnou kapitolou jsou pak speciální oddělení nemocnic, například psychiatrie, kde může docházet k napadení nejen ze strany návštěvníků, ale také ze strany pacientů. Na všechny tyto situace má krizový svolávací systém scénáře, které aktivně informují personál i návštěvníky o aktuální nenadálé situaci, s cílem ochránit jejich životy a minimalizovat škody.

Další funkcí systému je pak monitoring a na něj navázané spuštění alertů ve chvíli vybočení z požadovaných podmínek. I zde je uplatnění poměrně široké. Dojde-li například k přerušení dodávky energie a růstu teploty v prostorech, kde se uchovávají chemikálie, léčiva, vzorky nebo výsledky letitých výzkumů vyžadující určitý teplotní režim, rozesílá krizový informační systém upozornění okamžitě a zabrání tak ztrátě zásob či plodů několikaleté práce.

Jak krizový informační a svolávací systém KISS funguje?



Scénáře v hlavní roli

Krizové scénáře na ochranu měkkých cílů jsou v dnešní době vzrůstajícího násilí stále více v popředí zájmu. Zdravotnická zařízení, vysoké školy, ale i další veřejné instituce jsou otevřené prostory, v nichž se dá jen stěží zabránit příchodu

V platformě jsou evidovány kontakty na všechny požadované cílové skupiny (zaměstnance a jejich podskupiny, spolupracovníky, externisty...), kterým je systém schopen ihned po aktivaci předat potřebné informace v různých formách komunikace (automatické vo-

lání hlasovým robotem, SMS, e-mail, push zpráva na chytré telefony, zpráva na sociální sítě, sdělení na pracovní stanice...). Jednotlivé typy komunikace jsou nastaveny individuálně, dle potřeb klienta, na základě konzultace s ním. Zároveň mohou vyjadřovat stupeň naléhavosti předávané informace.

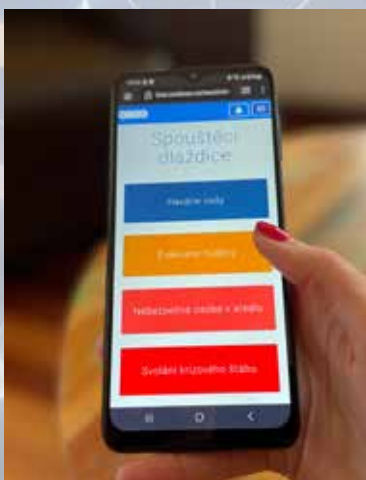
Mezi prioritní typy komunikace patří automatické zavolání a „přečtení“ konkrétní informace pomocí modulu TTS (Text To Speech), tedy tzv. hlasovým robotem. Svolavatel vybere skupinu kontaktů, do systému napíše text sdělení a vše ostatní již zařídí portál krizového informačního a svolávacího systému. Informaci předává paralelně všem kontaktům najednou, čímž výrazně zrychluje distribuci od svolavatele ke zvolené skupině kontaktů. Systém eviduje reakce příjemců – hovor bere/nebere, vzkaz si vypočetl, potvrdil přijetí zprávy či zvolil konkrétní odpověď z několika variant (DTMF volbou). Pokud volaný nereaguje, je systém schopen postupovat dále a sdělení odeslat formou SMS nebo začít kontaktovat náhradníka (tj. kontakt definovaný jako zástupce pro případ nedostupnosti).

Scénáře svolávání jsou jednou ze základních částí krizového svolávacího a informačního systému. V platformě jich může být navoleno neomezené množství, s distribucí informace na neomezené množství kontaktů. Platforma umí komunikovat v 17 jazycích a sdělení může přenášet i do interních systémů společnosti.

Uživatel je oprávněn definovat si sám libovolné scénáře komunikace a svolávání, včetně podmínek a rozhodovacích uzlů. Přiblížme si vše na příkladu z oblasti zdravotnictví. Tam jsou scénáře často využívány v krizových případech, kdy je nutno informovat o určité události konkrétní kontakty či typy pracovních pozic. Například při vážné nehodě je třeba volat lékaře a pomocný personál, který má v daný okamžik službu. Těmto osobám systém okamžitě po aktivaci sám

zavolá a předá informaci o události.

Ve scénáři je jasně definováno, jaké osoby má platforma oslovit v první linii, včetně toho, jakým kontaktům má telefonovat, jakým jen poslat informační SMS a jak postupovat v případě, že konkrétní osoba nereaguje. Pro spuštění celé akce je v objektu, kde je instalován krizový informační a svolávací systém, zapotřebí jen jednoduchá aktivace konkrétního scénáře, který si uživatel do systému předem nadefinoval. Svolávající se tak ve vypjaté situaci vyhne zmatkům a chybám vznikajícím v důsledku nedokonalosti lidského faktoru a vysoké míry stresu při nenadálých situacích. Odpadá také nutnost opakovaných kontaktů a potřeba pamatovat si, kdo hovor přijal/nepřijal atd.



Scénáře svolávání mohou být nadefinovány pro libovolné situace. Od krizových složitých událostí až po ty běžné, kdy je zapotřebí například jen poslat informaci zaměstnancům a evidovat jejich reakce nebo odpovědi. Tuto funkci v platformě zajišťuje informační modul. Zde se nejčastěji využívá komunikace formou zaslání SMS či e-mailu. Uživatel vybere skupinu osob z modulu kontaktů a těm požadovanou informaci rozešle. Systém pak eviduje seznamy oslovených kontaktů, včetně jejich odpovědí (jsou-li očekávány). Tímto způsobem mohou být rozesílány třeba i pozvánky na pravidelné prohlídky u lékaře, SMS ankety či informace marketingového charakteru. Výsledky a informační aktivity jsou detailně evidovány a v platformě jsou dostupné ve formě hotových reportů.

Důležité komponenty platformy KISS:

Modul reportů zobrazuje veškerou historii komunikace a svolávání, kterou systém prováděl. Eviduje jednotlivé odpovědi a reakce uživatelů (volaných osob) a informace o průběhu poskytnuté v tabulkové i grafické formě s mož-

ností automatického zaslání e-mailem oprávněné osobě.

Modul mapy je dalším velmi důležitým komponentem platformy. Umožňuje sledování a mapovou lokalizaci osob a uživatelů systému. Uživatel může používat smart-phone s nainstalovanou aplikací nebo některé z profesionálních zařízení, jež bývají dodávána spolu se systémem. Platforma pracuje s okamžitou polohou uživatele, ukazuje jeho časový pohyb ve zvolené periodě či poskytuje informace o volitelných stavech ze strany uživatele (ve službě, mimo službu, oběd...). Díky mapové lokalizaci lze také oslovovat vybrané uživatele, nalézající se ve zvoleném perimetru, čehož je možno využít třeba při nehodách velkého rozsahu a informování lékařů a zdravotnických pracovníků v dosahu.

Modul monitoringu podmínek představuje hojně poptávanou funkci. Při nastavení požadovaného rozmezí dokáže tento modul hlídat aktuální podmínky, a pokud se například teplota či vlhkost blíží nastavené kritické hranici, spustí okamžitě distribuci informace dle nastaveného scénáře. Tak může ve firmě zachránit léky, suroviny citlivé na teplo nebo vzácný biologický materiál.

Stručně řečeno – KISS je virtuální pomocník, který dokáže chránit nejen lidské životy, ale i finance a majetek firmy.

Tři otázky na Jana Buriana, jednatele společnosti SAFE Technology SAFETE, která krizový informační a svolávací systém KISS vyrábí a dodává.



Na českém trhu působíte více než 10 let. Změnil se nějak pohled Čechů na krizové informační a svolávací systémy po prosincových událostech na Filozofické fakultě UK?

Ačkoli systém vyvíjíme a implementujeme už celou dekádu, prosincový tragický incident změnil hodně. Před útokem na Filozofické fakultě UK nás znali jen lidé v oblasti zdravotnictví. Kamkoli jinam jsme přišli, museli jsme představovat, co to KISS je, k čemu je dobrý při krizi a jak se dá využít i ve standardním provozu. SAFE Technology SAFETE ani KISS skoro nikdo mimo tento obor neznal. Po prosincových událostech se řešení krizové komunikace stalo velmi aktuálním a vnímám, že pro státní i komerční sféru je nyní bezpečnost velké téma a priorit.

Od střelby na Filozofické fakultě UK uplynuly zhruba čtyři měsíce. Registrujete za tu dobu nějaký posun v přístupu univerzit a institucí k tématu bezpečnosti a ochrany měkkých cílů?

Musím především říct, že některé české univerzity přistupovaly k tomuto tématu velmi aktivně již před touto událostí. Systém byl doslova krok před spuštěním jak na Univerzitě Karlově, tak třeba na České zemědělské univerzitě. Obě tyto školy měly a mají intenzivní zájem zajistit pro studenty i zaměstnance maximální bezpečí.

Co se týče krizového zabezpečení, je to oblast, kde nikdy není úplně hotovo. Jde o kontinuální proces, který se pořád vyvíjí, a statistiky bohužel naznačují, že nebezpečí stále narůstá. I proto je třeba mít nejen kvalitní systém pro komunikaci a distribuci informací při krizových situacích, ale současně nepodceňovat ani nácvik chování v nich.

V Česku jste jedničkou ve výrobě a implementaci informačních a svolávacích systémů. Co je konkurenční výhodou systému KISS?

Obrovskou výhodou je fakt, že jsme systém KISS vystavěli od úplného základu a deset let, co existuje, ho neustále zlepšujeme, rozšiřujeme, reagujeme na specifické požadavky našich zákazníků. Dnes tedy máme v rukou rozsáhlý ekosystém, přičemž kvalita jeho fungování je denně prověřována v 70 % českých fakultních nemocnic v momentech, kdy se hraje o každou sekundu, a především o lidské životy. A KISS zde obstál, pomáhá, zachraňuje lidské životy. To celý náš tým velmi motivuje, s radostí se vrháme do dalších výzev a nových segmentů. Zkrátka a dobře si trůfnu říct, že nás to baví a na výsledném produktu, tedy krizovém informačním a svolávacím systému KISS, je to prostě vidět.

Jan Burian

SAFE Technology SAFETE

TEMPEST

ANEB NEZANEDBÁVEJTE „BLIND SPOT“ V ŘÍZENÍ KYBERNETICKÉ BEZPEČNOSTI

V dnešní době je kybernetická bezpečnost pro organizace nezbytná. S rostoucím počtem kybernetických hrozeb a sofistikovaných útoků je důležité, aby firmy měly v plánu řízení bezpečnostních rizik, který zahrnuje identifikaci a ochranu před různými hrozbami. Nicméně při navrhování a provádění těchto opatření je důležité si uvědomit existenci „blind spotu“ neboli tzv. mrtvého úhlu.

„Blind spot“ je oblast, která není dobře viditelná. V kontextu kybernetické bezpečnosti to může znamenat nedostatečné pokrytí určitých aspektů bezpečnosti nebo ignoraci potenciálních hrozeb a slabých míst v bezpečnostní infrastruktuře. Ignorování „mrtvého úhlu“ může mít zničující důsledky, protože útočníci často hledají právě tyto slabiny k proniknutí do systémů a způsobení škod.

Existuje několik zásadních oblastí, které by měly mít organizace při identifikaci a pro eliminaci „mrtvých úhlů“ v kybernetické bezpečnosti na paměti – jsou to:

- komplexní analýza rizik
- aktualizace bezpečnostních opatření
- vzdělávání zaměstnanců
- monitoring a detekce

Právě implementace efektivního monitorovacího a detekčního systému je pro odhalení neobvyklého chování nebo podezřelých aktivit v síti klíčová. Díky tomu lze potenciální hrozby spolehlivě identifikovat a rychle na ně zareagovat, což minimalizuje škody.

Co je TEMPEST?

TEMPEST se zaměřuje na analýzu a ochranu před nechtěným vyzařováním elektromagnetických signálů ze zařízení, jako jsou počítače, monitory, klávesnice a další elektronika. Tyto emise mohou být útočníky potenciálně využity k získání citlivých informací.

Některá elektronická zařízení produkují elektromagnetické záření nebo kompromitující vyzařování způsobem, který lze použít k rekonstrukci srozumitelných dat. Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) to považuje za problém v situacích, kdy mohou být utajované informace přístupné, ale musí být chráněny před vnějšími pozorovateli. Pro jakýkoliv systém existují specifické elektromagnetické frekvence, které musí být potlačeny, aby informace zůstaly neděšifrovatelné.

Ochrana zařízení před špionáží je zajištěna vzdáleností, stíněním, filtrováním a maskováním. Normy TEMPEST nařizují prvky, jako je vzdálenost zařízení od zdí, množství stínění v budovách

a zařízení. Nařizují například vzdálenost oddělující vodiče nesoucí klasifikované a neklasifikované informace anebo EMC filtry na datových a elektrických vodičích.

Společnost Nowatron Elektronik, spol. s r.o., nabízí produkty s certifikací dle NATO TEMPEST standardů pro práci s informacemi s různým stupněm utajení.

