KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČESKÉ REPUBLIKY

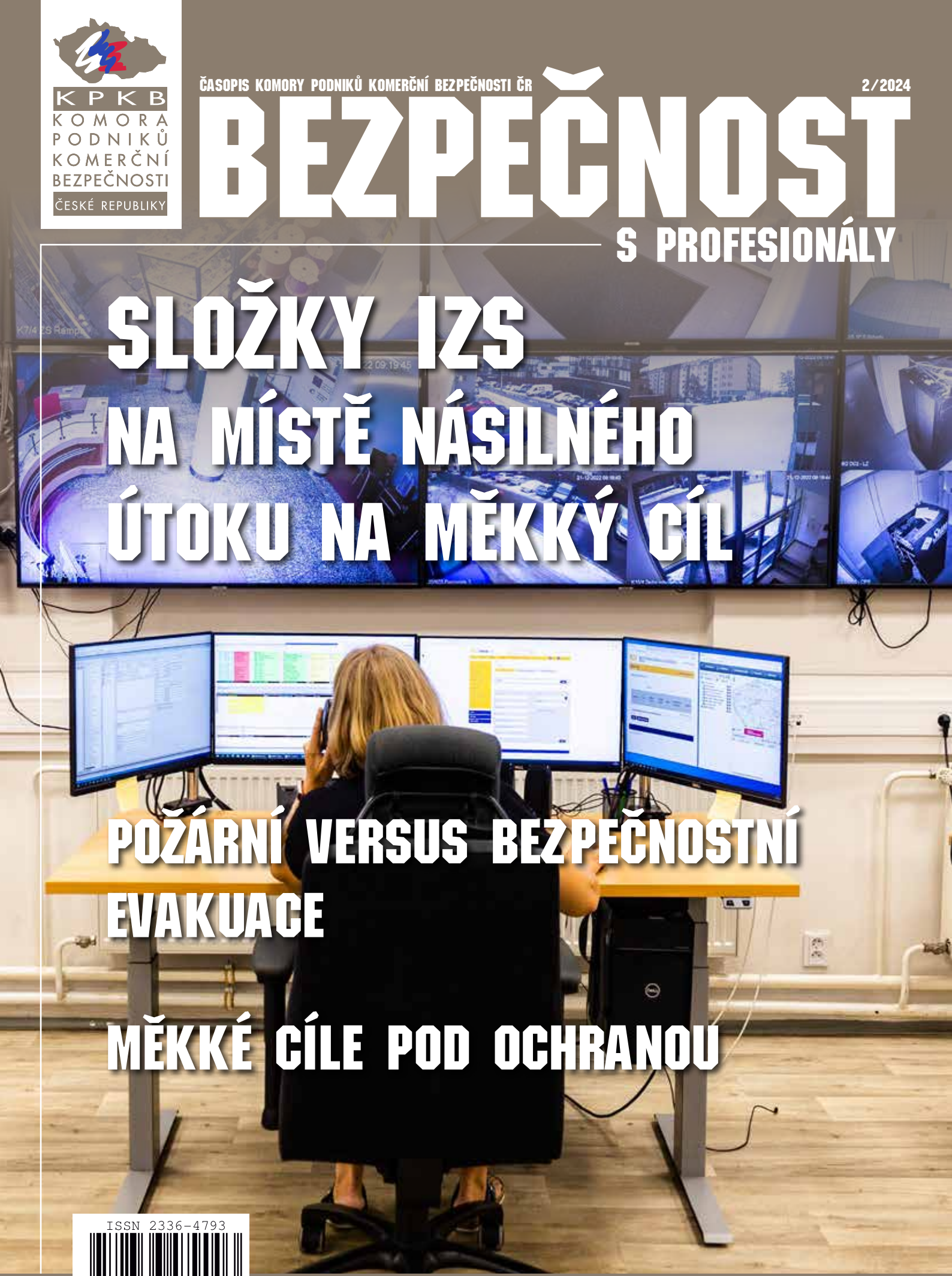
ČASOPIS KOMORY PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČR

2/2024

BEZPEČNOST

S PROFESIONÁLY

SLOŽKY IZS NA MÍSTĚ NÁSILNÉHO ÚTOKU NA MĚKKÝ CÍL



POŽÁRNÍ VERSUS BEZPEČNOSTNÍ EVAKUACE

MĚKKÉ CÍLE POD OCHRANOU

ISSN 2336-4793
9 772336 479003

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI
ČESKÉ REPUBLIKY

BEZPEČNOST
S PROFESIONÁLY

Šéfredaktor
Mgr. Bc. Kateřina Poludová, DiS.

Jazyková spolupráce
PhDr. Alena Hasáková

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

Inzerce
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

Na zadní straně obálky
členové KPKB ČR

ÚVODNÍ SLOVO

Vážení čtenáři,

je mi potěšením setkat se s Vámi opět u stránek našeho časopisu Bezpečnost s profesionály.
Věřím, že jste si letošní léto užili plnými doušky a podařilo se Vám najít čas i na trochu oddechu.

Přestože je léto příznačně časem dovolených, náš redakční tým ani o prázdninách nelenil a ve spolupráci s dopisovateli z řad odborníků na problematiku bezpečnosti pro Vás připravil řadu zajímavých příspěvků. Převážně ještě s tématy konference Ochrana měkkých cílů pořádané naší Komorou ve spolupráci s českou pobočkou AFCEA a Fakultou biomedicínského inženýrství ČVUT. Konference proběhla 13. června 2024 v pražském kongresovém hotelu Olšanka již po osmé a pozvání na ni přijaly více než tři stovky účastníků a zajímavých partnerů. Vnímáme ji i do budoucna jako velmi přínosnou platformu pro prezentaci nových trendů v oblasti bezpečnosti a možnost setkávání odborné veřejnosti.

Ovšem i na prahu podzimu se můžeme těšit na zajímavé odborné i společenské aktivity, a tím i nové pracovní výzvy.

Jednou z aktuálně připravovaných akcí je Mezinárodní konference obecních policií, která se uskuteční ve dnech 23.–25. října 2024 v Kulturním a společenském středisku Střelnice v Českém Těšíně. Jejím hlavním cílem bude výměna zkušeností z práce obecních/městských policií, která by měla přispět ke zkvalitnění práce strážníků nejen v obcích a městech České republiky, jelikož se jí zúčastní i zájemci a odborníci ze sousedních států. A my si opět nenecháme některá zajímavá vystoupení a přednášky ujít.

Na závěr nelze ovšem nepřipomenout, že konec léta nás bohužel zaskočil povodňovým přívalem, který se ne všude podařilo zvládnout bez újmy na majetcích, či ojediněle dokonce na životech občanů. Dovolím si jménem redakce časopisu i členů Komory vyjádřit účast a podporu lidem, které nedávné povodně zasáhly, a poděkovat všem, kteří se podíleli a namnoze dosud podílejí na pomoci v postižených oblastech.

S úctou k Vám a důvěrou v pokojnější průběh posledního kvartálu letošního roku.

Ing. Václav Jahodář
prezident KPKB ČR

OBSAH

TISKOVÁ ZPRÁVA KE KONFERENCI OCHRANA MĚKKÝCH CÍLŮ 2024

V Praze dne 8. července 2024

Vážení kolegové,
dne 13. června 2024 se uskutečnil již 8. ročník odborné konference „Ochrana měkkých cílů 2024 ", který pořádala Komora podniků komerční bezpečnosti České republiky, z.s., spolu se svými partnery AFCEA – českou pobočkou a ČVUT – Fakultou biomedicínského inženýrství.

Velmi si vážíme Vašeho zájmu a hlavně podpory, které se z Vaší strany této akci dostalo. Jsme si plně vědomi, že bez ní by se konference jen těžko dala uspořádat. Rovněž tak Vaše prezentace byly pro účastníky velmi atraktivní, užitečné a přínosné, o čemž svědčí nebývale vysoká účast široké odborné veřejnosti a následné reakce a pozitivní hodnocení konference.

Věříme, že i pro Vás byla možnost účasti na naší konferenci přínosná a přinese Vám v budoucnu naplnění Vašich očekávání.

Vhodně volenými aktuálními tématy a díky vysoké úrovni přednášek byla reflektována všechna současná palčivá úskalí, se kterými se při ochraně měkkých cílů musíme vypořádávat. Pochopitelně byly ukázány i směry a cesty, jak nejlépe tomuto fenoménu čelit.

Počet zaregistrovaných zájemců z řad odborné veřejnosti, a to jak ze státní, veřejné, tak i ze soukromé sféry, přesáhl 360 a množství účastníků, kteří se konference zúčastnili, bylo jen nepatrně nižší.

Velkým přínosem byli i hosté ze Slovenska, kteří se nechali naší konferencí inspirovat a hodlají podobnou pořádat na Slovensku.

Opět se nám potvrdilo, že pořádání této konference je nanejvýš důležité i z celospolečenského významu, neboť daná problematika zasahuje a ovlivňuje celou společnost bez rozdílu.
Vysoký zájem o tuto konferenci nás velmi těší a motivuje, takže v podstatě již teď se začínáme připravovat na příští ročník, který budeme pořádat **12. června 2025**.