Petr Chalupa
projektový manažer
Odolné PC, Military, TEMPEST



ŘÍDICÍ A DOHLEDOVÁ CENTRA – KLÍČOVÝ PILÍŘ KAŽDÉ SPOLEČNOSTI

Správně fungující dohledové a řídicí centrum je pro každou společnost klíčovým prvkem, zejména v oblastech, kde je potřeba koordinace, sledování a řízení operačních činností. Nezáleží na tom, zda jde o logistickou firmu, energetického provozovatele, zdravotnickou instituci nebo technologickou společnost – efektivní dispečink či dohledové centrum mohou významně zlepšit výkon a výsledky organizace.

Základním prvkem každého takového centra, zvláště v kritickém prostředí, jsou technologie velkoplošného zobrazení a řídicího systému, které nepřetržitě 24 hodin denně, 7 dní v týdnu umožňují zobrazovat, sledovat a vyhodnocovat ty nejdůležitější informace, popřípadě na jejich základě jednat. Obě technologie tedy musí být navrženy s ohledem na dlouhodobý a bezproblémový provoz po mnoho let. Z průzkumů mezi dispečery jasně vyplývá, že špatně fungující technologie je jim ve výsledku spíše na obtíž a šetřit v této oblasti se opravdu nevyplácí.

Nové trendy na trhu

Největší změny se odehrávají na poli řídicích systémů. Tradiční matice a kontroléry nahrazují systémy AV over IP (AVoIP), které nabízejí díky složení z mnoha menších komponent namísto jednoho velkého kontroléru flexibilitu, robustnost, rychlý servis a v neposlední řadě bezpečnost. Kromě velkoplošného zobrazení obsluhují i pracoviště operátorů, takže mají

přístup jen k těm zdrojům informací, ke kterým ho mít mají, a zároveň nahrazují změtí myši a klávesnic na stolech dispečerů, kteří potřebují mít přístup k mnoha různým systémům. Nově mají operátoři jednu myš, jednu klávesnici, jedno audiozařízení – bez ohledu na to, jestli mají před sebou jeden monitor se dvěma kamerami a jednou webovou stránkou nebo osm monitorů a desítky zdrojů dat.

Díky použití standardní ethernetové sítě odpadá náklady na drahé optické AV kabely a omezení vzdálenostmi. Serverovna je na opačné straně budovy, nebo dokonce celého areálu? Žádný problém. Ředitel chce mít přístup ke kamerám ve výrobě stejně jako operátoři na dispečinku? Opět žádný problém.

V zobrazovacích technologiích pak vidíme rapidní vývoj v oblasti LED video-stěn, které s poklesem cen budou technologií blízké budoucnosti a umožní perfektní obraz bez mezer mezi jednotlivými moduly. S každou novou gene-

rací modulů se snižuje prozatím vysoká spotřeba a zmenšuje rozteč bodů (pixel-pitch).

Bezpečnost

Zejména v poslední době je kladen velký důraz na zvýšení bezpečnosti ve všech oblastech. Tento trend je patrný jak ve veřejném, tak i soukromém sektoru a je reakcí na různé hrozby a výzvy, kterým čelíme v moderním světě. Nová řešení řídicích systémů umožní zcela oddělit systémy dispečinku od ostatní kritické infrastruktury v organizaci. Jsou stavěny s důrazem na maximální kyberbezpečnost a s výhledem na plnění nejnáročnějších požadavků zákona o kybernetické bezpečnosti NIS2. Často jsou certifikovány ISO 27001, automatické šifrování dat nebo přístupy pouze pro autentizované osoby.

Petr Barták

projektový manažer
Dispečerská pracoviště
Nowatron Elektronik

NOWATRON ELEKTRONIK, SPOL. S R.O.

Váš partner v oblasti profesionálních zobrazovacích systémů, projekční a prezenční techniky.

Nabízíme také širokou škálu průmyslových, odolných počítačů a IT hardwaru pro průmyslové, dopravní a armádní aplikace. Na českém a slovenském trhu

působíme více než 30 let. Dodáváme jednotlivá zařízení, ale také navrhujeme kompletní řešení na klíč.

Všechny produkty i celá řešení také servisujeme a udržujeme v kondici. Investujeme mnoho energie i prostředků do zkvalitňování servisu a technické

podpory, abyste mohli své technice věřit. Pro ty nejnáročnější provozovatele z kritické infrastruktury zajišťujeme servis 24 hodin denně.



Dispečerská pracoviště





TERMOKAMERY HIKVISION

A JEJICH NEPOSTRADATELNÉ VYUŽITÍ V PRŮMYSLU

Jakýkoliv objekt s teplotou vyšší než nula vyzařuje detekovatelný objem infračerveného záření (IR). Čím vyšší je teplota objektu, tím větší je intenzita vyzařovaného infračerveného záření. Termokamery využívají rozdílů v intenzitě IR mezi objekty a „zviditelňují“ neviditelné infračervené světlo ve formě zobrazení tepelných zón.

Termokamery Hikvision pokrývají řady Security, Thermography a Commercial Vision a zaručují několik vrstev situačního povědomí v celé řadě situací, například ochranu perimetru, měření teploty a detekci požáru. „Vidí“ z velkých vzdáleností prakticky za jakýchkoli světelných nebo povětrnostních podmínek a díky schopnostem deep learning dokáží rozlišit osoby a vozidla od jiných objektů. Termokamery Hikvision jsou posíleny o zobrazení viditelného světla a vizualizovaných metadat a představují ideální volbu pro rozšířené povědomí o událostech a nouzových situacích non stop.

Řada Security byla vyvinuta tak, aby dokázala odolat náročným venkovním podmínkám, a je vybavena nejmodernějšími technologiemi. Lze ji snadno přeměnit na pokročilé systémy ochrany perimetru důležitých infrastruktur. Řada ručních termografických kamer je navržena v elegantním provedení v několika různých modelech. Je hojně využívána pro prevenci požárů v interiéru, k elektrické a mechanické kontrole apod. S ručním monokulárním a binokulárním zařízením stejně jako s termo doplňky se řada Commercial Vision neustále rozšiřuje o nové možnosti v komerčním využití tepelných technologií.

Pro termovýrobky Hikvision jsou příznačné tři inovativní funkce zajišťující lepší adaptabilitu vůči prostředí:

- AGC (Auto Gain Control) neboli automatické řízení přírůstku – upravuje dynamický rozsah obrazu tak, aby pomohl zachovat vyvážený jas;

- DDE (Digital Detail Enhancement) neboli digitální korekce detailů – vychází z algoritmu pro oblast zájmu a vykresluje v obrazu na obrazovce více detailů;
- DNR (Digital Noise Reduction) neboli digitální potlačení šumu 3D – minimalizuje vliv „horkých pixelů“, takže obraz působí ještě ostřeji.

Minimalizace rizika požáru pomocí inteligentního videa a termálního zobrazení

Termokamery jsou velmi efektivní při odhalování vznikajícího abnormálního tepla. Svým způsobem velmi rychle zjistí bod tepla ve velkých lokalitách nebo na určitých stanovištích, pro něž není tradiční detekce vhodná – jsou to např. místa ošetření odpadu, skládky, bateriová úložiště, datová centra, elektrické skříně apod.

Na různých místech a typech zařízení může požár zapříčinit velkou zdravotní a bezpečnostní újmu stejně jako abnormální škody na zařízeních a zboží. Dobrou zprávou je, že nová generace inteligentního videa a termovizního řešení dramaticky zrychluje reakci na neúměrně zvýšené teplo a riziko ohně a pomáhá podnikům všech typů chránit jejich zaměstnance a majetek.

Vedle nevyčíslitelných škod na zdraví a životech lidí způsobují požáry i enormní škody na majetku (zboží, vybavení, budovách atd.), často za statisíce až miliony korun.

Aby se těmto negativním dopadům zabránilo a ochránilo se osoby i majetek, je třeba požárům předcházet a snižovat jejich potenciální rizika – detekovat nebezpečí jejich vzniku, a pokud k nim dojde, uhasit je dříve, než vyhoří mimo kontrolu.

Řešení pomocí termokamer jsou spolehlivá a stále více žádaná. Termokamery slouží k zajištění požární bezpečnosti výrobních areálů složených z voltaických panelů, k ochraně parkovišť, elektrických skříní, baterií pro elektromobily, některých historických památek (jako jsou například katedrály) aj. Termální kamery však nejsou „záchrankou“, který vyřeší všechno, proto by v žádném případě neměly nahrazovat konvenční prostředky detekce, jejichž použití je relevantní a účinné. S kamerami věnovanými protipožární prevenci se můžeme setkat na úzce specializovaném trhu, který se však vyvíjí s velmi specifickými technickými omezeními. Termokamery neslouží k pouhému videodohledu, ale především k detekci požáru. Je proto nezbytné navrhovat, instalovat a udržovat je stejně kvalitně jako všechny ostatní prostředky detekce požáru, se stejnou úrovní požadavků.

Minimalizace požárních rizik okamžitými reakcemi

Pro minimalizaci rizika požáru se mnohé organizace rozhodly nasadit inteligentní videořešení, která obsahují technologii tepelného zobrazování.

Minimalizace požárních rizik okamžitými reakcemi

Tato řešení okamžitě detekují objekty, které vyzařují nadměrné teplo, a spouštějí alarmy pro manažery nebo členy bezpečnostních týmů. Lze je nakonfigurovat také tak, aby aktivovaly vodní děla

nebo jiná „hasící“ zařízení, jež umožňují okamžité hašení požáru a předcházejí větším škodám.

Zachycení požáru odpadů před jejich vypuknutím

Požáry odpadů – jinými slovy požáry, které se vyskytují v zařízeních na zpracování odpadu nebo recyklaci – jsou velmi závažným globálním problémem. Země po celém světě trpí více než jedním požárem denně v odvětví odpadu a recyklace. Způsobuje to ohrožení zdraví a životů zaměstnanců, poškození pracovišť a strojů a poškození pověsti, nehledě k potenciálnímu dopadu na životní prostředí. Jedním z největších rizik požáru v zařízeních na likvidaci odpadu jsou poškozené lithium-iontové baterie, jelikož jsou dobíjecí a jsou navrženy tak, aby byly udržitelnější!

Co způsobuje požáry odpadu?

Lidé vytvářejí stále více odpadu, a proto se jeho recyklace stává zásadní záležitostí v boji za udržitelnost. Četné recyklační závody jsou tudíž postaveny tak, aby přetvářely nejrůznější druhy odpadových materiálů na materiály znovu použitelné.

Mnohé z těchto materiálů jsou ovšem hořlavé (například papír a lepenka) a v zájmu šetření místem bývají co nejvíce stlačovány k sobě. Ke zvyšování teploty v hromadách takto stlačených odpadů přispívá pochopitelně i počasí v horkých a suchých obdobích. Kumulace podobných rizikových podmínek tak vytváří potenciálně hořlavé prostředí, kdy stačí už jen jiskra.

Toto je příkladem toho, co je v průmyslu známé jako „opaření“. Teplo se může nekontrolovaně hromadit v místě, které nelze tradičními způsoby vidět ani sle-

dovat. Například právě uprostřed hromady odpadu. Není vidět doutnání ani žádný kouř, protože zdroj nebezpečí je zakryt vnějšími vrstvami odpadu.

Stále častějším viníkem vzniku požárů jsou dobíjecí baterie. Podle nedávné zprávy WEEE způsobily za poslední čtyři roky nejzávažnější požáry zaviněné dobíjecími bateriemi škody v průměru za více než milion eur. Lithium-iontová technologie v těchto bateriích funguje pomocí různých chemikálií v samostatných článcích. „Stěny“ těchto článků jsou poměrně tenké, aby byla baterie lehká. Pokud jsou poškozeny (propíchnutím nebo zkratováním kombinací oddělených prvků), mohou způsobit hromadění tepla vedoucího nejen k požáru, ale dokonce i k výbuchu.

Hašení požárů odpadu

Tradiční metody řešení problému jsou založeny na rychlé reakci na požár odpadu, pokud možno ihned po jeho vypuknutí. Používají se požární hlásiče a sprinklerové systémy a „horká linka“ na místní hasičský sbor. Stanoviště také používají sirény a světla k varování lidí před nebezpečím.

K aktivaci těchto opatření však dosud obvykle dochází, až když požár vypukne.

Nově vyvinutá technologie Hikvision však nabízí řešení problému dříve, než k němu dojde. Jinými slovy mu předchází – umožňuje detekovat hromadění tepla dříve, než se vznítí oheň. Úspěšně zvládá snižovat rizika úrazu zaměstnanců nebo návštěvníků stanoviště. Kromě toho také snižuje náklady za práci na opravě

případných škod požárem způsobených.

Hikvision zasahuje

Termokamery Hikvision se používají ke sledování teplot uvnitř i vně závodu. Lze je nakonfigurovat dvoulimitně tak, aby vyvolaly poplach, už když je sledována předdefinovaná teplota, a poté znovu, když je dosažena teplota ještě vyšší.