Veškeré informace týkající se našich konferencí jsou k dispozici na webových stránkách:
https://www.ochranamekkychcilu.eu/

Jako příjemný bonus, nejen pro účastníky konference, ale i ty, kteří se zúčastnit nemohli, jsou od neděle 23. 6. 2024 postupně umísťovány záznamy jednotlivých přednášek na stránky:
https://youtube.com/channel/UCBUxiqwV92hRxp9bKSZkrhg

Několik konkrétních informací k 8. ročníku konference Ochrana měkkých cílů 2024:

- registrace byla kvůli kapacitě sálu otevřena pouze pro 320 posluchačů
- na konferenci přišlo 280 návštěvníků
- meziroční nárůst je 20 % osob
- v auditoriu naslouchali reprezentanti:
  - 12 ústředních orgánů státní správy
  - 23 krajů a významných měst
  - 10 nemocnic
  - 19 vzdělávacích institucí včetně univerzit
  - 13 kulturních a církevních institucí,
  - provozovatelé kritické infrastruktury, zástupci policie a dalších složek IZS

Shrnutí dotazníkového šetření mezi účastníky konference:

- 98 % návštěvníků deklarovalo zájem přijít příští rok znovu
- 97 % účastníků ocenilo možnost setkání s partnery; příště chtějí pro setkávání více prostoru (a my jim vyhovíme)
- 92 % návštěvníků bylo spokojeno s prostředím konferenčního centra
- 88 % návštěvníků pro jevilo zájem o sborník nebo jinou formu publikace z konference (v letošním roce máte možnost článku v časopisu Bezpečnost s profesionály)
- 86 % účastníků vysoce kladně hodnotí aktuálnost a potřebnost témat konference
- jako nejpotřebnější tematické okruhy hodnotí účastníci nová řešení, analýzy útoků, případové studie, vzdělávání/výcvik a „pohled útočníka"
- z nově zařazených témat vzbudil největší zájem deepfakes jako bezpečnostní hrozba

Tématy, která se do programu nevešla a podle dotazníkového šetření je o ně mezi návštěvníky velký zájem, jsou „Zahraniční inspirace", „AI a bezpečnost měkkého cíle" a „Bezpečnost veřejných prostranství a open air akcí". Tato témata zařadíme do programu menších akcí mezi výročními konferencemi a vy máte možnost se stát jejich partnery.

V úctě

Ing. Václav Jahodář
prezident
Komora podniků komerční bezpečnosti ČR, z.s.

Ing. Tomáš Muller
prezident ČP AFCEA

SLOŽKY IZS NA MÍSTĚ NÁSILNÉHO ÚTOKU NA MĚKKÝ CÍL

Jakým způsobem spolupracují jednotlivé složky IZS na místech mimořádné události typu „aktivní střelec"? Kdo je zodpovědný za celý průběh zákroku a jak nás může tato situace na místě i v nejbližším okolí ovlivnit?

To jsou otázky, na které jsem po tragické události z 21. prosince 2023 na Filozofické fakultě UK v Praze odpovídal několikrát a v rámci vyhodnocení našich činností na místě to bylo nutné vysvětlit nejen laické veřejnosti, ale i některým kolegům z řad policie, kteří neměli vůbec žádnou zkušenost s typem mimořádné události Aktivní střelec.

Přiznejme si, že i pro nás to bylo reálně poprvé, ale právě díky organizaci součinnostních cvičení složek IZS ve velkém formátu jsme si mohli co nejblíže skutečnosti zacvičit a vyzkoušet postupy podle schválených Typových činností složek IZS při společném zásahu, z nichž právě Soubor typové činnosti STČ 14/IZS se věnuje mimořádné události Amok – útok aktivního střelce. Nejkomplexnějšími cvičeními byla cvičení Anděl 2019 v OC Nový Smíchov a cvičení Národní muzeum 2021, v obou případech zaměřená na teroristický útok, držení rukojmí apod.

Dovolím si svůj výklad postupu složek IZS vysvětlit na již zmiňované tragické události z 21. prosince 2023.

14:59 h – operační důstojník policie (IOS) získává informaci, že je hlášeno napadení a střelba na náměstí Jana Palacha. Vysílá na místo okamžitě nejbližší hlídky policie, bez ohledu na to, zda jde o hlídky prvosledové, vybavené balistickou ochranou a dlouhými zbraněmi, nebo ty ostatní.

15:02 h – máme potvrzenou informaci, že ke střelbě opravdu došlo. Studenti utíkají pryč z budovy, policisté do ní vstupují a jejich úkolem je eliminace aktivního střelce. Zahajujeme postup dle STČ 14/IZS Amok – útok aktivního střelce.

15:03 h – IOS vysílá další síly a prostředky na místo události a žádá o součinnost další složky IZS (ZZS a HZS) prostřednictvím KOPIS (krajské operační a informační středisko). Zapojují se další pražská operační střediska a událost automaticky nabírají i další krajská operační střediska PČR, protože operátoři na 158 v Praze jsou již obsazeni.

První hlídky, tři kriminalisté v civilu a dvojčlenná uniformovaná hlídka, vstupují do budovy a díky získaným informacím od utíkajících studentů míří do vrchních pater, kde útočník střílí do lidí. Následující hlídky se vydávají také nahoru. Úkol policie je jasný, eliminace střelce jako nejvyšší priorita, nelze se zastavovat u zraněných a evakuovaných. Dochází k tzv. „rychlé evakuaci", kdy utíkající studenty směřují policisté na místě pryč z místa dolů k východu, kde už očekávají další policisty, kteří se o evakuaci postarají. V případě zraněných je možné jim předat základní zdravotnický materiál, ale je nutné jít dál a zastavit pachatele.

Venku mezitím přijíždějí další policisté, a to včetně velitele policie, který začíná organizovat činnost policie a dalších složek IZS na místě. Zastavuje rychlou evakuaci, označí nebezpečný prostor a určuje místo pro seřadiště složek IZS mimo nebezpečný prostor, v tomto případě za Rudolfinem. Na místě přebírá velení a velí všem složkám IZS. Vytváří taktický štáb na hranici nebezpečného prostoru, jehož součástí je i velitel ZZS a HZS. V rámci vymezeného prostoru může omezovat fyzické i právnické osoby, nařídit evakuaci, žádat o spolupráci apod.

15:20 h – máme informaci od hlídky, že střelec spáchal sebevraždu zastřelením. Je nutné to však ještě bezpečně prověřit.

Velitel policie určí hranice vnitřní a vnější zóny, kde do vnitřní zóny může vstupovat pouze policie. On jako velitel policie je zodpovědný za to, aby se do nebezpečného prostoru nedostal nikdo nepovolaný. Později přijíždí na místo policejní důstojník, který od něj přebírá velení, krajský ředitel policie brig. gen. Petr Matějček. Taktický štáb ponechává na veliteli policie a sám se zapojuje do velení ve štábu strategickém, který je na místě do cca 45 minut od začátku události. Strategický štáb je zodpovědný za řízení celého opatření, za koordinaci všech složek IZS, za kontakt s médii a dalšími subjekty a zároveň přizývá do štábu další zástupce organizací nutných pro řešení mimořádné situace, např. zástupce Filozofické fakulty, magistrátu, dopravního podniku, městské policie a další. Ve strategickém štábu je přítomen i ministr vnitra.

Úkoly strategického i taktického štábu se prolínají. Je potřeba zorganizovat místo pro zraněné, jejich předávání ZZS a zajistit převoz zraněných do nemocnic, které musí vyhlásit traumatologický plán. Je nutné vytvořit místo pro evakuované – vybrána je budova Rudolfina. Následně je potřeba všechny do tohoto místa bezpečně převést, zkontrolovat jejich stav, zkontrolovat, zda nejsou ozbrojeni, a zjistit jejich totožnost. Je nutné zřídit intervenční linku, informovat rodinné příslušníky, veřejnost, odpovídat na dotazy ambasád a další.

Zásadním krokem pro další postup po eliminaci pachatele je prohlášení pro-

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI
ČESKÉ REPUBLIKY

storu za bezpečný. V tomto konkrétním případě však nastávají komplikace. IOS všem hlídkám oznamuje, že na místě může být potenciální další pachatel, komplic. Je nutné prohledat budovu, zda není někde schovaný, vstupovat i násilným způsobem do jednotlivých místností a přítomnost dalšího útočníka vyloučit. Po provedené bezpečnostní kontrole je oznámeno další nebezpečí, možnost umístění nástražného výbušného systému. Na místo jsou povoláni pyrotechnici a budova je prohlížena znovu.

18:00 h – prostor je prohlášen za bezpečný. Budova je předána orgánům činným v trestním řízení k zajištění stop, zjištění totožnosti obětí atd. Vstup dalších složek IZS už není nutný.

Na strategickém štábu se začíná řešit další komunikace s médii, jakým způsobem policie převezme věci po evakuovaných, zraněných a obětech, jak se budou řešit škody, které policie způsobila svým postupem, kdo po zajištění všech stop a převozu obětí provede úklid budovy, aby se fotografie z místa nedostaly do médií… Upřesňují se informace o zraněných, kde jsou umístěni a v jakém stavu. To vše řeší zejména velitel opatření a zástupce univerzity s podporou zaměstnance Magistrátu hl. m. Prahy a velitelem ZZS na místě.