První teplotní limit je naprogramován pro „předběžný alarm“, který způsobí, že kamera vyšle signál, jakmile je teplota sledovaného prostředí vyšší než obvykle. Druhý limit je nakonfigurován na kritickou teplotu, aby bylo jasné, že jakmile se ozve druhý alarm, je nutné okamžitě jednat.

Oba alarmy mohou být ověřovány zaměstnanci sledujícími situaci jak na místě, tak mimo něj pomocí bispektrální kamery. Ta poskytuje živé obrazy spolu s termálními, což dostává problém do kontextu. Poté mohou příslušné osoby vybavené ověřenými situačními informacemi podniknout kroky k zabránění vzniku požáru, potažmo k jeho hašení. Mohou to být zaměstnanci stanoviště nebo vzdálené monitorovací služby.

Pomocí softwaru pro správu videa Hik-Central lze obrazy odesílat správcům stanoviště také vzdáleně. Mohou vidět, co se děje, prostřednictvím tabletu nebo mobilu, ať jsou kdekoli.

Franck Carette

Thermal Product manager Europe
Security & Safety



BUDOUCNOST MANAGEMENTU

V SEGMENTU KOMERČNÍ BEZPEČNOSTI 2. ČÁST

Pro management budoucnosti je důležitá mimo jiné podpora diverzity a inkluze v pracovním prostředí a na pracovišti firem. Tento trend je relevantní i v následujícím deseti-letém období. Zajištění rozmanitosti a inkluze na pracovišti se stalo jednou z největších výzev, kterým čelí dnešní moderní organizace firem i management do budoucna.

Management budoucnosti ovlivní v dalších deseti letech technické a technologické inovace, jako například virtuální nábor, virtuální přijímací řízení, úprava pracovních činností na dálku i udržení zájmu potencionálních zaměstnanců o práci v dané firmě.

Diverzita na pracovišti se zaměřuje na respektování a oceňování všech zaměstnanců pro jejich odlišnosti. Typicky je to jejich etnický původ, věk, náboženství, vzdělání, pohlaví, zdravotní postižení a další. Inkluze se naproti tomu zaměřuje na zajištění toho, aby se všichni zaměstnanci cítili ceněni a podporováni jako jednotlivci, bez ohledu na jejich fyzické nebo kulturní odlišnosti.

Analytické společnosti McKinsey se podařilo prokázat, že firmy s rozmanitější pracovní silou dosahují lepších výsledků než ostatní zaměstnavatelé. Stejně tak výzkum provedený v prostředí evropských firem i do budoucna ukazuje, jak může budování inkluzivnější kultury na pracovišti výrazně zvýšit angažovanost a pohodu zaměstnanců. Je však rozhodně nutné udržet tyto inovativní trendy v rozumných mezích pro firemní praxi i v české společnosti a firemních segmentech včetně komerční bezpečnosti.

S přechodem na práci na dálku však musí dnešní manažeři najít nové způsoby, jak být inkluzivní v našem neustále se měnícím pracovním prostředí. Toto bude důležitý trend i v období dalších deseti let z hlediska managementu budoucnosti. Personální manažeři mohou také pracovat na náborových strategiích, jejichž cílem je lépe přilákat různorodé kandidáty. Tímto způsobem je možné firmy v období dalších několika let připravit na větší inovace a ziskovost i konkurenceschopnost v daném segmentu trhu.

Řízení komunikace mezi pracovními týmy je též trendem managementu budoucnosti v období dalších několika let v segmentu komerční bezpečnosti, a to v českém i evropském kontextu. Firemní kultura má být postavena na efektivní komunikaci a týmové práci. Poslední pracovní trendy skutečně zvyšují nároky na komunikaci mezi pracovními týmy.

Analytické výzkumy ukazují, že až 97 % zaměstnanců považuje komunikaci za významnou pro plnění svých každodenních úkolů i pracovních činností. Zapojení zaměstnanců pozitivním způsobem do budoucna je klíčové, proto by ma-

nažeři neměli váhat prozkoumat různé komunikační kanály. Stále rostoucí bude i význam sociálních sítí pro náborové strategie i pro interní prostředí firem různých velikostí a významu, a to zejména v segmentu komerční bezpečnosti. Skutečnost, že technologie a digitalizace jsou důležitým trendem vývoje managementu v dalším období, se zcela jistě projeví i v segmentu komerční bezpečnosti. Představovat budou hlavně zdroje technických a technologických inovací managementu budoucnosti. Digitalizace ve firemní praxi již není volbou, ale nezbytným způsobem konkurenčního boje.

Vzhledem k monumentálním změnám, jichž jsme byli svědky v roce 2023, se nadále daří těm organizacím, které přijaly digitální obchodní model. Všechny ostatní firmy v jednotlivých segmentech se budou muset konkurenčnímu prostředí přizpůsobit. Vysoká fluktuace zaměstnanců v některých firemních segmentech je problematická a pro budoucí management bude jednoznačnou výzvou a trendem do budoucna. Jedná se opět o exponované obory, jako jsou zdravotnictví, sociální služby či cestovní ruch a v neposlední řadě zcela jistě i komerční bezpečnost.

Pokud se nepodaří vyřešit prakticky fluktuaci zaměstnanců i v segmentu komerční bezpečnosti, mohou být i náklady neúměrně vysoké. Nahrzení zaměstnance si vyžádá 33 % jeho ročního finančního ohodnocení průměrného zaměstnance. V případě vedoucích odborných zaměstnanců se toto číslo zvyšuje na neuvěřitelných 400 %, jak ukazují současné analytické studie. Přitom lze předpokládat, že v dalších deseti letech nabude tento problém dále na významu, protože náklady se získáním a zapracováním nových zaměstnanců se budou dále navyšovat.

Další analytická studie prokázala, že zaměstnanci, kteří jsou podporováni v rozvoji svých dovedností, mají dvakrát větší pravděpodobnost, že v dané společnosti stráví celou svou profesní kariéru. Fluktuaci zaměstnanců jako takovou lze snížit například tím, že firma zaměstnancům nabídne smysluplné možnosti rozvoje, zejména školení, která jsou přizpůsobena osobním cílům pracovních týmů i v současné firemní praxi.

Vytváření inovativních pracovních týmů a přístupů k řízení je dalším trendem v prostředí managementu budoucnosti i efektivního řízení zaměstnanců. Pro management budoucnosti je důležité pečovat o kreativní týmy. Závisí na tom

úspěch a konkurenceschopnost dané firmy. Ze strany managementu je žádoucí podporovat inovace v pracovních týmech, protože je to důležité i pro vývoj firem v dlouhodobém časovém horizontu. Mnoho lidí chce v zaměstnání spolupracovat. Manažer proto celkem účelně může svým týmům poskytnout nástroje, které potřebují ke sdílení svých nápadů, a podporovat tak kreativní prostředí v rámci pracovního prostředí i pracovišť firmy. Přitom kreativita a inovace se zdaleka nemusí týkat jen velkých nápadů, ale důležité je postihnout a podporovat i dílčí kroky plynoucí z technických a technologických možností.

Se stále rostoucím problémem, že zaměstnanci z různých důvodů a pohnutek z firem odcházejí, se musejí manažeři vyrovnávat po celém světě. A ještě horším faktem je, že když zaměstnanci z firem odcházejí, odnášejí si s sebou i své znalosti a zkušenosti. A to je nutné zdůraznit, protože v konečném důsledku to může působit velké problémy, zejména pokud nebyly tyto důležité znalosti a zkušenosti sdíleny.

Jednou z největších výzev managementu budoucnosti je tedy zapojení zaměstnanců. Výzkumy ukazují, že angažovaní zaměstnanci jsou produktivnější, kreativnější a méně často odcházejí. Toto vede k větší konkurenceschopnosti a ziskovosti firem různých velikostí a významů.

V další části článku se pokusím shrnout **hlavní trendy z hlediska budoucnosti**, na které by se měl management v komerční bezpečnosti zaměřit, aby efektivně reagoval na nové výzvy a zabezpečil aktiva a zájmy organizací soukromých bezpečnostních firem.

Integrace fyzické a kybernetické bezpečnosti

Jedním z hlavních trendů je stírání hranic mezi fyzickou a kybernetickou bezpečností. Zatímco v minulosti byly tyto oblasti často řízeny samostatně, nyní je nutné je koordinovat a integrovat do jednoho komplexního systému. Tato integrace umožňuje organizacím lépe identifikovat a reagovat na hrozby, které mohou mít dopad jak na fyzická, tak digitální aktiva.

Využití umělé inteligence a strojového učení

Moderní technologie umělé inteligence (UI) a strojového učení nabízí v oblasti bezpečnosti mnoho příležitostí. Díky analýze velkých datových souborů mohou tyto nástroje rychle identifikovat

neobvyklé vzory chování nebo aktivity, které by mohly signalizovat bezpečnostní hrozbu. Výsledkem je rychlejší a přesnější reakce na potenciální incidenty.

Proaktivní přístup k hrozbám a problémovým situacím

Tradiční reaktivní modely řízení bezpečnosti postupně ustupují proaktivnímu přístupu. Místo toho, aby organizace reagovaly na incidenty až po jejich vzniku, zaměřují se nyní na předvídání a předcházení potenciálním hrozbám. To zahrnuje vývoj scénářů, simulaci útoků a pravidelné testování bezpečnostních systémů. Konkrétně se toto projevilo během několika let pandemie COVID-19 a jejich dopadů.

Důraz na vzdělávání a rozvoj zaměstnanců v segmentu komerční bezpečnosti

Většina bezpečnostních incidentů má kořeny v lidském chování. Ať už jde o neopatrnost, nedostatečné vzdělání nebo nedbalost, lidský faktor je často klíčovým prvkem v bezpečnostní rovnici. Budoucí trendy v managementu komerční bezpečnosti tak kladou velký důraz na vzdělávání a osvětu zaměstnanců, aby se snížil počet incidentů způsobených lidskou chybou.

Důraz na pravidla compliance a regulace v segmentu komerční bezpečnosti

Vzhledem k rostoucímu počtu regulací a standardů v oblasti bezpečnosti je důležité, aby organizace nejen splňovaly tyto požadavky, ale také je aktivně využívaly jako nástroje pro zlepšení svých bezpečnostních postupů. Compliance tak přestává být pouhým splněním povinnosti a stává se integrální součástí bezpečnostní strategie.

Integrace s externími bezpečnostními agenturami a jejich vzájemná spolupráce

V dnešní propojené a globalizované době není dostatečné spoléhat se pouze na interní zdroje a kapacity. Spolupráce s externími bezpečnostními agenturami, sdílení informací o hrozbách a společné reakce na incidenty nabízí nový rozměr ochrany. Přístup k externím databázím o hrozbách, sdílení analýz a společné cvičné simulace mohou výrazně posílit obrannou schopnost organizace a připravit ji na nové, dosud nepoznané hrozby.

Personalizace bezpečnostních řešení v segmentu komerční bezpečnosti

Stejně jako v mnoha jiných odvětvích je i v oblasti komerční bezpečnosti pozorován trend směřující k personalizaci. Nejde již jen o generické bezpečnostní protokoly; nyní jsou řešení navrhována tak, aby reflektovala specifika dané organizace, její kulturu, byznys model a konkrétní hrozby, kterým čelí. Personalizované bezpečnostní strategie umožňují organizacím lépe využít své zdroje a zaměřit se na oblasti s nejvyšším rizikem.

Důraz na duševní zdraví a wellness zaměstnanců v segmentu komerční bezpečnosti

Stres a vyhoření mohou mít významný dopad na kvalitu práce bezpečnostních týmů. Proto se stále více organi-

zací zaměřuje na péči o duševní zdraví a wellness svých zaměstnanců. Toto téma je stále častěji začleňováno do širšího kontextu komerční bezpečnosti, protože zaměstnanci v dobré psychické kondici jsou mnohem lépe vybaveni ke správnému rozhodování v krizových situacích.

Ekologická a sociální bezpečnost a důraz na udržitelnost

V současné době, kdy se stále více hovoří o udržitelnosti a sociální odpovědnosti, se tato témata stávají i součástí debat o komerční bezpečnosti. Organizace nejen reagují na tradiční hrozby, ale také berou v úvahu dopady svých činností na životní prostředí a společnost. Vznikají tak nové protokoly, které reflektují tento širší pohled na bezpečnost a berou v úvahu celkový dopad na planetu a společnost.

Růst decentralizace a hybridních pracovních modelů

V důsledku pandemie COVID-19 a technologického pokroku se mnoho organizací přiklonilo k decentralizovaným a hybridním pracovním modelům. Zaměstnanci nyní pracují z různých geografických míst, včetně svých domovů, což přináší nové bezpečnostní výzvy. Management komerční bezpečnosti musí nyní zajistit bezpečný přístup k firemním zdrojům z různých míst a zároveň zohlednit různé úrovně kybernetické ochrany v rámci domácností zaměstnanců.

Zahrnutí etiky do bezpečnostního rozhodování

Etika se stává stále důležitějším aspektem v komerční bezpečnosti. Ať už jde o otázky soukromí, zpracování dat nebo interakce s technologiemi, jako je umělá inteligence, musí organizace zohlednit etické aspekty svých rozhodnutí. To zahrnuje transparentnost v postupech, zohlednění práv jednotlivců a etické zásady při nasazování nových technologií.

Větší důraz na bezpečnostní kulturu v komerční bezpečnosti

Místo toho, aby se bezpečnostní protokoly vnímaly jako izolované postupy, stává se bezpečnostní kultura klíčovým prvkem organizací. Tím se myslí vytvoření prostředí, kde jsou bezpečnostní postupy a protokoly vnímány jako součást každodenního života a kde je každý zaměstnanec považován za součást bezpečnostního řešení. Toto zapojení všech zaměstnanců do bezpečnostního procesu vede k větší odpovědnosti a lepšímu povědomí o potenciálních rizicích.

Spolupráce s veřejným sektorem, zejména v oblasti veřejných zakázek a grantů

Ve světě, kde hrozby mohou mít i geopolitický charakter, je spolupráce mezi soukromým a veřejným sektorem nezbytná. Informace o hrozbách, společné reakce na incidenty a strategická partnerství mohou posílit schopnost organizací reagovat na hrozby a chránit své zájmy.

V náročném a dynamicky se měnícím prostředí komerční bezpečnosti je nezbytné, aby byl management schopen rychle se adaptovat a přijímat inovativ-

ní přístupy. Spolupráce, etika, kultura a pružnost se stávají klíčovými slovy pro budoucnost komerční bezpečnosti. Organizace soukromých bezpečnostních firem, které dokážou tyto principy začlenit do svých strategií, nejenže zlepší jejich bezpečnostní postavení, ale posílí i důvěru a loajalitu zaměstnanců a zákazníků.

PhDr. Mgr. Dávid Dömény, MBA

Seznam použitých zdrojů

- URBANCOVÁ, H., VRABCOVÁ, P. Strategický management lidských zdrojů. Praha: Grada Publishing, 2023. ISBN 978-80-271-3675-9.
- FOTR, J., VACÍK, E. Tvorba strategie a strategické plánování. 2. vyd. Praha: Grada Publishing, 2020. ISBN 978-80-271-2499-2.
- Valentine, D., & Forrest, T. (2018). „Cybersecurity Hygiene and Small to Medium-sized Enterprises (SMEs): Best Practices in Commercial Security.” *Journal of SME Operations and Security*.
- Xu, L., & Ng, P. (2020). „The Role of Ethics in Artificial Intelligence and Commercial Security Management.” *Ethics and Information Technology Journal*.
- Zell, A., & Jacobs, K. (2019). „Interplay of Distributed Ledger Technology (DLT) and Commercial Security: A Comprehensive Review.” *Distributed Ledger Technology Review*.
- Benton, J., & Char, W. (2020). „Incorporating Human Factors in Commercial Cybersecurity: An Overlooked Element?” *Journal of Human-Centered Security*.
- Dunn, E., & Valladares, L. (2018). „Smart Cities and Implications for Commercial Security Management.” *Urban Technology and Security Review*.
- Engel, K., & Fischer, B. (2020). „The Growing Relevance of Voice Assistants and Smart Homes in Commercial Security.” *Journal of Ambient Intelligence and Smart Environments*.
- Nash, K., & Livingston, P. (2019). „Automated Threat Intelligence: The Next Frontier in Commercial Security.” *Journal of Automated Security Analysis*.
- O'Donnell, S., & Pierce, Q. (2020). „Physical and Digital Security Convergence: A Management Perspective.” *Journal of Integrated Security Solutions*.
- Park, J., & Wu, L. (2018). „Edge Computing and Its Role in Modern Commercial Security Frameworks.” *Journal of Edge Computing*.
- Roberts, C., & Thompson, S. (2020). „Commercial Security in the Age of Deepfakes.” *Journal of Visual Computing and Security*.
- Singh, A., & Hassan, M. (2018). „Post-Quantum Cryptography: Implications for Commercial Security Operations.” *Journal of Quantum Information Science*.
- Tucker, P., & Vega, Y. (2019). „Social Engineering Attacks and Their Evolving Threat to Commercial Entities.” *Journal of Cybersecurity and Social Behavior*.
- Upton, Z., & Wallace, R. (2020). „Geospatial Analysis and Commercial Security: Modern Approaches and Techniques.” *Geospatial Intelligence Review*

ŘÍZENÍ LIDSKÝCH ZDROJŮ A VYBRANÁ TÉMATA MANAGEMENTU A LEADERSHIPU

Publikace pro management soukromých
bezpečnostních firem a pro další subjekty
v segmentu komerční bezpečnosti



PhDr. Mgr. Dávid Dömény, MBA

PŘEDSTAVUJEME ODBORNOU PUBLIKACI

DÁVIDA DÖMÉNYHO

Náš přispěvatel a odborný poradce PhDr. Mgr. Dávid Dömény, MBA, přichází na knižní trh s knižní novinkou pod názvem „Řízení lidských zdrojů a vybraná témata managementu a leadershipu“, jejíž zacílení prozrazuje již samotný podtitul – „Publikace pro management soukromých bezpečnostních firem a pro další subjekty v segmentu komerční bezpečnosti“.

Odborné pojednání se zaměřuje na význam řízení lidských zdrojů (HRM – z angl. Human Resources Management) jako klíčového prvku pro efektivní management a leadership v oblasti komerční bezpečnosti, v níž autor sám profesně a akademicky působí.

Cílem publikace je analýza hlavních přínosů HRM pro komerční bezpečnost, včetně zásadních principů, atributů a strategických cílů spojených s personální strategií. Zvláštní pozornost je zde věnována moderním technologiím a jejich vlivu na řízení lidských zdrojů, motivaci zaměstnanců a odměňování.

Autor zúročuje vlastní zkušenosti a poznatky z oblasti řízení pracovního týmu

a motivace zaměstnanců v komerční bezpečnosti, přičemž využívá i výsledků analýzy leadershipu a jeho vztahu k aktuálním trendům a problémům v oblasti bezpečnosti. V příslušných pasážích přibližuje a v kontextu komerční bezpečnosti aplikuje vybrané nástroje strategické analýzy, jako jsou SWOT analýza nebo Porterova analýza.

V poslední části publikace se autor zaměřuje na aktuální problémy ovlivňující trendy v managementu a leadershipu, jako jsou mimo jiné vliv a dopady pandemie COVID-19, koncept Age Management či vzdělávání zaměstnanců nad 50 let věku a jejich uplatnění v segmentu komerční bezpečnosti. Primární důraz přitom klade na společenskou odpovědnost a specifika řízení malých

a středních soukromých bezpečnostních firem.

Souhrnně řečeno, publikace poskytuje komplexní pohled na roli řízení lidských zdrojů a managementu v oblasti komerční bezpečnosti, s důrazem na aktuální trendy a výzvy i příležitosti v krátkodobém a střednědobém časovém horizontu.

Pokud by si chtěl někdo knihu objednat, pište na e-mail: david.domeny@email.cz

Redakce

KROUŽEK „MLADÝ STRÁŽNÍK“ A DALŠÍ ČINNOSTI NA POLI PREVENCE

Kroužek „Mladý strážník“ je pouze jednou z mnoha společných aktivit preventistů městských policíí v Karlovarském kraji.

Spolupráce v oblasti prevence se začala formovat v roce 2014. Zpočátku do ní byla zapojena jen města Karlovy Vary, Sokolov, Ostrov a Chodov, později se přidal Cheb, Mariánské Lázně, Františkovy Lázně a Nejedek.

Prvotním a stěžejním cílem bylo vytvoření pracovní skupiny preventistů městských policíí Karlovarského kraje a naplňování společných akcí zaměřených na bezpečnost v dopravě nebo posílení osobního bezpečí cílových skupin. Pak následovala postupná realizace naplánovaných akcí – od výroby společných motivačních a didaktických pomůcek, přes projekt „Notes strážníka Pavla“ pro 1. stupeň základních škol a několik osvětové vzdělávací kurzů až po Celostátní setkání preventistů městských policíí v roce 2019.

Významným počinem sdílení příkladů dobré praxe se stal právě kroužek „Mladý strážník“, který začali nejdříve realizovat strážníci v Chebu a následně

v Ostrově. V Karlových Varech vznikl jako navazující aktivita na „Notes strážníka Pavla“ a je určen dětem ve věku 9 až 12 let.

Činnost kroužku (zájmového útvaru) „Mladý strážník“ probíhá ve spolupráci s Domem dětí a mládeže v Karlových Varech, který zajišťuje jeho aktivity po administrativní a legislativní stránce. Děti se scházejí jednou týdně v Centru zdraví a bezpečí, které je pro podobné aktivity ideálním prostorem, a pod vedením preventistky městské policie získávají znalosti a dovednosti související s prací strážníků. Hlavním cílem je nastavit u dětí pozitivní přístup ke společenským normám. Důraz je kladen především na dobré vztahy v kolektivu, vzájemnou pomoc a spolupráci, rozvoj komunikace mezi dětmi a strážníky a zvýšení právního povědomí dětí.

Atraktivní je kroužek pro děti zejména díky zážitkům, které jim zprostředkovávají strážníci z výkonu služby – děti

se tak mohou seznámit se spoustou činností i pomůcek strážníků.

V závěru školního roku je pro děti připraven výlet do Muzea Policie ČR v Praze a při slavnostním zakončení obdrží mladí strážníci certifikát o absolvování kroužku, tričko a upomínkové předměty.

S dětmi se tím ale městská policie neloučí úplně. Společná setkávání pokračují i na 2. stupni základních škol a na středních školách, kde mají podobu besed týkajících se prevence v nejrůznějších oblastech negativních jevů. Záměrem kroužku je vytvořit z absolventů tým peer aktivistů, kteří budou fungovat jako mediátoři mezi školní mládeží a strážníky.

Mgr. Kamila Hofmanová

Městská policie Karlovy Vary
www.mpkv.cz



BEZPEČNOSTNÍ SYSTÉM S MLHOU

Bezpečnostní systémy (technologie) se za poslední roky staly běžnými zařízeními a setkáváme se s nimi takřka na každém kroku – v obchodech, na úřadech, na pracovištích a v posledních letech i v domácnostech.

Stejně jako mobilní telefon, notebook či televize potřebuje i zabezpečovací technika jednou za čas vyměnit či provést alespoň údržbu. Velmi často se setkávám s názorem, že výměna alarmu za nový a technicky vyspělejší není nutná, poněvadž stávající systém funguje a plně postačuje. Jaký by tedy měl být důvod k jeho výměně? Nějaký bonus?

Asi stojí za zmínku, že moderní zabezpečovací systémy již dávno nemají podobu jen nějaké klávesnice, pohybového čidla, sirény či centrály s napájecími a datovými kabely. Moderní systémy zdaleka nemusí být omezeny pouze na střežení objektů, nýbrž mohou zastávat funkce automatizace a optimalizace.

Ano, moderní bezpečnostní systémy pracují na platformě, kterou lze nazvat „chytrá domácnost“.

Koho by před několika lety napadlo ovládat vrata, bojler, světla či zásuvky s využitím zabezpečovacího systému? U dnešních zabezpečovacích systémů to ovšem není problém – docílíme toho za pomoci relátok či chytrých zásuvek nebo vypínačů.

Zabezpečovací systémy jsou prioritně zaměřeny na střežení a ochranu nemovitostí a všechny zmiňované prostředky můžeme mít pod kontrolou v jedné aplikaci. Navíc dnešní systémy umožňují zapojení drátové i bezdrátové, případně kombinované (hybridní).

Pokud máme doma čtyřnohého mazlíčka, můžeme ho klidně nechat doma i v době naší nepřítomnosti, jelikož většina čidel obsahuje tzv. pet imunitu, což znamená, že zvíře do velikosti 50 cm a váhy do 20 kg čidlo ignoruje.

A co pohyb záclon či pavouci na čidlech anebo létající hmyz? I tyto ruchy čidla zcela ignorují.

A jak je to s připojením na dohledové centrum? To je samozřejmě možné – i když máme díky aplikaci celý systém pod kontrolou, můžeme nemovitost napojit i na pult centralizované ochrany bezpečnostní agentury.



Běžné je dnes již otvírání vrat garáže.



Plynový kotel a obava z úniku CO₂? Žádný strach – detektor kouře a CO₂ si s tím dokáže poradit.



V případě úniku vody lze případné škody minimalizovat do několika sekund za použití detektoru úniku vody a uzavíracího ventilu vody.



Seniorům, kteří jsou sami doma, se může hodit SOS tísňové tlačítko.



Dnešní detektory mohou reagovat i na otřesy, rozbití a tříštění skla, pohyb či zvuky a zároveň mohou zajistit pořízení snímků pomocí čidel s fotoverifikací.

V poslední době se na českém trhu objevily vedle bezpečnostních systémů i takzvané mlhové systémy.