22:00 h – orgány činné v trestním řízení začínají postupně potvrzovat totožnosti zemřelých a jejich těla jsou převážena pohřební službou k dalším úkonům. Poslední oběť je předána v 9:00 h dalšího dne a budova je následně předána zástupci Univerzity Karlovy.

Útok střelce trval 21 minut. Prostor byl za bezpečný prohlášen tři hodiny po zahájení útoku. Celé opatření trvalo cca 18 hodin.

Shrnutí

V případě útoku aktivního střelce postupují všechny složky IZS podle **STČ 14/IZS** „Amok – útok aktivního střelce“. Velitelem celého zákroku je zodpovědný důstojník policie na místě a ostatní složky IZS jsou mu podřízeny. Všechna operační střediska složek IZS úzce spolupracují. Velitel policie prohlásí za nebezpečný prostor konkrétní objekt a okolí. Do tohoto prostoru mohou vstupovat pouze policisté. Prioritním úkolem policistů je eliminace pachatele a do té doby se nemohou věnovat zraněným ani ostatním osobám, kterým pouze určí jejich další pohyb ven nebo do místnosti, aby se tam ukryli. Po eliminaci pachatele a vyloučení dalších hrozeb prohlásí velitel policie prostor za bezpečný. Probíhá řádná evakuace a kontrola osob, a pokud jsou na místě ještě zranění, zapojuje se i ZZS a HZS k ošetřování a transportu. Na hranici vnější zóny je vytvořen filtr pro zraněné, kde ZZS zraněné třídí a podle priorit ošetřuje a převáží do nemocnic, kde je vyhlášen traumaplán.

V případě aktivního útočníka může následně dojít k souběhu několika dalších typových plánů IZS. V tomto případě šlo o **STČ 09/IZS** „Zásah složek IZS u mimořádné události s velkým počtem zraněných osob“, **STČ 03/IZS** „Hrozba použití NVS, podezřelého předmětu, výbušnin a výbušných předmětů“ a **STČ 12/IZS** „Typová činnost složek IZS při poskytování psychosociální pomoci“. Přesto však na místě mimořádné události postupují všichni primárně dle **STČ 14/IZS** Amok a v rámci jejích mantinelů pak podle ostatních STČ.

Pokud je v nebezpečném prostoru nutné provést jakoukoli činnost, kterou standardně provádějí ZZS nebo HZS, provádí ji samotná policie, která si ovšem může pro tento úkol vyžádat jejich součinnost, např. tak, že se nechá vybavit adekvátními ochrannými pomůckami nebo dalším materiálem. Pouze v nejnutnějších případech je možné do nebezpečného prostoru vpustit jiné složky IZS, a i to jen za předpokladu jejich maximální ochrany. Může se jednat o přistavení plošiny, osvětlení místa, přistavení cisterny apod.

Na začátku článku jsem se zmínil, že do doby útoku na Filozofické fakultě UK jsme obdobnou situaci pouze nacvičovali a málokdo z přítomných si připouštěl, že ho může opravdu potkat. Troufám si však říci, že zejména proto jsme vlastní zákrok i následné kroky proti aktivnímu střelci zvládli tak dobře, že i ohlasy kolegů a profesionálů ze zahraničí byly jen a jen pozitivní. Dokonce se vyjádřili v tom smyslu, že lepší reakci a koordinaci na místě takto ještě nikdy neviděli, přestože mají s podobnými útoky své vlastní zkušenosti.

Já jen doufám, že nadále budeme pokračovat už jen ve cvičeních a nikdo z nás už nebude muset podobnou událost zažít.

Zdeněk Orel
major v. v.
policejní vyjednavač

PREVENCE ZTRÁT A KRÁDEŽÍ V LOGISTICKÝCH CENTRECH

Společnost Rohde & Schwarz nabízí nejmodernější bezpečnostní technologie pro prevenci ztrát

Krádeže drobných předmětů s vysokou hodnotou jsou stále větším problémem v celé řadě provozoven, od skladů a distribučních center po obchody a supermarkety. Řešením mohou být moderní technologie, které byly úspěšně implementovány na letištích a nyní jsou dostupné i pro komerční účely.

Problém v hodnotě 6 miliard korun

Odhaduje se, že ročně přijdou podniky kvůli krádežím zaměstnanců o zhruba 6 miliard korun, jedná se především o krádeže hotových výrobků nebo materiálu. Mezi nejčastěji zcizované předměty patří kosmetika a značkové zboží, elektronika, kancelářský materiál zakoupený pro využití ve firmě nebo cenná data vynesená na paměťových kartách, USB či jiných nosičích.

Řešení těchto krádeží je pro zaměstnavatele velmi choulostivé. Ale je třeba se mu věnovat, jak z pohledu financí (tedy úspora nákladů, ušlý zisk) tak s ohledem na poctivé pracovníky. Firmy musí nastavovat opatření bránící ztrátám velmi obezřetně, vše musí probíhat v souladu se zákonem a s ohledem na důstojnost zaměstnanců. V tomto ohledu je nejdůležitější komunikace se zaměstnanci a dostatečné vysvětlení zavedených opatření. Prevence je vždy lepší než řešení následků.

Pokud se podaří zabránit ztrátám způsobeným krádežemi zboží či materiálu, povede to jak ke zlepšení ekonomické bilance, tak ke zvýšení morálky zaměstnanců. Celotělové skenery slouží i jako prevence krádeží, zavedená účinná opatření mohou odradit potenciální zloděje. Dnes nejčastěji využívané metalické rámy odhalí pouhý zlomek vynášených předmětů, tato technologie je zaměřena na detekci primárně kovových předmětů, což je již v dnešní době nedostačující.

CELKEM SE ODHADUJE, ŽE PODNIKY PŘIJDOU KVŮLI KRÁDEŽÍM ZAMĚSTNANCŮ O ZHRUBA 6 MILIARD KORUN ROČNĚ

Techniky detekce

Metalické rámy instalované v halách logistických center u vstupů a východů, jsou dobře viditelné a mohou tak působit jako prevence. Jejich účinnost je však omezená, metalické rámy nejsou schopny detekovat nekovové předměty. Detektory kovů jsou většinou průchozí rámy doplněné ručním detektorem pro manuální kontrolu. Pokud je metalický rám doplněn ručním detektorem, je nutné mít k dispozici další zaměstnance a vyškolit je k provádění bezpečnostních kontrol.

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČESKÉ REPUBLIKY

Další alternativou jsou dohledové kamery (CCTV), toto řešení vyžaduje nepřetržité sledování obrazovek a využití CCTV se řídí striktními právními předpisy, vyžaduje informování zaměstnanců atp. Skryté natáčení zaměstnanců není povoleno a důvody natáčení musí být jasně zdůvodněny, protože použití záznamů z kamerového systému k jiným, než přesně určeným účelům je nezákonné. Je třeba také zvážit dopady na poctivé zaměstnance.

Firma může samozřejmě zaměstnávat bezpečnostní pracovníky, kteří kontrolují zavazadla a provádějí osobní prohlídky. Obecně jsou ale osobní prohlídky spíše nežádoucí, nehledě na to, že pravděpodobnost odhalení malých nebo dobře ukrytých předmětů je velmi malá. Další možností bezpečnostních kontrol jsou rentgeny. Ty se hojně používají ke skenování zavazadel na místech, jako jsou letiště, pro běžnou kontrolu osob jsou ale nevhodné kvůli nadměrnému rentgenovému záření.
Kontrola osob pomocí celotělových skenerů na bázi milimetrových vln se ukázala jako účinná na místech, jako jsou bezpečnostní kontroly na letištích. Elektromagnetické vlny s nízkou energií jsou schopny detekovat všechny předměty včetně nekovových materiálů ukrytých pod oblečením.
Skenování je neinvazivní a chrání soukromí – nejsou shromažďovány ani nejsou zobrazovány žádné snímky těla. Skenování metodou „Pose-and-go" je rychlé a snadné, umožňuje velkou propustnost, vyzařované vlny jsou neionizující, a proto neškodné pro lidský organismus.
Skenery využívající milimetrové vlny lze použít k detekci nejrůznějších drobných předmětů, které jsou obtížně dohledatelné. Firmy, které budou nyní investovat do zařízení využívajících milimetrové vlny, mohou očekávat rychlejší návratnost, zejména při ochraně velmi hodnotných předmětů. Tyto technologie jsou již na dostatečně vysoké úrovni a na trhu je k dispozici mnoho různých systémů. Příkladem mohou být skenery R & S QPS 201 (Quick Personnel Security) a nedávno vyvinuté skenery R & S QPS Walk2000 z produkce společnosti Rohde & Schwarz.

ŘEŠENÍM MOHOU BÝT MODERNÍ TECHNOLOGIE, KTERÉ BYLY ÚSPĚŠNĚ IMPLEMENTOVÁNY NA LETIŠTÍCH A NYNÍ JSOU DOSTUPNÉ I PRO KOMERČNÍ ÚČELY

Tyto systémy se skládají ze statického pole vysílačů zabudovaného do velkého panelu, jež je osazen soustavou vysílačů a přijímačů, které jsou rozmístěny po celé ploše. Panel může být přizpůsoben potřebám zákazníka, libovolně barevný, případně s digitálním potiskem, k oskenování jedné osoby stačí pouhých několik milisekund. Dostatečné množství vysílačů a přijímačů umožňuje rychlé skenování, panely neobsahují žádné pohyblivé části.