Mlhový systém propojený s bezpečnostním systémem je určen k zastrašení či dezorientaci narušitele, který vstoupí do zastřeženého prostoru. Po aktivaci vypustí mlhový systém hustou, zdravotně nezávadnou mlhu, s viditelností do jednoho metru. V aplikaci lze nastavit reakci na pohybové čidlo, dveře, okna anebo na SOS tísňové tlačítko.



Modely	Vlastnosti bezpečnostních mlhových systémů
MODULAR 200 AJAX READY	pokryje až 200 m ³ za 28 sekund  NOVISIBILITY
MODULAR 300 AJAX READY	pokryje až 300 m ³ za 40 sekund  NOVISIBILITY
MODULAR 400 AJAX READY	pokryje až 400 m ³ za 46 sekund  NOVISIBILITY
MODULAR 500 AJAX READY	pokryje až 500 m ³ za 48 sekund  NOVISIBILITY
MODULAR 800 AJAX READY	pokryje až 800 m ³ za 69 sekund  NOVISIBILITY

Existují i výkonnější modely, než uvádí tabulka – například nejvýkonnější Fast 14000 Pump Pro Plus Wide dokáže pokrýt prostor o velikosti 14 000 m³. Uvádíme pouze modely, které měla naše společnost možnost otestovat v našich bezpečnostních systémech.

Mlhový systém lze propojit s bezpečnostním systémem, a to tak, že do mlhového systému se zapojí dvě relátka od výrobce alarmu a pomocí aplikace se spárují – relátka ovládají dobu a délku výstřelu mlhy. Tento systém je možné ovládat i přes síťovou či wifi kartu.



Ukázky využití mlhových systémů v zahraničí:



Na benzinových stanicích.



V bankách.



Ve skladech.



V kancelářích.

CHRÁNÍME VÁS
JIŽ OD ROKU
1992



BEZPEČNOSTNÍ TECHNOLOGIE A SLABOPROUDÉ SYSTÉMY

ABAS IPS MANAGEMENT



WWW.ABASCO.CZ



SETKÁNÍ STRÁŽNÍKŮ

OBEČNÍCH POLICIÍ ZE STŘEDNÍ EVROPY V OLOMOUCI

Ve dnech 20.–22. 3. 2024 se na Právnické fakultě Univerzity Palackého v Olomouci konala VIII. mezinárodní konference obecních policíí. Jedná se o ojedinělé a největší mezinárodní setkání obecních a městských policíí ve střední Evropě, kterého je Bezpečnost s profesionály dlouholetým mediálním partnerem.

Domácí násilí, bezdomovectví, rizikové chování dětí a mládeže, ochrana měkkých cílů, kriminalita environmentální či kybernetická, navíc spojená s nárůstem generativní umělé inteligence. A samozřejmě současné otázky a problémy tížící obecní a městské policie, jejichž zástupci tvořili převážnou část auditoria konference, kterých se letos do Olomouce sjelo na 250. Spolu s nimi v něm zasedli jejich partneři ze státní správy, samospráv, integrovaného záchranného systému a bezpečnostních sborů, exekutivy, akademické sféry a dalších subjektů a organizací, včetně neziskového sektoru a dobrovolnických aktivit.



„Jedná se o ojedinělou platformu pro osobní setkávání a výměnu zkušeností ve čtyřech hlavních programových okruzích, a to bezpečný prostor, technologie, prevence a edukace, legislativa. A jak dokládají vyjádření účastníků také o významnou společenskou událost s nezapomenutelnou atmosférou,“ popisuje setkání manažer konference Pavel Boháč ze společnosti FT Technologies, která ojedinělé a největší mezinárodní setkání zástupců obecních a městských policíí ve střední Evropě organizuje. Konferenci, která se pravidelně koná za podpory profesních organizací strážníků z České republiky, Slovenska a Polska, zástupců policejních prezidií a v neposlední řadě Ministerstva vnitra ČR. Že má toto každoroční setkání strážníků patřičnou váhu, dokládá i fakt, že právě zde bylo

před dvěma lety mezi zástupci českých strážníků a prvním místopředsedou vlády a ministrem vnitra Vítem Rakušanem dohodnuto zřízení pracovní skupiny pro obecní policie mající za cíl zlepšení jejich postavení.

„Já si práce strážníků opravdu vážím. Nejen proto, že vidím tu souhru s celým integrovaným záchranným systémem, ale protože jsem dělal starostu a vím, jak je ta Vaše práce nelehká a chtěl bych Vám za to poděkovat,“ poznamenal v úvodu svého vystoupení ministr vnitra Vít Rakušan, který nad konferencí pravidelně přebírá osobní záštitu. Tentokrát k posluchačům promlouval a následně s nimi diskutoval prostřednictvím půlhodinové telekonference. Zdůraznil, že role strážníků při zabezpečování hlavně místních záležitostí veřejného pořádku v obcích je nezastupitelná a toto tvrzení záhy podložil několika čísly. *„Strážníci podle statistik ročně vyřeší více než 600 000 přestupků na místě, více než 2 000 000 jich oznámí správním orgánům a také oznámí 7 000 podezření o spáchání trestného činu. Zavedou a předvedou na policii 3 000 osob, které se dopouštějí nějakého protiprávního jednání. Ta čísla jsou až ohromující a svědčí o obrovském významu městských policíí, o tom, že je to etablovaná složka v bezpečnostním systému České republiky a potvrzuje většinou zcela bezproblémovou souhru mezi městskou a obecní policií a státní policií,“* zmínil Rakušan.

Nejvíce očekávaná část jeho vystoupení, jak bylo patrné i z tváří přítomných, se ovšem týkala aktuálních informací o připravované krizové legislativě a ukotvení českých obecních a městských policíí

v ní, a především pak problematiky sociálních výhod a benefitů strážníků – tedy témat, která posléze rezonovala v nejedné diskusi v plénu i kuloárech a také v následných vystoupeních.

Na debatu s ministrem vnitra vzápětí navázal se svým každoročním zhodnocením bezpečnostní situace v České republice za poslední rok a s možnou prognózou pro následující období policejní prezident generálporučík Martin Vondrášek. Také on hned v úvodu potvrdil, že spolupráce PČR s obecními a městskými policiemi je velice pozitivní a že si jí on i policie jako taková váží. *„Jsem zde minimálně počtvrté, abych se setkal a osobně pozdravil alespoň jednou ročně zástupce městských policíí a poděkoval jim. Jsou naším nejvýznamnějším partnerem v oblasti zajišťování veřejného pořádku pro občany naší země,“* zdůraznil mimo jiné Vondrášek, který si do Olomouce přichází vyslechnout náměty a připomínky strážníků k práci české policie každoročně. Loni to podle něj byla například otázka měření rychlosti, letos je to projednání témat spojených s výcvikem. *„Beru tuto konferenci jako důležitou platformu pro zpětnou vazbu, ale také možnost sdílet zkušenosti, navíc na mezinárodní úrovni. Je rovněž inspirací. Často jsou tady představovány nové technologie a my samozřejmě musíme v této překotné době umět držet krok, takže se zde dozvídáme spoustu informací z této oblasti, které pro nás mohou být zajímavé,“* doplnil policejní prezident.

Stejně tak vnímá konferenci jako skvělou platformu pro výměnu zkušeností i Milan Rakowský ze společnosti Au-



diopro, hlavního partnera konference, kterého vystoupení policejního prezidenta velmi zaujalo. „*I my se tady chceme naučit spoustu věcí, vyslechnout si potřeby policistů a strážníků, abychom mohli zdokonalovat naše řešení*“, vysvětlil Rakowský, podle kterého mohou být policistům a strážníkům nápomocní třeba právě v klíčové otázce komunikačních technologií v kontextu přechodu od radiostanic k datové komunikaci.

Generálporučík Vondrášek přitom nebyl jediným přednášejícím za českou policii, jenž v programu konference mezi více než dvaceti řečníky vystoupil. Policejní prezidium se tentokrát zaměřilo na přiblížení problematiky domácího násilí a kompetencí policistů a do diskuse vyslalo i další své experty, kteří hovořili například o kybernetické kriminalitě. Pozadu nezůstali ani kolegové ze slovenské policie, kterou zde reprezentoval plukovník Ivan Hapšták, viceprezident Policajného zboru pre migráciu, operativu a riadenie služieb Policajného zboru Slovenskej republiky. Slovenští účastníci konference vysvětlili posluchačům ve svých vystoupeních například aktuální legislativní kompetence slovenských strážníků a přiblížili i jedno z témat na konferenci dosud nediskutovaných – nové výzvy ve spolupráci městské a státní policie v oblasti nebezpečných materiálů, environmentální bezpečnosti a ochrany zvířat.

Jedním z hlavních témat letošního ročníku však byla umělá inteligence ve všech možných formách využití, jak v pozitivním, tak negativním smyslu – věnovalo se jí hned několik přednášek a v jejím duchu probíhal i tradiční doprovodný program prvního konferenčního dne. Organizátoři si tentokrát pro účastníky připravili opravdovou lahůdku – pozvání do světa umělé inteligence v podobě besedy s novinářem, komentátorem, stand-up komikem, podcasterem a technologickým guru Milošem Čermákem.

Setkání strážníků totiž zdaleka nenabízí pouze „tradiční poslech“ bezesporu zajímavých a inspirativních přednášek, a to nejen ze samotné praxe strážníků. Jeho součástí je rovněž bohatý doprovodný program, ať už společenský, či ryze pracovní, a to formou dalších význačných přidružených aktivit. „*Jednou z nich bylo celorepublikové jednání zástupců profesních sdružení obecních a městských policií z Česka a Slovenska, které se uskutečnilo v reprezentativních prostorách Krajského úřadu Olomouckého kraje*“, uvedl pro příklad manažer konference Pavel Boháč.

Olomoucká konference není podle Pavla Boháče pouze uzavřeným setkáním bezpečnostní komunity, ale má důležitý „zásah“ i do veřejného prostoru v podobě doprovodných akcí pro širokou veřejnost. Ta měla již potřeby možnost přijít si pro radu a seznámit se například s činností Bílého kruhu bezpečí (BKB), organizací poskytující pomoc obětem, svědkům a pozůstalým po obětech trestných činů. Své služby příchozím nabídli vyškolení pracovníci na prostranství před budovou právnické fakulty. „*Když se Bílý kruh bezpečí před dvěma lety prezentoval na naší konferenci poprvé, zaznělo, že by strážníci měli být takovým mostem mezi ním a oběťmi trestných činů. Je to pravda, protože jsou to obecní a městské policie, které mnohdy v terénu sbírají ty první střípky, že se děje něco nekalého, na co je potřeba odborně reagovat. Takže nás nesmírně těší, že můžeme nabídnout naši konferenci k prohlubování této spolupráce a pomáhat tak tento most stavět*“, zdůraznil Boháč.

Jeho slova potvrdila i Petra Pitrová, vedoucí olomoucké pobočky BKB, podle které je toto propojení určitě prospěšné k osvětě mezi strážníky. Ještě větší přínos pak spatřuje v tom, že určité napomáhá jejich potenciálním klientům, obětem trestných činů. Během těchto veřejných prezentací se totiž několik takových obětí rozhodlo učinit ten první, nejdůležitější a také nejtěžší krok a přišli svěřit se či pro radu k expertům na stánek. „*Jde nejen o ojedinělou příležitost, kdy můžeme v průběhu konference diskutovat s dalšími odborníky, ale zejména provádět velice důležitou osvětu a být nablízku těm, kteří naši pomoc potřebují*“, dodala Pitrová, podle níž byli i letos pracovníci na stánku kontaktováni s prosbou o pomoc ze strany obětí trestných činů.

Několik dnů před zahájením konference oznámili organizátoři ještě jednu doprovodnou aktivitu – zveřejnili jednu z novinek letošního ročníku: kampaň „Daruž život na VIII. mezinárodní konferenci obecních policií“, která měla za cíl oslovit nejen účastníky konference, ale i studenty univerzity a širší veřejnost k dárcovství krvetočným buňkám. V průběhu tohoto náboru se přihlásila řada potenciálních dárců a rýsují se, jak sami organizátoři potvrdili, po dohodě účastníků s náboráři i následné další náborové aktivity.

Olomoucká mezinárodní konference obecních policií je ojedinělým a největším mezinárodním setkáním obecních a městských policií ve střední Evropě. Jedná se nejen o společenskou událost, ale především o ojedinělou platformu

pro osobní setkávání a výměnu zkušeností. Hlavním organizátorem je společnost FT Technologies a.s. (založená roku 2004), která je považována za lídra trhu v oblasti poskytování informačních technologií pro obecní a městské policie. Spoluorganizátorem je Právnická fakulta Univerzity Palackého v Olomouci a hlavním partnerem osmého ročníku byla společnost Audiopro 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 také náš časopis Bezpečnost s profesionály.

Redakce



NĚKOLIK POZNÁMEK K PSYCHOLOGII VÝSLECHU DĚTÍ A MLADISTVÝCH

Na uvedené téma bylo sepsáno již množství publikací. V následujícím textu se zaměříme na některé psychologické zvláštnosti výslechové praxe dětí. Nebudou vyčerpány všechny, hlavně se dotkneme těch, které považujeme pro úspěšnost výslechové práce za významné.