Během skenování vyzařují vysílače milimetrové vlny a přijímače shromažďují odražené signály. Přijaté signály pak procházejí rozsáhlými úpravami a analýzou s využitím velmi výkonných signálových procesorů (DSP) se zabudovanou špičkovou umělou inteligencí (AI).

Ochrana soukromí

Systémy, které jsou zde popisovány, umožňují velmi rychlé, účinné a automatizované skenování. Jejich další zásadní výhodou je, že výsledkem snímání s využitím milimetrových vln není záznam ani tvorba jakýchkoli obrazů osob. Všechna data existují pouze v digitální podobě a jsou zlikvidována ihned po zobrazení výsledku skenování.

Pokud systém zjistí v zachycených vlnách anomální vzor, signálový procesor určí jeho polohu a označí ji na avataru. Bezpečnostní pracovníci ji pak mohou využít pro cílenou manuální kontrolu.

Zařízení pracující s milimetrovými vlnami využívají automatizaci procesu kontroly a odstraňují nevýhody typicky spojené s bezpečnostním skenováním, které je prováděno lidmi. Zařízení je nezaujaté, odolné vůči zastrašování a dokáže udržet pracovní tempo po neomezenou dobu bez únavy nebo ztráty pozornosti.

Popisované typy bezpečnostních skenerů se nyní běžně používají pro bezpečnostní kontroly na letištích a nabízejí vysokou propustnost, vynikající přesnost detekce s minimem falešných poplachů a také neuvěřitelně snadné používání. Systémy jsou u bezpečnostních pracovníků velmi oblíbené, protože jim pomáhají pracovat nestranně a zároveň zachovat během směn konzistentní ostražitost.

Jsou také používány u vstupů do veřejných budov a zábavních podniků, na výstavách a k ochraně návštěvníků nejrůznějších akcí.

Snadná instalace a používání

Pokročilé bezpečnostní skenery s milimetrovými vlnami, mezi něž patří řada R & S QPS, nabízejí bezpečné a účinné řešení pro prevenci ztrát výrobků i zásob. Lze je instalovat v továrnách, skladech nebo kancelářích bez potřeby dalších zvláštních služeb. Jsou nekomplikované a po minimálním technickém zaškolení i snadno použitelné, což bezpečnostním pracovníkům umožňuje rychle se zdokonalovat a dosahovat vynikajících výsledků.

Firmy, včetně prodejců, distributorů a velkoobchodů, tedy mohou s využitím těchto systémů výrazně omezit nákladné ztráty.

„Pokročilá bezpečnostní technologie"

Gary Mackay, generální ředitel společnosti Rohde & Schwarz UK, k tomu dodává: „Krádeže zaměstnanců jsou závažným problémem, který ovlivňuje podniky v různých odvětvích. Ve společnosti Rohde & Schwarz si uvědomujeme důležitost ochrany majetku našich zákazníků, a proto jsme vyvinuli takovou bezpečnostní technologii, která pomáhá tento problém řešit. Naše skenery nabízejí cenově dostupné, účinné a neinvazivní řešení pro odhalování odcizených věcí předtím, než opustí areál podniku."

Kontakt:
ROHDE & SCHWARZ - Praha, s.r.o.
Evropská 2590/33c, 160 00 Praha 6
www.rohde-schwarz.com

MĚKKÉ CÍLE POD OCHRANOU ANEB KOMPARACE BEZPEČNOSTNÍCH PŘÍSTUPŮ ČR A VELKÉ BRITÁNIE

Přestože se mohou jednotlivé přístupy států v rámci ochrany měkkých cílů lišit, jedno mají všechny společné, a to postavit se jedné z nejtěžších bezpečnostních výzev současnosti a co nejvíce elimininovat možné ztráty na životech nevinných obětí, které jsou cílem útočníků.

Otázka ochrany měkkých cílů, bezpečnosti veřejných budov a prostranství, přípravy občanů i včasné reakce jednotlivých složek IZS rezonuje společností stále, avšak o to hlasitěji, pokud dojde kdekoli ve světě k teroristickému či jinému násilnému činu.

Každý útok vyvolá zvýšenou reakci a poptávku po revizi a aktualizaci všech dosud vydaných dokumentů i předešlých opatření s nevyřčenou otázkou, zda se nedalo udělat více. Předkládaný příspěvek se zabývá komparací a hodnocením současného stavu ochrany měkkých cílů a míst s velkou koncentrací osob v České republice a Velké Británii. Článek je zaměřen na prevenci útoků, připravenost personálu i složek IZS a zodolnění měkkých cílů v podobě prezentovaného přehledu preventivních bezpečnostních projektů přímo z praxe.

Příspěvek se zaměřuje na analýzu nových postupů, výcviku i osvěty v oblasti crowded places s důrazem na otázky připravenosti jednotlivých subjektů čelit možným útokům. Cílem je komparace osvědčených postupů s ukázkou příkladů dobré praxe i možné inspirace a ponaučení ze zahraničních zkušeností.

Na počátku nebylo slovo, ale strategie aneb geneze a vývoj ochrany měkkých cílů v České republice

Problematika zabezpečení *„crowded places"* (doslova „přeplněných míst", jinak řečeno měkkých cílů) a jejich ochrany, zejména z pohledu terorismu a aktivních útočníků, je velmi aktuální, nadčasová a ukrývá v sobě řadu bezpečnostních konsekvencí. Význam dané problematiky pro Českou republiku potvrzuje i zařazení do jednoho ze zásadních stavebních pilířů vládní *„Strategie boje pro terorismu 2010–2012"* schválené v roce 2010 či navazující *„Strategie České republiky pro boj proti terorismu"* z roku 2013.

Jedna z neproblematičtějších bezpečnostních výzev současnosti zaměstnává ve větší míře již delší dobu vládní i bezpečnostní složky napříč celým světem. Důležitost této výzvy dokreslují minulé i současné útoky či včasná zadržení útočníků před jejich dokonáním. Problematikou měkkých cílů se na půdě ministerstva vnitra zaobíral též samostatný dokument *„Současný stav ochrany potenciálních cílů včetně prevence teroristických útoků na vybraných místech, jejich silné a slabé stránky a návrhy zlepšení jejich ochrany"*.

Genezi problematiky ochrany měkkých cílů v ČR pokrývá v praktické rovině mimo výše uvedené strategické dokumenty taktéž činnost pracovní skupiny Národní centrály proti organizovanému zločinu či zřízení telefonní linky určené k podpoře provozovatelů a vlastníků měkkých cílů. Cílem veškerých aktivit byl však prioritní úkol v podobě vypracování a přípravy návrhu Koncepce ochrany měkkých cílů v ČR, která byla předložena v lednu 2017. Vývoj bezpečnostní situace v Evropě zejména v letech 2014–2016 si však vyžádal komplexní řešení problematiky ochrany měkkých cílů, které vedlo k celé řadě dalších aktivit ze strany Ministerstva vnitra ČR a nově zřízeného Centra proti terorismu a hybridním hrozbám (CTHH) až po sérii klíčových koncepčních a metodických dokumentů. Zanedbatelná nebyla v této době ani aktivita akademické obce, zejména Policejní akademie ČR či navazujícího bezpečnostního výzkumu.

33 opatření jako reakce na tragický útok na FF UK

Policie + hasiči

- výzbroj, výcvik, vzdělávání, zlepšení analytických schopností
- digitální dokumentace, systém cellbroadcast (odesílání varovných SMS v krizové situaci), tísňová komunikace

Ministerstvo vnitra + ministerstvo školství

- zbraňová legislativa, registr zbraní, psychologická vyšetření,
- školení, komunikační kampaň v online prostoru
- vytvoření a zvýšení standardů bezpečnosti pro VŠ
- aktualizace bezpečnostních metodik v oblasti školství

Obdobná situace panovala u dalšího z klíčových hráčů na poli bezpečnosti, a to Policie ČR, která se v reakci na aktuální hrozby i útoky aktivně připravovala již od roku 2011. V souvislosti s tragickou událostí na Filozofické fakultě Univerzity Karlovy musela však opět řešit otázky spojené nejen s bezpečností univerzit, ale též dalších klíčových míst s velkou koncentrací osob a do popředí se dostaly palčivé otázky, jak je to s bezpečností na českých školách, jaké jsou možnosti podobným činům předejít a zda můžeme takovýmto činům vůbec zabránit.

Nejprve představila policie své *„Desatero k ochraně měkkého cíle"*, na které posléze navázal ministr vnitra představením 33 opatření, která lze přijmout pro zvýšení efektivity celého již fungujícího systému. Jedná se o prvotní soubor konkrétních opatření, jež lze přijmout k posílení bezpečnosti ze strany ministerstva vnitra, policie, hasičů i ministerstev školství a zdravotnictví.