Základní podmínkou při výsleších dětí, aby nedošlo k narušení jejich psychiky, je sestavení kvalitního týmu, v němž jsou zastoupeny všechny složky OČTŘ (orgánů činných v trestním řízení) lidmi, kteří mají s dětmi a mládeží náležité zkušenosti. Práce s tak citlivým organismem, jako je dětský, může totiž bez dostatečných zkušeností napáchat velkou škodu, táhnoucí se pak celým dalším životem dítěte. Proto by takovou práci měl vykonávat pouze zkušený a stabilní tým, který je dobře seznámen s celým případem, v jehož rámci je dítě vyslýcháno.

Na počátku 20. století panoval názor silně zpochybňující schopnost dětí podávat pravdivou výpověď – zdůrazňovala se přirozená tendence dětí dotvářet realitu ve fantazijních představách. Teprve na základě dlouhodobých zkušeností psychologů došlo ve výslechové praxi dětí ke změně a do současnosti převládá názor, že děti jsou běžně způsobilé poskytnout věrohodnou výpověď. Utváření výpovědi probíhá u dětí stejně jako u dospělých – s analogickými riziky.

Úspěch výslechu dítěte je závislý na mnoha faktorech:

a) Mentální zralost dítěte

Jsou-li v tomto směru oprávněné pochybnosti, je vhodné přizvat k výslechu a k následné konzultaci odborného psychologa. Je nutno brát v potaz problém dětské **suggestibility** – schopnosti přijímat nekriticky, automaticky a bezděčně cizí názory (zejména dospělých, rodičů) za své a převádět je do vlastního prožívání a chování. Je zjištěno, že v dětství je suggestibilita v průměru vyšší a teprve s přibývajícím věkem jí ubývá. Malé děti podléhají sugestivnímu působení častěji, snaží se vcítit či odhadnout očekávání vyslýchajícího a také mu vy-

hovět. Dítě pak při výslechu uvádí to, co si myslí, že chce vyslýchající slyšet. Proto je nutná velmi pečlivá příprava formulace jednotlivých otázek, a to tak, aby nenapovídaly a nenaznačovaly směr odpovědi.

b) Typ kladených otázek

Svá rizika mají zejména tzv. *otázky uzavřené*. Z výzkumů je známo, že i dospělí mají tendenci spíše přitakat, než říci ne. U dětí a mládeže je tato tendence ještě výraznější. Mají pocit, že záporná odpověď navozuje dojem odporu, a proto se jeví jako neslušná a nevychovaná. Tato tendence je výraznější zejména v situacích, kdy si není dítě svou vzpomínkou jisto, přičemž lze odpovědět slovy „já nevím, nepamatuji se“. Proto je žádoucí dítě při rozhovoru na tuto eventualitu upozornit, aby u něj nevznikl pocit nevychovanosti a neochoty.

Někdy se používají tzv. *kontrární otázky*. To jsou dotazy na to, co se objektivně nemohlo přihodit, s cílem, že dítě bude evidentní nesmysl vyvracet, a přitom spontánně zmíní důležité okolnosti, na které by si jinak nevzpomnělo.

c) Vliv vnějšího prostředí a celková atmosféra výslechu

Výslechová místnost i celková atmosféra by měly být uspořádány tak, aby pokud možno navozovaly pocit bezpečí a uklidnění. Vybavení místnosti by mělo být využitelné již pro první navázání kontaktu s dítětem (např. vhodné obrázky, hračky, knihy), za první navázání kontaktu odpovídá vyslýchající. K nejzávažnějším výsledkům dětí dochází často v souvislosti se sexuálním zneužíváním a týráním dítěte.

d) Akomodační (adaptační) syndrom

Vychází ze vzájemné známosti dospělého pachatele a dětské oběti, která se promítá do psychologie celého výsle-

chu. Děti zneužívané známým pachatelem často lžou, mění nebo odvolávají svá svědectví a střídají na první pohled protichůdné vzorce chování. Toto jejich chování je třeba vnímat jako součást vyrovnávání se s traumatem, dítě se snaží vnitřně strávit své traumatické zážitky, přizpůsobit se prožitě újmě.

Hlavní znaky akomodačního syndromu, jež popisují a vysvětlují chování a prožívání sexuálně atakovaných dětí:

Utajování – jde o tendenci dětí mlčet o zážitcích pramenících z pocitů provinění, myšlenka na přiznání v nich vyvolává různě motivovaný strach (např. z veřejného odsouzení, z odepření náklonnosti blízkých). Děti do 6–7 let nejsou schopné nechat si své zážitky jen pro sebe, utajování však klade na kognitivní, emoční a sociální předpoklady menší nároky než aktivní uvádění v omyl (studie doložily schopnost utajování již u 3–4letých dětí). Důležitá je otázka efektivnosti utajování. Tedy jak dlouho a s jakým úspěchem dovedou děti utajovat při různých způsobech doptávání se (např. je prokázáno, že 6–8leté děti mají problém efektivně utajovat skutečnost a poměrně rychle se prozradí).

Bezbrannost – dítě se cítí být vydáno pachateli na pospas, chápe, že by se mělo bránit, je však přesvědčeno, že na to nemá sílu, a má pocit, že se momentálně nemá na koho obrátit. Je-li odpor dítěte chabý, pachatel jej vnímá jako souhlas s jeho chováním a jednáním.

Bezvýchodnost – prolíná se často s bezbranností, dítě se považuje za špatné, protože snášelo či trpí aktivity pachatele. Pocit bezvýchodnosti posiluje mnohdy přítomnost dalších dětí v rodině. Dítě za ně cítí odpovědnost

a chápe situaci tak, že se za ně obětuje, až po určité době přivyká situaci. K vyrovnávání se situací používá dítě různé obranné mechanismy – mimo jiné dochází k tzv. disociaci, kdy dítě zasouvá do podvědomí stresující prvky myšlenek, např. zcela nevědomě vytěšňuje z paměti nepříjemné detaily, což pak při výslechu ztěžuje informace o celém průběhu činu.

Opožděné oznámení – mnohdy se objevuje nečekaně, jako reakce na jinou událost. Nejde tedy o včasné a uvědomělé řešení problému zneužívání, spouštěčem pro oznámení bývá zpravidla jiný konflikt v rodině nebo je dítě aktuálně trestáno za něco, co nevnímá tak dramaticky.

Odvolání obvinění – zneužívaná dětská oběť často mění svou výpověď či odvolává svá obvinění. Často jde o obtížné snesitelné obavy, jimiž dítě trpí, např. strach z rozbití rodiny nebo z toho, že bude označeno za lháře, nebo má k pachateli činu v podstatě kladný vztah.

Věrohodnost výpovědi dítěte – chyby při posuzování věrohodnosti dítěte mohou být způsobeny nekvalitním vedením výslechu. Je třeba striktně rozlišovat mezi lží dítěte a neuvědomělými sugescemi způsobujícími posuny ve výpovědi dítěte. Svou roli mohou hrát i pravděpodobné psychologické problémy, např. psychopatologické dispozice dítěte. Dítě také může být ke klamné výpovědi ovlivněno záměrně třetí osobou a ztožní se nevědomě s jinou skutečností.

Některé praktické zásady pro výslech dítěte při podezření na sexuální zneužívání

Malé děti (předškolního věku) by měly být vyslýchány jednou osobou, v délce 30 až 60 minut, přičemž je třeba zabránit všem rušivým vlivům. Pro začátek by měl vyšetřovatel používat jednoduché dotazy typu „chodíš do školky?“, „s čím si nejraději hraješ?“ apod. To je důležité pro prvotní navázání kontaktu, aby si vyšetřovatel udělal obrázek o celkové mentální zralosti dítěte. Není podstatné, zda je u výslechu hned od počátku žena či muž, nejlépe když jsou přítomni oba dva. Zcela zásadní je, aby se nikdo z nich vůbec v ničem nepodobal osobě pachatele (pokud jsou známy tyto informace). Hračky jsou vhodné pouze na počátku, při tvorbě kontaktu, během dalšího výslechu mohou odvádět pozornost.

Před vlastním výslechem je nutné navázat hlavně emocionální kontakt,

odstranit plachost a rozpačitost dítěte a počkat, až tzv. roztaje, získá důvěru. Toho lze nejlépe docílit otázkami, na které existuje snadná odpověď. To může signalizovat psychickou normu či případnou psychickou poruchu u dítěte. Poměrně brzy by mělo být dítě přeorientováno, samozřejmě nenásilně, na předmět výslechu. Je důležité dítěti vysvětlit, proč se s vyslýchajícím setkává, co ten bude od něj asi chtít, snažit se pro dítě zprvu nesrozumitelnou a nepřehlednou situaci přetvořit v přátelský obraz chápavého, kompetentního a trpělivého vyslýchajícího.

Při vlastním výslechu je dobré dítě nejdříve povzbudit, aby o celé situaci vyprávělo volně, teprve následně je vhodné klást detailní, upřesňující a jiné otázky.

V průběhu celého výslechu je důležitý oční kontakt. Ten by měl být přirozený, ne vynucený. Pokud se mu dítě vyhýbá, lze mu nabídnout kreslení, to umožní vyhnout se očnímu kontaktu přirozeným způsobem. Pokud se však dítě vyhýbá kontaktu s vyslýchajícím stále, může to znamenat, že je unavené nebo jej otázky nepřiměřeně zatěžují, případně intelektově a emočně nezvládá situaci. Při podezření na jakoukoli psychickou zátěž dítěte je třeba v průběhu výslechu otázky vhodněji přeformulovat a spíše se ptát na pocity dítěte než na faktické události, které se odehrály – k nim se lze postupně vrátit.

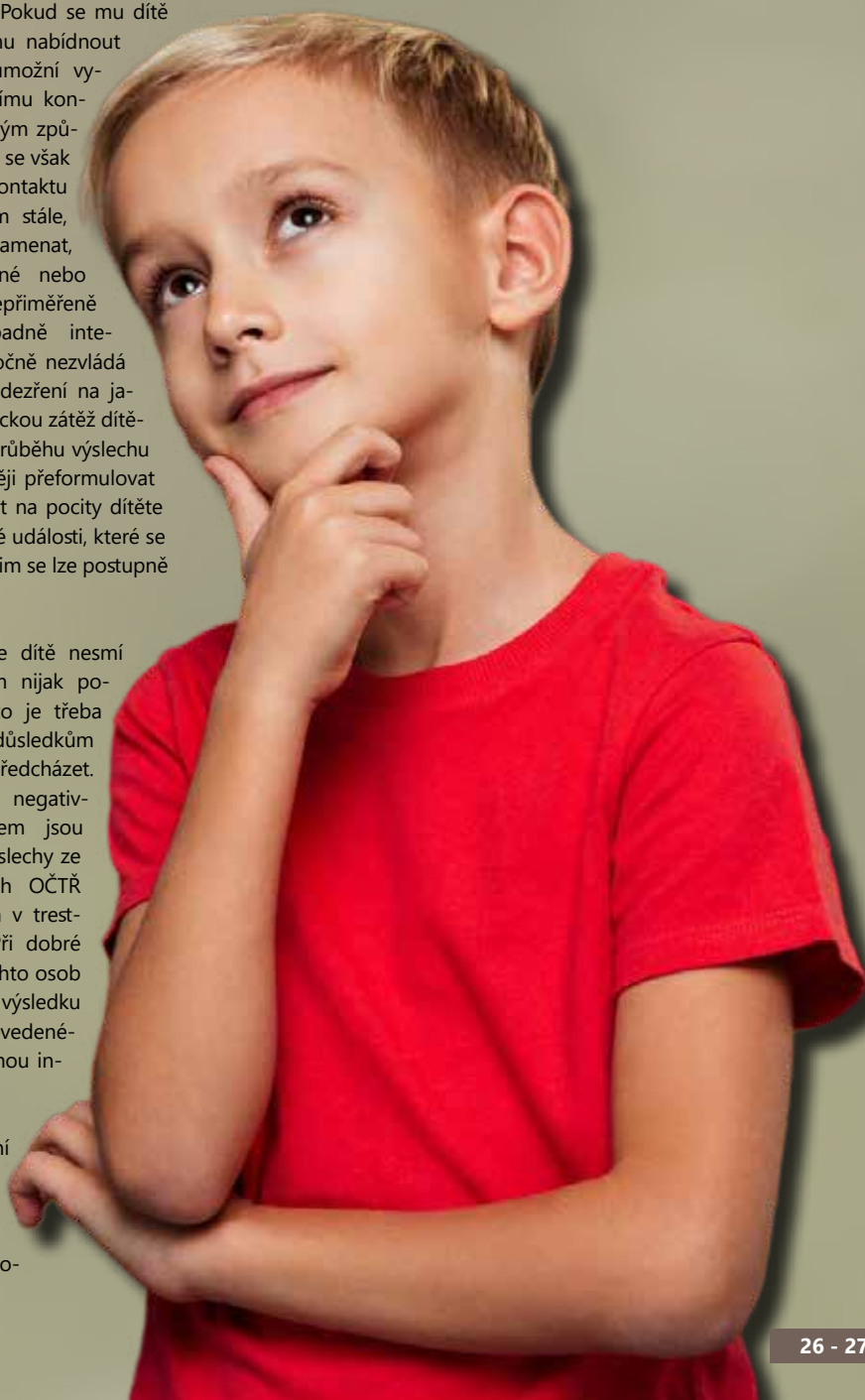
Zásadní je, že dítě nesmí být výslechem nijak poškozeno. Proto je třeba negativním důsledkům vyšetřování předcházet. Nejčastějším negativním důsledkem jsou opakované výslechy ze strany různých OČTŘ (osob činných v trestním řízení). Při dobré spolupráci těchto osob lze čerpat z výsledku výslechu provedeného pouze jednou instancí.