Inspirace, ponaučení i ukázka dobré praxe na příkladu Velké Británie

Jak již bylo uvedeno výše, představuje problematika snižování možné zranitelnosti měkkých cílů neboli crowded places oblast bližšího zájmu řady států, bezpečnostních organizací i mezinárodních institucí. Pokud se však podíváme na koncept crowded places, respektive měkkých cílů, poněkud blíže a detailněji, zjistíme, že za jednoho z významných leaderů v této oblasti lze považovat Velkou Británii, která vyvinula ve vztahu ke snížení zranitelnosti v důsledku teroristických útoků na přeplněná a hojně navštěvovaná místa strategický rámec několika zásadních dokumentů.

V prvé řadě je tak potřeba jmenovat ucelenou řadu dokumentů a směrnic britského ministerstva vnitra týkajících se projektování protiteroristických opatření v zastavěném prostředí či Národního protiteroristického bezpečnostního úřadu (NaCTSO), který přešel od roku 2022 díky nové samostatné webové platformě PROTECT UK do on--line prostředí.

Opomenout nelze ani v současné době velmi často citovaný Martyn's Law (Martynův zákon) pojmenovaný po Martynu Hettovi, jedné z obětí bombového teroristického útoku v roce 2017, k němuž došlo v Manchesteru po koncertu zpěvačky Ariany Grande. Zákon upravuje ochranu měkkých cílů s důrazem na jednoduché kroky a opatření, jejichž nedodržení nicméně bude sankcionováno.

Vynechat nelze stejně jako v případě ČR strategii boje proti terorismu CONTEST, zaměřující se na nejvýznamnější bezpečnostní hrozby týkající se všech občanů, a to včetně eliminace hrozeb a dopadů mezinárodního terorismu, stojící na čtyřech základních principech.

S výše uvedenými dokumenty je velmi úzce provázána činnost Národní technické agentury pro bezpečnost (NPSA) s řadou bezpečnostních preventivních kampaní proklamujících fyzickou a personální bezpečnost, s cílem snižování zranitelnosti.

Za zmínku stojí jistě i dokumenty Královského institutu architektů (RIBA), věnující se projektování protiteroristických opatření v podobě společné iniciativy zaměřené na bezpečnostní aktivity institutu a dalších bezpečnostních aktérů ve všech fázích stavby či životního cyklu budov.

Významné a inspirující jsou též samotné bezpečnostní projekty a iniciativy, jako například:
Security – Minded Communications (SMC) – síla komunikace
• komunikace zaměřená na bezpečnost

Security on your Side (SOYS)
– vidět neviděné
• opatření zaměřená na zmírnění útoků pomocí vozidel (HVM)

Recognising Terrorist Threats
– rozpoznání teroristických hrozeb
• přehled modu operandi (způsobu útoků útočníků)

SCaN – See, Check and Notify
• sada školicích modulů (vidět, zkontrolovat a oznámit)

Secured by Design (SBD)
– systém bezpečnostních akreditací a certifikací
• policejní iniciativa ke zlepšení zabezpečení budov a jejich okolí

Project Servator
– včasná identifikace trestných činů
• včasné odhalení teroristických útoků ve fázi jejich plánování

Project Agrus
– protiteroristická iniciativa v oblasti výcviku
• tříhodinová multimediální simulace na téma terorismu

Secure Stations Scheme
– akreditační systém zabezpečení stanic
• pro provozovatele železniční sítě hlídané britskou dopravní policií

Railway Guardian
– nejbezpečněji společně (Safest Together)
• mobilní aplikace britské dopravní policie pro zvýšení bezpečnosti

Bus & Coach Security
– rizika v autobusové a autokarové dopravě
• bezpečnost stanic, terminálů, dep

Zásadní roli sehrává činnost protiteroristické policie (COUNTER TERRORISM POLICING) spolupracující s policejními složkami s prioritním cílem chránit veřejnost a národní bezpečnost s důrazem na předcházení, odrazování a vyšetřování teroristické činnosti, v duchu motta „je důležité být ostražitý, ale ne vyděšený", či rozsáhlou kampaň ACTION COUNTERS TERRORISM (ACT).

Závěrem nelze opomenout komplexní příručky a pokyny (celkem se jedná o 10 manuálů) poskytující informace a opatření, která lze přijmout k minimalizaci dopadů útoků v reakci na záškodnické (diverzní) teroristické útoky – MARAUDING TERRORIST ATTACKS (MTA). S daným souvisí též MTAS – standardy poskytující specifika pro určení doby odolnosti jednotlivých fyzických bariér, jako jsou například dveře, turnikety, rolety, zámky, stěny, okna a řada dalších objektů.

V tomto kontextu je též potřeba připomenout, že jednotlivé bezpečnostní kampaně jsou všudypřítomné, a to i se zapojením známých osobností, aby byly pro občany co nejvíce srozumitelné, efektivní a přínosné.

Na závěr chci vyjádřit přesvědčení, že uplatňování konceptu ochrany měkkých cílů a míst s velkou koncentrací osob se postupem času stane zcela běžnou záležitostí realizovaných preventivních aktivit všech zainteresovaných subjektů, a nikoli jen dočasným bezpečnostním opatřením v případě jakéhokoliv útoku.

Mgr. et Mgr. Pavel Krčílek, DiS.
Úřad městské části Praha 11
Odbor kancelář starosty
vedoucí Oddělení krizového řízení

ACTION COUNTERS TERRORISM (ACT)

Rozsáhlá protiteroristická kampaň (včasná informovanost, bdělost, školení)

- **ACT Early**
  - prevence radikalizace a předcházení násilnému extrémismu
- **ACT Awareness**
  - školení pro zvyšování povědomí o boji proti terorismu
- **ACT Security e-Learning**
  - e-learningový kurz pro oblast vzdělávání (školní prostředí)
- **ACT in a box (IED, MTA)**
  - simulace útoku v rámci modelových interaktivních scénářů
- **ACT Faith Security**
  - bezpečnostní opatření náboženských komunit a bohoslužeb

BEZPEČNOSTNÍ DOPORUČENÍ A KAMPANĚ

POŽÁRNÍ vs. BEZPEČNOSTNÍ EVAKUACE

POSOUZENÍ VÝZNAMNÝCH OBČANSKÝCH STAVEB A JEJICH PŘILEHLÉHO OKOLÍ V KONTEXTU BEZPEČNOSTI PŘI MIMOŘÁDNÝCH UDÁLOSTECH

„Jaká je vzájemná symbióza přístupů fyzické bezpečnosti a požární bezpečnosti? Je vůbec vzájemná symbióza těchto dvou oblastí možná a jak k tomu všemu přispívá vysoká koncentrace osob?"

Toto jsou otázky, kterým je vhodné věnovat pozornost v bezpečnostním diskurzu. Společným zájem inkriminované segmentace druhů bezpečnosti je ochrana majetku, ale co možná nejvíce je kruciální zdraví a život osob, které se nacházejí v zájmovém objektu, v jehož provozním cyklu je požární bezpečnost de iure, na rozdíl od opatření spadající do fyzické bezpečnosti. Přičemž tyto druhy bezpečnosti sledují každá svůj cíl, využívají své specifické metody, nástroje, síly a prostředky k dosažení žádoucího stavu, a to je v konečném důsledku v obou případech ochrana integrity a snížení zranitelnosti na minimum.

Každá osoba se zájmem o svůj pocit bezpečí v kontextu posledních událostí, které se staly na území České republiky, ale i ve světě, si uvědomuje flagrantní relevanci problematiky ochrany míst s vysokou koncentrací osob. Nikdy nebyl zájem o tuto problematiku více aktuální, nežli tomu je nyní.

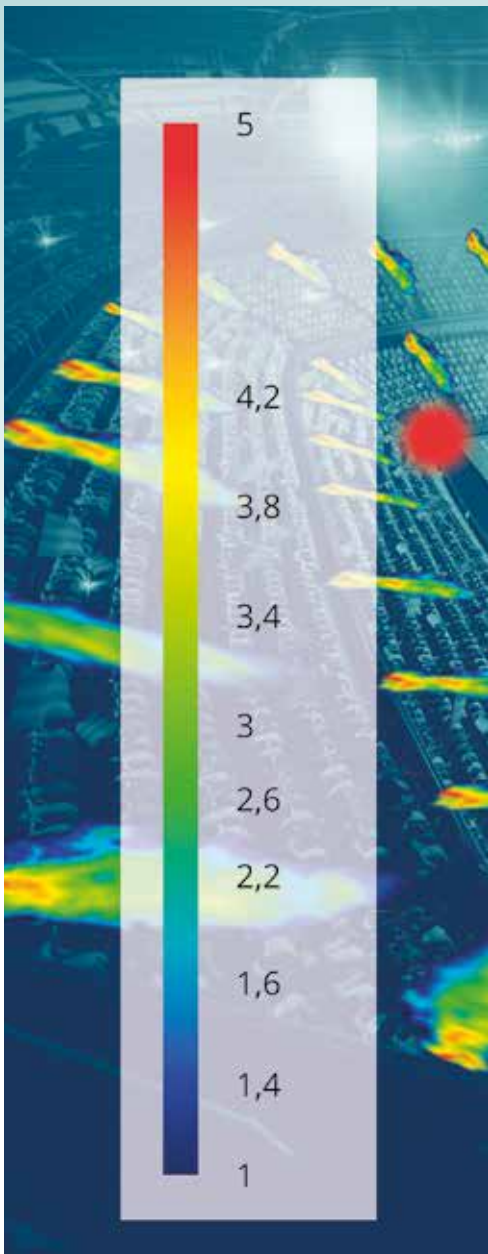
Místa s vysokou koncentrací osob (spíše známá jako měkké cíle) jsou nedílnou součástí pojmového aparátu bezpečnostních expertů nejen bezpečnostní politiky. Je také lucidní, že mezi místa s charakterem měkkého cíle spadají podle aktuálních dokumentů nelegislativní povahy místa spojená s kulturním dědictvím, dopravní infrastruktura (hlavní nádraží), obchodní centra a samozřejmě školní a univerzitní kampusy apod. Je doslova nutné také zaznamenat skutečnost, že lze dále tato místa segmentovat na místa s dočasným a místa s trvalým shromážděním osob.

Ovšem s pojmem „měkký cíl" nepracují **výhradně experti z řad ozbrojených sborů, komerční bezpečnosti a zástupci bezpečnostního managementu ve vztahu ke korporátním společnostem.**

S tímto pojmem pracují i zástupci Hasičského záchranného sboru České republiky (dále jen HZS ČR). Hasiči vnímají tento pojem z jiného pohledu, kterým je a ochrana před různorodou škálou hrozeb, nikoliv apriori zaměření na násilné a teroristické útoky, jak k tomu přistupuje např. policie. **Záchranný sbor nahlíží na tuto výzvu pod optikou ochrany obyvatelstva.** Označení měkkých cílů z pohledu HZS ČR zní, ***„společensky významné objekty"*** a za tyto prostory se považují *„místa (stavby, prostory nebo plochy) s vysokou koncentrací osob a nízkou úrovní zabezpečení ochrany života a zdraví obyvatelstva, kde je vazba na zajištění plnění opatření ochrany obyvatelstva v těchto objektech."* [1] V citované definici je deklarována právě ochrana obyvatelstva pro jejíž účel se stavby či objekty mohou využít. Obyvatelstvo můžeme označit jako sociální entitu. Různé druhy hrozeb znamenají pro zmíněnou entitu jisté nebezpečí, které lze synonymně označit jako druhy mimořádných událostí (dále jen MU) naturogenního (způsobené živou či neživou přírodou) či antropogenního charakteru (způsobené činností člověka). Mimo jiné terorismus a násilné útoky vůči společensky významným objektům spadají do antropogenních MU se subkategorizací: *sociogenní interní a sociogenní externí MU.*

Výše uvedená textace je pouhým marginálním exkurzem, který je však v konečném důsledku relevantní ve vztahu k ambici tohoto článku.

Kontext ve vztahu k požární bezpečnosti



KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČESKÉ REPUBLIKY

Zájem na ochraně míst s vysokou koncentrací osob má mnoho subjektů a opatření a povinnosti spojené s požární bezpečností po věcné a formální stránce upravuje lex specialis (tj. zákon č. 133/2000 Sb., o požární ochraně, ve znění pozdějších předpisů), dále jej konkretizují prováděcími předpisy (např. velice klíčová vyhláška č. 246/2001 Sb., o požární prevenci, či mimo jiné vyhláška č. 23/2008 Sb., o technických podmínkách požární ochrany staveb).

Zájmové stavby musí v kontextu výše uvedených právních předpisů splňovat závazné podmínky a v této souvislosti vytvářet management požární ochrany v souladu s příslušnou právní materií. Pro účel tohoto textu hraje stěžení roli výše uvedená vyhláška č. 23/2008 Sb., o technických podmínkách požární ochrany staveb. Tento prováděcí předpis v Příloze č. 1 uvádí taxativní výčet technických norem nejen z kodexu norem požární bezpečnosti staveb, **tj. normy z řady 73 08.** Příslušná vyhláška činí některé normy, jež **stanovují technické podmínky požární bezpečnosti závaznými.** Mezi ně konkrétně patří základní projektové normy v oblasti požární bezpečnosti, tj. **ČSN 73 0802 Požární bezpečnost staveb – Nevýrobní objekty, či ČSN 73 0804 Požární bezpečnost staveb – Výrobní objekty.**

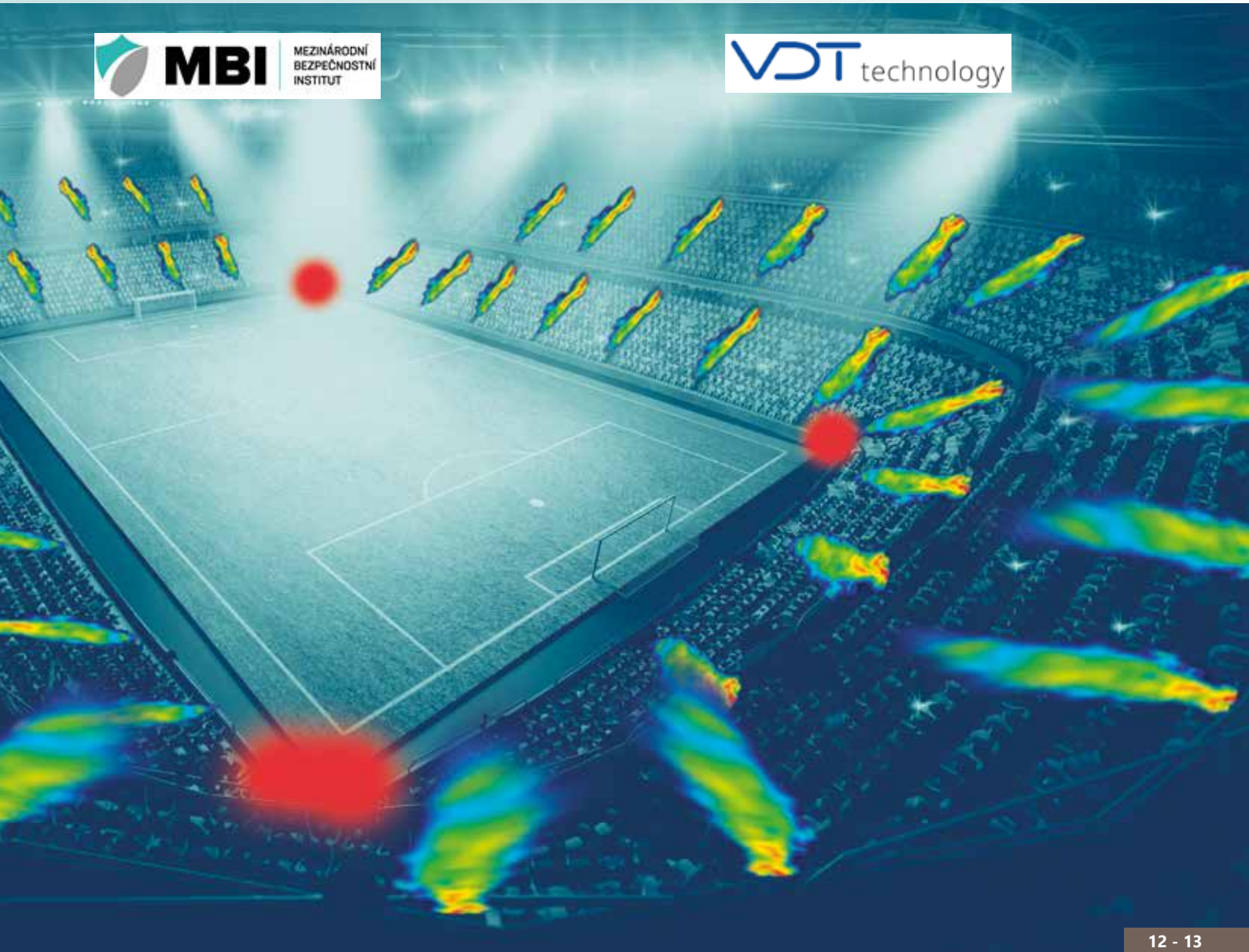
Kontext ve vztahu k fyzické bezpečnosti

Aspekty spojené s opatřeními v zájmu fyzické bezpečnosti jsou implementované až ve fázi předprovozní/funkční příslušného zájmového objektu. Projektová dokumentace je v tomto kontextu téměř nedotčená. Toto prizma však není univerzální, neboť jsou případy, kdy jsou požadavky na ochranu a fyzickou bezpečnost dány charakterem a provozem objektu či jeho konkrétní části.[2] Povinnost ve vztahu k fyzické bezpečnosti není vymahatelná, v tom je zásadní rozdíl oproti legislativnímu vnímání požární ochrany/bezpečnosti.
Nezbývá nic jiného než využívat maximálně metodické materiály a doporučení, které mnohdy mohou být v podobě bezpečnostního standardu či technické specifikace, např. pro školská zařízení **ČSN 73 4400 Prevence kriminality – řízení bezpečnosti při plánování, realizaci a užívání škol a školských zařízení,** nebo **ČSN/TS 16850 Ochrana společnosti – pokyny pro řízení bezpečnosti ve zdravotnických zařízeních –** pomůže v nemocnicích.