Při vyšetřování např. sexuálního násilí je dítě při výslechu konfronto-

váno se spoustou věcí, jimž nerozumí. Proto je nutná pečlivá a přesná protokolace celé situace, stejně tak spolupráce s referenčními osobami (zpravidla se jedná o rodiče dítěte). Ti často trpí pocity viny, vyčítají si nedostatečnou péči o dítě. Psychicky stabilní rodiče jsou schopni se se situací vyrovnat, labilní rodiče trpí přehnanými výčitkami a mají blízko k agresivnímu chování zacílenému proti pachateli nebo policii jako složkám, které zanedbání dozoru ze strany rodičů odhalily.

Optimální je přizvat k výslechu někoho, kdo má zkušenosti s dětskou výchovou, mohou to být i psychologové či pedagogové, kteří mohou výraznou měrou přispět ke správnému vedení výslechu.

Mgr. Zoja Kalivodová



DETEKTIVNÍ OCHRANA SPORTOVNÍCH, KULTURNÍCH A SPOLEČEN- SKÝCH AKCÍ – OCHRANA MĚKKÝCH CÍLŮ

Sportovní, kulturní a společenské akce v občanské demokratické společnosti jsou z hlediska bezpečnosti zajišťovány především komerčně bezpečnostními opatřeními, případně bezpečnostním servisem vlastních provozovatelů. Vyplývá to již ze zákonné úpravy – občanského zákoníku. Každý vlastník, tedy i provozovatel, má nejen práva, ale i povinnosti. K nim patří i povinnost chránit svůj majetek a dbát na veřejný pořádek. Policii ČR a obecním policiím připadá ze zákona subsidiární povinnost.

V první části článku se zaměřím na některé stěžejní formy detektivní ochrany měkkých cílů. Vycházím při tom z nejčastějších forem napadání měkkých cílů, kterými jsou:

**BEZPEČNOSTNÍ OCHRANA
SPORTOVNÍCH, KULTURNÍCH
A SPOLEČENSKÝCH AKCÍ**

==

**OCHRANA TZV.
MĚKKÝCH CÍLŮ**

přestupky proti občanskému soužití, trestné činy výtržnictví, útoky proti životu a zdraví, teroristické útoky.

Komerční bezpečnostní opatření stejně jako bezpečnostní servis lze jako svépomocná bezpečnostní opatření rozdělit do dvou základních skupin:

- bezpečnostní opatření prováděná službou ochrany majetku a osob,
- bezpečnostní opatření prováděná detektivními činnostmi.

DETEKTIVNÍ PRŮZKUM¹

Základ činnosti při detektivní ochraně sportovních, kulturních a společenských akcí (ochraně měkkých cílů) tvoří:

a) Detektivní průzkum v místě konání předmětné akce

Jde v podstatě o využití detektivní metody detektivního osobního pátrání, v jejímž rámci detektiv v místě budoucí akce tipuje slabá (riziková) místa – například:

- možná přístupová místa a místa odchodu mimo řádnou propustkovou službu,

nosti a spolehlivosti, a snaží se s nimi navázat kontakt. Další možností je, že detektiv v rámci detektivního průzkumu v předpokládaném závadovém prostředí infiltruje již existující lidský informační zdroj do tohoto prostředí. V rámci tohoto průzkumu detektiv dále tipuje možné agresivní osoby a jejich vůdce.

Velmi významnou roli v tomto detektivním průzkumu zaujímá detektivní legenda. Mnohdy je třeba připravit i více kvalitních legend. Těmi je třeba zakrýt skutečnou činnost a skutečný zájem detektiva. Legenda poskytuje detektivovi krytí, které musí zajistit bezproblémový pobyt detektiva v předmětném závadovém prostředí, případně ve více závadových prostředích. Legenda či legendy musí detektiva kryt při jeho kontaktech se závadovými osobami v daném závadovém prostředí. Připravit dobrou legendu, která je tato krytí schopna zajistit, není vůbec jednoduchou záležitostí.

c) Detektivní průzkum v době konání akce

V rámci této činnosti detektiv v místě a v době konání akce:

- tipuje podezřelé osoby,
- sleduje pohyb závadových osob vytipovaných v rámci předchozí činnosti,
- předává potřebné informace službě ochrany majetku a osob, případně pořadatelům, obecní policii nebo Policii ČR.

V rámci detektivní ochrany sportovních, kulturních a společenských akcí (ochrany měkkých cílů) realizuje detektiv různé formy detektivní činnosti, jejichž význam spočívá v tom, že pomáhají detektivovi již od počátku správně stanovit a vytyčit další zaměření jeho postupu.

K formám detektivní činnosti patří:

V souvislosti s ochranou měkkých cílů se zpravidla myslí činnost služeb. Pod pojmem soukromá detektivní činnost rozumíme komerční detektivní činnost, tedy činnost, která je vykonávána na smluvním základě za finanční úhradu, a detektivní servis, který představuje detektivní činnost realizovanou vlastními silami organizace (pořadatele) ve prospěch vlastní organizace (pořada-

- místa, kde by se mohl případný pachatel skrývat,
- místa, kde by mohl mít pachatel ukrytou zbraň apod.

b) Detektivní průzkum v předpokládaném závadovém prostředí

V rámci tohoto průzkumu si detektiv tipuje možné lidské informační zdroje, a to z hlediska jejich vhodnosti, schop-



KPKB
KOMERČNÍ
PODNIKŮV
KOMERČNÍ
BEZPEČNOSTI
ČESKÉ REPUBLIKY

a) *charakteristika obecných cílů*, jimiž má být detektivní činností v konkrétním případě v procesu realizace zakázky dosaženo,

b) *formulace obecných cílů*, jimiž má být detektivní činností v konkrétním případě v procesu realizace zakázky dosaženo.

Jde o obecný model rozhodování detektiva, kdy detektiv ještě před sebou nemá jasné a jednoznačně vymezený cíl a nemá ještě propracovány všechny možné alternativy (verze) postupů ani jejich důsledky. Má však v obecné podobě správně zvolenou formu detektivní činnosti a teprve poté konkrétně stanoví, čeho má být dosaženo.

DETEKTIVNÍ PÁTRÁNÍ ³

V rámci zajišťování bezpečnosti a veřejného pořádku při sportovních, kulturních a společenských akcích dochází i k tomu, že se ztrácejí malé děti (zatoulají se). Pak zpravidla nastoupí detektiv a provádí pátrání. Detektivní pátrání je forma detektivní činnosti směřující k nalezení hledaného objektu – osoby, věci.

Detektivní pátrání je jedním ze základních druhů (forem) detektivní činnosti. Pátrání po osobách a věcech může být, a zpravidla také je, realizováno souběžně s pátráním Policie ČR, kdy klient (zákazník detektivní činnosti) se z různých důvodů rozhodne dát po osobě (osobách) či věcech pátrat detektivní kanceláři (detektivem). Pátrání po osobách a věcech ale může být kromě toho prováděno v celé řadě dalších případů, kdy to Policii ČR ze zákona nepřísluší, a proto ho také neprovádí. Detektivní pátrání po osobách a věcech je možno provádět v některých případech individuálně, v jiných případech týmově. Součinnost a spolupráce při pátrání po osobách a věcech směřuje k získání co možná nejúplnějších (optimálních) informací s cílem učinit si nezbytný přehled, aby bylo možno stanovit verze a směry pátrání.

DETEKTIVNÍ DOHLED A BODYGUARDING ⁴

V průběhu sportovních, kulturních a společenských akcí detektiv provádí dohled nad vytípanými narušiteli. Rovněž může provádět osobní ochranu osob určených pořadatelem. Detektivní dohled je formou detektivní činnosti, jež spočívá v souhrnu úkonů a opatření využívajících různých metod detektivní činnosti, metod kriminalistiky, metod kriminologie, sociologie, psychologie a řady forenzních disciplín, metod policejní praxe, zejména kriminální policejní praxe, a dalších, které směřují ke

kontrole dodržování žádoucího stavu a ke včasnému zjištění (odhalení) nežádoucích odchylek od stavu žádoucího. V rámci ochrany sportovních, kulturních a společenských akcí připadá v úvahu i doprovod VIP osob. Tuto formu ochrany nazýváme bodyguardingem. Osobní ochrana osob (bodyguarding) může být prováděna i skrytým či konspirativním způsobem.

DETEKTIVNÍ PROVĚRKA ⁵

Detektivní prověrka představuje základní činnost detektiva jednak před sportovní, kulturní či společenskou akcí nebo i po ní. Zaujímá v komerční detektivní činnosti jakési výsadní postavení a v podstatě prolíná i do dalších forem detektivní činnosti, kterými jsou:

- detektivní pátrání
 - detektivní dohled a ochrana (bodyguarding)
 - detektivní prověrka
 - detektivní rozkrývání (rozpracování, vyšetřování)
 - detektivní zpravodajství
- Velmi významným zdrojem informací jsou přitom otevřené zdroje.

Cílem detektivní prověrky je prověřit:

- jednání a chování zájmových osob, a to jak v minulosti, tak v současnosti, a získání významných, z hlediska předmětného případu relevantních informací,
- prověření věrohodnosti informací v konkrétním případě.

Prověřování může mít různé podoby – děje se např. jako:

- samostatný, jednorázový postup,
- součást celého cyklu detektivní činnosti (detektivní zakázky),
- prověrka zájmového prostředí (z hlediska výskytu negativních skutečností či osob),
- prověrka podnikatelského subjektu či jiné organizační struktury (firmy, společnosti, sdružení, hnutí či jiné organizace, instituce).

DETEKTIVNÍ ROZKRÝVÁNÍ PROTIPRÁVNÍHO JEDNÁNÍ ⁶

Jde zejména o rozkrývání připravovaného protiprávního jednání závodovými skupinami či jednotlivci před zahájením sportovní, kulturní či společenské akce. Pokud je příprava protiprávního jednání odhalena, pak detektiv spolupracuje nejen se službou ochrany majetku a osob, ale podle závažnosti informuje obecní policii či Policii ČR. V rámci této detektivní formy

je uplatňována i detektivní prověrka a detektivní zpravodajství.

DETEKTIVNÍ ZPRAVODAJSTVÍ ⁷

Představuje formu detektivní činnosti směřující k získání informací o připravovaných protiprávních jednání, o činnosti pachatelů takovýchto jednání apod.

U formy detektivního zpravodajství je zajímavá skutečnost, že touto formou není v praxi naplňován obsah komerčního zpravodajství a zpravodajského servisu. Proč je to třeba zmínit? Komerční či zpravodajský servis (dále jen zpravodajství) má totiž i další formy, kterými jsou:

- zpravodajská informatika,
- zpravodajská sociotechnika neboli zpravodajské sociální inženýrství,
- zpravodajské hry,
- zpravodajská prověrka (je v podstatě aplikací detektivní prověrky do procesu zpravodajství),
- zpravodajská lobbistika (jedná se v podstatě o vlivové působení).

Více méně jde o teoretické členění, neboť detektivní činnost je ve své podstatě z velké části činností zpravodajskou a zpravodajská činnost je nedílnou součástí činnosti detektivní.

Rozdíl mezi klasickou detektivní činností a zpravodajskou činností spočívá v předmětu (objektu) zájmu (působení).

V rámci detektivně zpravodajského průzkumu jsou naplňovány formy jak detektivní, tak zpravodajské činnosti. Základem detektivní i zpravodajské činnosti jsou informace. To samozřejmě platí v plném rozsahu při detektivně zpravodajském průzkumu v souvislosti se sportovními, kulturními a společenskými akcemi.

Uvedené formy detektivní činnosti jsou realizovány prostřednictvím metod a prostředků detektivní činnosti. Základním prostředkem v činnosti detektiva je v současné době mobilní telefon umožňující pořizování fotografií, natáčení videí či nahrávání audiozáznamů.

DETEKTIVNÍ LEGENDA ⁸

Představuje základ veškeré detektivní či zpravodajské činnosti. Je obsažena při realizaci kterékoli detektivní formy a je základem realizace veškerých detektivních metod. Cílem legendy je zakrýt skutečný záměr (skutečnou činnost detektiva či zpravodajce). Jejím cílem je tedy krytí.