Vzhledem k tomu, že posouzení významných občanských staveb a jejich přilehlého okolí v kontextu bezpečnosti při mimořádných událostech vyžaduje širokou škálu pohledů a nástrojů, vycházíme obzvláště:

- **z důkladné analýzy hrozeb a z nich linoucích se rizik;**
- **identifikace a agregace pravděpodobných mimořádných událostí, které mohou v zájmovém objektu či v jeho okolí nastat (lze označit také jako vyhodnocení ohroženosti měkkého cíle);**
- **vyhodnocení možného dopadu a kvantifikace;**
- **návrh vhodných opatření.**

Mezinárodní bezpečnostní institut, z. ú., vnímá budoucnost v zapojení



a využívání detailních modelů a simulací pohybu osob pro bezpečnostní otázky. Zároveň si je vědom, že je nevyhnutelné zaujímat nekonvenční přístup k bezpečnostnímu managementu předmětných objektů, a to již v rané fázi návrhu projektu objektu.

Při uvědomění si nepopíratelného faktu, že každý objekt má povinnost mít zpracované požárně bezpečnostní řešení stavby (dále jen PBŘ) **a že v současné době jsou zájmové objekty vystavovány širokému spektru hrozeb, které tradiční posouzení v kontextu požární bezpečnosti nedokáže postihnout** (zaobírá se primárně neantropogenními hrozbami, tj. požáry), **vzniká skvělá příležitost pro hledání symbiózy mezi opatřeními fyzické a požární bezpečnosti již v rané fázi projektu objektu. Modelační nástroje a simulace mohou být nekonvenčním přístupem k bezpečnostnímu managementu, nanejvýš vhodným pro současnou turbulentní dobu.** Jedná se o jedinečnou dimenzi proaktivního a preventivního přístupu zainteresovaných osob (bezpečnostního manažera) k využití moderních postupů a umělé inteligence.

Pod tíhou výše uvedených souvislostí je vhodné PBŘ doplňovat o následující podněty, a tím vytvářet komplexní a ucelený pohled na fyzickou a požární bezpečnost:

- **analýza hrozeb a rizik – dopady podle metodického materiálu nelegislativní povahy Ministerstva vnitra ČR - Vyhodnocení ohroženosti měkkého cíle[3],**
- **simulace pohybu osob pro bezpečnostní otázky (kontext evakuace a únik osob mimo nebezpečí,)**
- **simulace šíření toxických látek v objektu (konkrétně kouře, zplodin hoření).**

Klíčové faktory pro modelování pohybu osob v rámci posuzování bezpečnosti staveb a jeho okolí je vnímáno apriori následující optikou:

1) Modelováním pohybu osob pro bezpečnostní otázky lze ověřit a komparovat aktuálnost PBŘ (prokázání bezpečné evakuace osob je mimo jiné jedním z cílových požadavků na požární bezpečnost stavby a je obsaženo v PBŘ).

V rané fázi návrhu lze zohlednit situace či nejkrizovější scénář, např. nedostupnost únikových východů či jejich případné úmyslné zablokování útočníkem. Vytvořit model evakuace s přihlédnutím na jistá ad hoc omezení.

2) Ověření vhodnosti evakuačního shromaždiště s ohledem na umístění objektu (3m průjezd a rozložení sil a prostředků složek integrovaného záchranného systému). Predikce pro zajištění bezpečnosti evakuovaných osob.

Schopnost zajištění volného prostoru pro rychlý zásah jednotek integrovaného záchranného systému v případě MU.

3) Predikce a zohlednění variant dalších operativních úkonů či jiných procedur.

Možnost flexibilní reakce na různé druhy MU díky možnosti vybrání preferovaných a pravděpodobných scénářů vývoje MU.

Modelování pohybu osob je doporučováno u významných staveb s charakterem měkkého cíle. Jedná se konkrétně o **Stavby kategorie III – podle vyhlášky č. 460/2021 Sb., o kategorizaci staveb z hlediska požární bezpečnosti a ochrany obyvatelstva (např. fakultní nemocnice či stanice metra).**

Navzdory tomu, že se jedná o nový nástroj, který však prozatím postrádá povinnost aplikace modelovacím softwarem, **ČSN 73 0802 Požární bezpečnost staveb – Nevýrobní objekty** v **Příloze I (Postup při specifickém posouzení rizikových podmínek požární bezpečnosti) bere toto opatření na zřetel a inkriminovaná příloha to popisuje, nikoliv explicitně.**

Nicméně na tomto půdorysu lze aplikovat modelaci scénářů požáru a evakuace. Již výše v textu zmiňovaná vyhláška č. 23/2008 Sb., o technických podmínkách požární ochrany staveb, **činí některé normy závaznými. ČSN 73 0802 je v předpisu explicitně uvedena, což v konečném důsledků může znamenat jistý krok vpřed v aplikaci modelovacích softwarů.**

PODĚKOVÁNÍ
poskytovateli finančních prostředků Ministerstvu vnitra České republiky za podporu **projektu DIMEP** (Digitální modelování evakuačních plánů ve společensky významných objektech s prvky umělé inteligence **– VBO1000034) z programu bezpečnostního výzkumu ČR 2021–2026 (SECTECH).**

Doba řešení projektu

1. 1. 2022 – 31. 12. 2023
Vývoj a testování softwarové platformy k modelování mimořádných událostí za účelem zlepšení a zefektivnění evakuačních opatření v zájmových stavbách a měkkých cílech. Jádrem platformy byl software na simulaci pohybu osob (Pathfinder, společnosti Thunderhead Engineering Consultants Inc.), který bude v rámci platformy obohacen softwarovou analýzou reálných videozáznamů ke kalibraci behaviorálního modelu simulací.

Na projektu spolupracovali:

- **Mezinárodní bezpečnostní institut, z.ú.**
- **Vysoké učení technické v Brně**
- **VDT Technology a.s.**
- **Gatum Group s.r.o.**

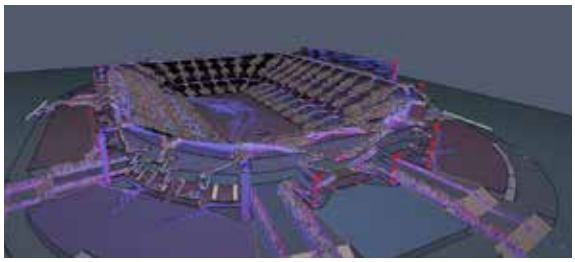
Mgr. Filip Gundza, MBA
Výkonný ředitel
Mezinárodní bezpečnostní institut, z.ú.

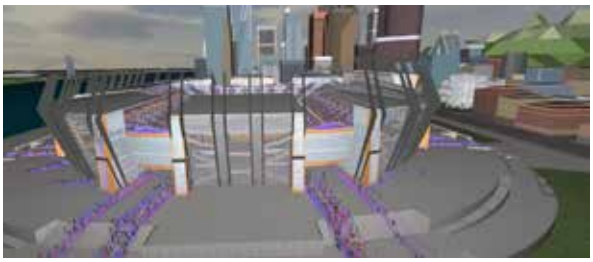
poznámky pod čarou

[1] ROSENKRANZ, J. „Měkké cíle" v pojetí Hasičského záchranného sboru České republiky. In Měkké cíle a jejich ochrana: Perspektiva spolupráce veřejného a soukromého sektoru. Policejní akademie České republiky: Praha, 2018, 104 s., ISBN: 978-80-7251-493-9.

[2] Explicitní podmínky vycházející ze zvláštních zákonů, jako např. č. 412/2005 Sb., o ochraně utajovaných informací, ve znění pozdějších předpisů, či zákona č. 224/2005 Sb., o prevenci závažných havárií, vyhlášky č. 361/2016 Sb., o zabezpečení jaderného zařízení a jaderného materiálu.

[3] Odtajněno v rámci tzv. „protiteroristického balíčku".





CHRÁNÍME VÁS
JIŽ OD ROKU
1992

BEZPEČNOSTNÍ TECHNOLOGIE A SLABOPROUDÉ SYSTÉMY

ABAS IPS MANAGEMENT

WWW.ABASCO.CZ

ABAS®
IPS MANAGEMENT

ÚTOK NA OBCHODNÍ CENTRUM

PŘÍPADOVÁ STUDIE

V červnu 2024 jsem měl tu čest vystoupit na konferenci Ochrana měkkých cílů 2024 s příspěvkem „Útok na obchodní centrum – případová studie".

Při hledání podkladů k této přednášce jsem zjistil, že většina útoků vedených v minulosti na obchodní centra, tedy místa s velkou kumulací lidí, proběhla v modu operandi „jednoduché" – pachatel se na obchodní centrum zaměří primárně, pobodá zde nožem nebo zraní střelnou zbraní návštěvníky či zaměstnance a je zneškodněn; útok často proběhne v řádu několika minut. Jindy bývá útok v obchodním centru „sekundární" – pachatel má původně v plánu „vraždit jinde, ale nevyšlo mu to", proto se zaměří na jiný měkký cíl, který je v dané chvíli nejblíže, a tím může být právě obchodní centrum.

Dá se říci, že obchodní centra, pro něž je příznačná velká koncentrace lidí, jsou pro teroristy obzvlášť přitažlivými cíli útoků.
Pro svou případovou studii jsem si nakonec vybral smutný masakr z roku 2013 v Keni. Odehrál se v Nairobi, hlavním městě Keni, v obchodním centru Westgate Mall, luxusním čtyřpodlažním nákupním středisku, které v té době provozovalo na prodejní ploše o výměře 33 tisíc m^2 na 80 obchodů a dvouposchoďový supermarket.