Detektivní legendu je třeba chápat jako⁹ nepravdivé, smyšlené podání s pravdivými prvky, které je pro danou

KOMERČNÍ DETEKTIVNÍ ČINNOST DETEKTIVNÍ ZAKÁZKA

Formami je realizována
detektivní činnost

FORMY DETEKTIVNÍ ČINNOSTI:

- ❖ DETEKTIVNÍ PÁTRÁNÍ
- ❖ DETEKTIVNÍ PROVĚRKA
- ❖ DETEKTIVNÍ DOHLED
- ❖ DETEKTIVNÍ ROZPRACOVÁNÍ
- ❖ KOMERČNÍ ZPRAVODAJSTVÍ

DETEKTIVNÍ DOKUMENTOVÁNÍ

Metodami
jsou realizovány
formy DČ

METODY DETEKTIVNÍ ČINNOSTI:

- DETEKTIVNÍ VYTĚŽOVÁNÍ
- DETEKTIVNÍ POZOROVÁNÍ
- TVORBA A PROVĚŘOVÁNÍ DETEKTIVNÍCH VERZÍ
- DETEKTIVNÍ LEGENDA
- DETEKTIVNÍ KOMBINACE
- DETEKTIVNÍ INFORMAČNÍ PRONIKNUTÍ
- DETEKTIVNÍ PROVĚRKA MÍSTA
- DETEKTIVNÍ VYHODNOCOVÁNÍ EVIDENCÍ, REGISTRACÍ A ARCHIVŮ
- DETEKTIVNÍ VYHODNOCOVÁNÍ DOKUMENTŮ
- DETEKTIVNÍ OSOBNÍ PÁTRÁNÍ
- DETEKTIVNÍ DEZINFORMACE
- DETEKTIVNÍ FYZICKÁ OCHRANA;
- VEDENÍ A HODNOCENÍ DETEKTIVNÍCH EVIDENCÍ

chvíli neprověřitelné ze strany osoby (osob), na niž působí a kterou má ovlivnit ve prospěch detektiva. Úspěšná detektivní legenda musí vycházet z objektivně existující situace působící na osobu (osoby), již je určena. Pravdivé prvky musí být ze strany osoby (osob), proti níž legenda směřuje, lehce ověřitelné, případně známé.

DETEKTIVNÍ DEZINFORMACE ¹¹

I když to je na první pohled paradoxní, významná je metoda detektivní dezinformace, která se využívá:

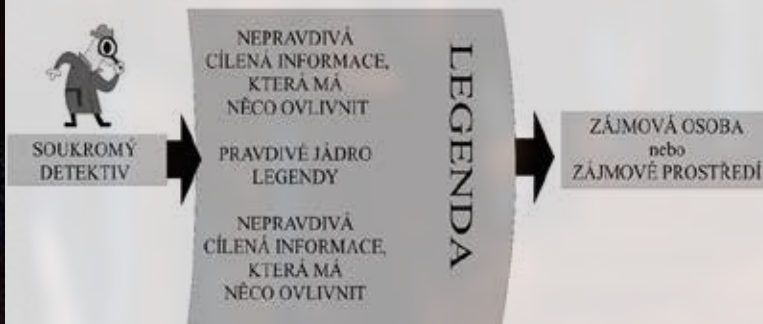
- jako součást detektivní legendy (její nepravdivé krycí části),
- jako nedílná součást detektivní kombinace,
- jako samostatná činnost směřující k ovlivnění – lobbyingu, vlivovému působení.

Nesmí ale nikdy směřovat proti státnímu orgánu – úřadu, protože tím by mohla být naplněna skutková podstata trestného činu.

Dezinformace je v podstatě záměrně nepravdivá nebo zkreslená informace.

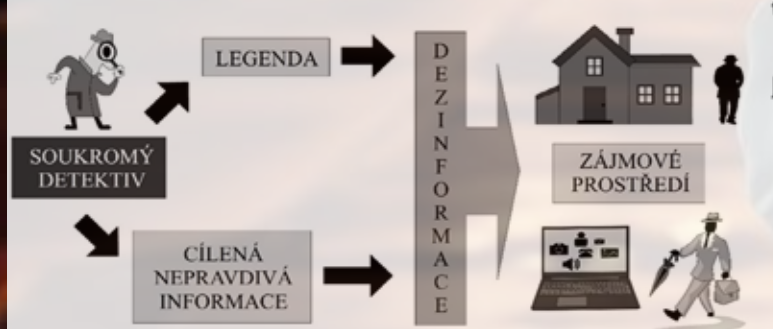
10

METODA - DETEKTIVNÍ LEGENDA:



12

METODA - DETEKTIVNÍ DEZINFORMACE:



KPKB
K O M E R Č N Í
P O D N I K Ů
K O M E R Č N Í
B E Z P Ě Č N O S T I
Č E S K É R E P U B L I K Y

DETEKTIVNÍ OSOBNÍ PÁTRÁNÍ¹³

Plní specifickou funkci v rámci detektivní činnosti. Detektiv zpravodajec si v jejím průběhu rozšiřuje a aktualizuje osobní a místní znalost. Tato metoda obsahuje v průběhu realizace prvky dalších metod (metoda pozorování, metoda vytěžování apod.). Krytí realizace této metody je prováděno pomocí metody legendy a metody dezinformace.

Metodu osobního pátrání je třeba chápat jako soustavnou aktivitu detektiva realizovanou v rámci jeho každodenní činnosti. Jedná se o nejčastěji užívanou komplexní (souhrnnou či kombinovanou) metodu detektivní činnosti. V jejím rámci detektiv (detektiv zpravodajec) přímo a bezprostředně užívá veškerých detektivních prostředků, způsobů a postupů za účelem získání

informací o věcech a písemnostech, které by mohly v budoucnu sloužit jako důkazy.

Jde tedy o jeden ze způsobů využívání detektivů k naplňování obsahu jednotlivých forem detektivní činnosti. Detektivní osobní pátrání není a nemůže být pouhým souhrnem různých opatření. Je totiž složitým, vnitřně diferencovaným systémem detektivních postupů a opatření, který plní specifickou funkci v rámci realizace detektivní zpravodajské činnosti. Detektivnímu osobnímu pátrání, stejně jako každému systému, přísluší určitá množina prvků (subsystémů), jimiž jsou další jednotlivé metody detektivní činnosti.

DETEKTIVNÍ PROHLÍDKA MÍSTA

Při provádění detektivní prohlídky místa v rámci ochrany při sportovních,

kulturních a společenských akcích je velmi důležité obeznámit se dopředu s prostorem, kde se mají akce připravovat, následně odehrávat a zpravidla i kde po skončení akce může dojít ke střetům mezi protistranami. V takových případech je vhodné využití metody detektivní prohlídky místa (rekognoskace). I v tomto případě detektiv kryje svůj pohyb a pobyt legendou.

JUDr. František BRABEC
čestný prezident ČKDS
výkonný ředitel ČS ESOB

15

METODA - DETEKTIVNÍ OHLEDÁNÍ - PROVĚRKA MÍSTA



Poznámky pod čarou:

- 1) Srov. BRABEC, František a kol. SOUKROMÉ DETEKTIVNÍ SLUŽBY, Praha 1995, EUROUNION, ISBN, str. 132.
- 3) Srov. KAMENÍK, Jiří; BRABEC, František a kol. KOMERČNÍ BEZPEČNOST 2, Praha 2019, vydavatel Wolters Kluwer ČR, ISBN 978-80-7598-303-9, str. 248 & Srov. BRABEC F. a kol. SOUKROMÉ DETEKTIVNÍ SLUŽBY, Praha 1995, EUROUNION, ISBN 80-85858-16-9, str. 133.
- 4) Srov. KAMENÍK, Jiří; BRABEC, František a kol. KOMERČNÍ BEZPEČNOST 2, Praha 2019, vydavatel Wolters Kluwer ČR, ISBN 978-80-7598-303-9, str. 265. & Srov. BRABEC F. a kol. SOUKROMÉ DETEKTIVNÍ SLUŽBY, Praha 1995, EUROUNION, ISBN 80-85858-16-9, str. 132.
- 5) Srov. KAMENÍK, Jiří; BRABEC, František a kol. KOMERČNÍ BEZPEČNOST 2, Praha 2019, vydavatel Wolters Kluwer ČR, ISBN 978-80-7598-303-9, str. 250. & Srov. BRABEC, František a kol. SOUKROMÉ DETEKTIVNÍ SLUŽBY, ISBN 80-85858-16-9, Praha 1995, EUROUNION, str. 133.
- 6) Srov. KAMENÍK, Jiří; BRABEC, František a kol. KOMERČNÍ BEZPEČNOST 2, Praha 2019, vydavatel Wolters Kluwer ČR, ISBN 978-80-7598-303-9, str. 242. & Srov. BRABEC F. a kol. SOUKROMÉ DETEKTIVNÍ SLUŽBY, Praha 1995, EUROUNION, ISBN 80-85858-16-9, str. 133.
- 7) Srov. KAMENÍK, Jiří; BRABEC, František a kol. KOMERČNÍ BEZPEČNOST 2, Praha 2019, vydavatel Wolters Kluwer ČR, ISBN 978-80-7598-303-9, str. 253.
- 8) Srov. KAMENÍK, Jiří; BRABEC, František a kol. KOMERČNÍ BEZPEČNOST 2, Praha 2019, vydavatel Wolters Kluwer ČR, ISBN 978-80-7598-303-9, str. 274-275. & Srov. BRABEC, František a kol. SOUKROMÉ DETEKTIVNÍ SLUŽBY, Praha 1995, EUROUNION, ISBN 80-85858-16-9, str. 192.
- 9) Srov. KAMENÍK, Jiří; BRABEC, František a kol. KOMERČNÍ BEZPEČNOST 2, Praha 2019, vydavatel Wolters Kluwer ČR, ISBN 978-80-7598-303-9, str. 274-275. & Srov. BRABEC F. a kol. SOUKROMÉ DETEKTIVNÍ SLUŽBY, Praha 1995, EUROUNION, ISBN 80-85858-16-9, str. 192.
- 10) BRABEC, František. DETEKTIVNÍ LEGENDA, Praha 2001, nová grafická úprava ZAPLETAL, Karel, 2021.
- 11) Srov. KAMENÍK, Jiří; BRABEC, František a kol. KOMERČNÍ BEZPEČNOST 2, Praha 2019, vydavatel Wolters Kluwer ČR, ISBN 978-80-7598-303-9, str. 284.
- 12) BRABEC, František. DETEKTIVNÍ ZPRAVODAJSKÁ DEZINFORMACE, Praha 2001; nově grafické zpracování ZAPLETAL, Karel, Praha 2021.
- 13) Srov. BRABEC František. SOUKROMÉ DETEKTIVNÍ SLUŽBY, Praha 1995, Eurounion, ISBN 80-85858-16-9, str.167. & Srov. KAMENÍK, Jiří; BRABEC, František a kol. KOMERČNÍ BEZPEČNOST 2, Praha 2019, vydavatel Wolters Kluwer ČR, ISBN 978-80-7598-303-9, str. 289-290.
- 15) BRABEC František, Praha 2023.VYHODNOCOVÁNÍ DATABÁŽÍ, obrázek je složen z komponentů stažených z internetu.

ČLENOVÉ KOMORY PODNIKŮ KOMERČNÍ 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 Pancēr, s. r. o.

K dubu 2330/2b, Chodov
149 00 Praha 4
www.pancer.cz



European Security Solutions s.r.o.

Tyrsova 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



3S security s.r.o.

Holušická 2253/1
148 00 Praha 4
www.3ssecurity.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



SYBENAM - Systém bezpečnosti na míru

U Klavírky 2627/7
150 00 Praha 5
www.sybenam.cz



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



RAM SECURITY s. r. o.

Na Výhledu 139
250 66 Zdíby
www.security-cz.eu



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.

Jeřábková 419
230 73 Radonice
www.solidita.cz



APEurope s. r. o.

Kaprová 42/14
110 00 Praha 1
www.apecurope.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.abas.cz



Preventa Service s.r.o.

Kutuzovova 547/13
703 00 Ostrava – Vítkovice
www.preventa.cz



Synergia management czech s.r.o.

Drtinova 557/10
150 00 Praha 5
www.synergia.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



SEKURO & Group s.r.o.

Na Mlýnici 33/1a
702 00 Ostrava
www.sekuro.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



OKO 69 s.r.o.

Březinova cesta 192/1
412 01 Litoměřice
www.oko69.cz



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 Revnice
info@incrisco.cz



Národní stálá konference o bezpečnosti (NSKB), z.s.

Chudenická 1059/30
102 00 Praha 10
www.nskb.cz

Gatun Group, s.r.o.

Italská 2581/67
120 00 Praha 2
www.gatun.cz



ČVUT - Fakulta biomedicínského inženýrství

Sportovců 2311, Kladno
https://www.fbmi.cvut.cz/



Ing. Martin Neuschl

Šachetní 391
261 01 Příbram