Dne 21. září 2013, přibližně ve 12:30 hod., přijíždí před hlavní vchod nákupního centra osobní vozidlo se čtyřmi teroristy – v celém objektu se v té době pohybuje na dva tisíce osob, zaměstnanců a návštěvníků.

Útočníci vyskakují z auta a začínají zabíjet již před vchodem do obchodního centra. Byli vybaveni AK47 a házeli granáty. První útok byl veden na venkovní terasu restaurace a druhý na „přístřešek" ostrahy na parkovišti. Následně útočníci pokračovali ve střelbě v kavárnách a obchodech, v zabíjení postupovali systematicky. Mezitím stovky zákazníků utekly přes supermarket k rampám.
Pachatelé se rozdělili a dva z nich šli přes venkovní parkoviště na střechu, kde probíhala dětská soutěž ve vaření. Vyděšení zákazníci utíkali do nejzazšího rohu parkoviště. Tam se neměli kam schovat a utéct a byli zabíjení včetně dětí (teroristé: nikdy nezabíjíme ženy a děti, ale v Somálsku jste naše zabili).
Střelba na střeše vyděsila lidi, co chtěli utéct přes rampy supermarketu a vrátili se zpátky na prodejní plochu, kde byli další dva střelci. Lidé v supermarketu se neměli kam schovat, vysoké regály bránily výhledu. Někteří se schovali za pulty s masem, tam je teroristé našli a zranili nebo zabili.

Teroristé také vnitřním rozhlasem supermarketu sdělili, proč tu jsou a že budou zabíjet, což vyvolalo další paniku mezi návštěvníky a zaměstnanci.
V jednom případě propustili útočníci matku s dětmi a omlouvali se: „nejsme zrůdy", a dali dětem čokoládové tyčinky Mars z regálu, na děti se pak smáli a mávali jim.
Informace o střelbě se začala šířit na sociálních sítích a v médiích, prvotní zprávy hovořily o loupežném přepadení, následně, že je do útoku je zapojeno až 15 střelců…
Policie dorazila na místo po 15 minutách, po 4 hodinách si moc převzala keňská armáda, panoval zmatek ve velení a NIKDO nešel dovnitř zachraňovat návštěvníky centra a zaměstnance. Mezitím teroristé v obchodním centru dále zabíjeli. Několik hodin trvalo bezpečnostním složkám i zajištění perimetru.

Po několika hodinách nečinnosti se do nákupního centra odvážilo pár policistů v civilu s krátkými zbraněmi a dobrovolníci, mezi nimi a teroristy vznikla přestřelka a policisté použili slzný plyn, čímž přinutili teroristy se stáhnout do zadní části supermarketu a mohli zachránit některá rukojmí. Následně policie a armáda zahájila akci, jenže po 4hodinovém řádění už byla většina ohrožených osob po smrti.

Policie a vojáci střílely po všech, koho viděli, jenže to byli už jen zaměstnanci a nakupující. Současně policie a vojáci střílely i po sobě. Následně, protože panoval zmatek, KDO bude velet, se po 90 minutách všichni z obchodního centra stáhli.

Teroristé už v té době na prodejní ploše nebyli, sjeli služebním výtahem do skladu nábytku, kde odpočívali, modlili se a připravovali na další boj.
Na místo se začali stahovat příbuzní a známí lidí uvězněných v centru, úřady dávají první prohlášení, že vše budou mít brzo pod kontrolou.
V noci vojáci zahájili útok, útočníci byli zabarikádováni ve skladu nábytku, armáda a policie prohledávaly patro po patře, místnost po místnosti. S útočníky se snažily vyjednávat, nevědělo se, zda mají u sebe rukojmí.
Armáda použila ruční granátomety, následoval požár a zhroucení části centra, teroristé byli zneškodněni. Armáda tvrdila, že za požár a zhroucení objektu mohou teroristé. Nicméně agentura AFP citovala jednoho z účastníků zásahu proti teroristům: *„Armáda pak proti nim použila přenosnou protitankovou zbraň Carl-Gustav ráže 84 milimetrů."*

Akce trvala celkem **4 dny**. Na místě zahynulo **67** osob, bylo více než **200** zraněných a **27** osob pohřešovaných. Oběťmi byli občané zemí Keňa, Velké Británie, Indie, Kanada, Francie, Austrálie, Čína, Nizozemí a dalších.
Útok provedla teroristická skupina Al-Shabaab jako odvetu za to, že Keňa zahájila intervenci na území Somálska ve snaze pomoci somálské vládě proti Al-Shabaab.
V říjnu 2020 uznal keňský soud dva muže vinnými ze smrtonosného útoku na obchodní centrum v roce 2013. Muži byli usvědčeni ze spiknutí a napomáhání útočníkům a byli odsouzeni do vězení. Ostatní podezřelí zůstali na svobodě.

ÚTOČNÍCI:

- útok byl plánován měsíce z uprchlického tábora Kakuma v Keni;
- útočníci „studovali" nákupní centrum, obchodní aktivity a typ osob, které ho navštěvují;

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČESKÉ REPUBLIKY

- údajně si útočníci v nákupním centru „pronajali" obchod a udělali si z něj sklad zbraní, které tam postupně nosili;
- útočníci si registrovali 8 telefonních karet;
- útočníci spolupracovali s „místními";
- zabíjeli „nemuslimy", pokud někdo znal jméno Mohamedovy matky nebo odrecitoval verš z Koránu, byl propuštěn;

BEZPEČNOSTNÍ SLOŽKY, GOVERMENT:

- o hrozbě útoku věděla tajná služba Keni rok dopředu
- rada bezpečnosti OSN varovala před útokem měsíc předem
- vstoupit „útočníkům" do Keni dovolila korupce u policie
- bezpečnostní složky se nebyly schopny „koordinovat" (kdo velí), proto obléhání trvalo 4 dny
- policisté a vojáci „stříleli i proti sobě", následně „vyrabovali Westgate" (na záběrech z kamer obchodního centra jsou vidět, jak si v igelitkách odnášejí drahé hodinky, šperky, mobilní telefony)
- nedbale byla provedena forenzní práce (několik pachatelů skončilo bez trestu)
- úředníci uvalili embargo na informace až do roku 2021 (útok se stal v roce 2013)

WESTGATE MALL:

- částečné obnovení provozu nákupního centra v roce 2015
- plné obnovení nákupního centra v roce 2018
- ostrahu nově zajišťuje izraelská soukromá společnost
- škody nákupního centra v řádu několik milionů dolarů
- Keňa zaznamenala pokles turistiky a tím i pokles ekonomiky

ZAJÍMAVOSTI:

- na místě pracovali bezpečnostní poradci z Izraele
- s vyšetřováním pomohly USA
- do obchodního centra dorazili „dobrovolníci", jimž náleží poděkování, protože díky nim byly zachráněny životy několika stovek osob a oni neváhali riskovat ty svoje. Jejich příběhy z médií:
- **Střelecký klub:** *Raju se skryl a ze svého telefonu začal psát zprávy známým ze střeleckého klubu. Ti si zprávu předávali vzájemně dál a vyzbrojeni svými civilními zbraněmi vyráželi překotně k obchodnímu centru, kde* ***společně s dalšími civilisty, členy soukromé bezpečnostní služby a v civilu oblečenými policisty zahájili prvotní odpor proti útočníkům a pomohli utéct do bezpečí stovkám návštěvníků centra.***

- **Mark a John:** *Mark (pseudonym, bývalý důstojník SAS) a John (pseudonym, bývalý člen irských Rangers) se 21. září 2013 nacházeli v centrále ropné společnosti, které poskytovali ochranu, když se chvíli po poledni dozvěděli, že do místního obchodního domu Westgate vrazili ozbrojenci. Když obvolávali zaměstnance společnosti, zjistili, že dva se schovávají v sushi restauraci v druhém patře obchodního domu. Zachránili je a s nimi spousty dalších osob.*
- **Abdul Haji** – *sms od bratra:* ***„****Jsem v pasti ve Westgate. Teroristický útok. Modli se za mě." Sotva vystoupil z auta, díval se do hlavně zbraně. Harishi Patelovi, členu indické domobranné skupiny „Krišnova jednotka", se totiž vůbec nelíbil. V té chvíli bylo už jasné, že nejde o loupežné přepadení, ale o teroristický útok somálské islamistické skupiny Al-Shabaab, která takovým činem už dříve několikrát vyhrožovala. Haji, viditelně Somálec, muslim a s pistolí v ruce, tak v tu chvíli vůbec nevzbuzoval asociaci dobrého samaritána. Rychle vytáhl zbrojní průkaz a přesvědčil Patela o tom, že je taky jeden z „good guys with a gun". Společně s Patelem se pak přidali k policistům v civilním oblečení – Nurovi Alimovi a jeho dvěma kolegům. Postupovali dovnitř obchodního centra a snažili se zachránit co nejvíce lidí, zatímco policie venku hodiny čekala na příjezd zásahovky.*
- **Troulan,** *vyzbrojený pouze svou osobní pistolí, vyvedl z obchodního domu více než 100 osob. Celkem se do centra vrátil více než desetkrát, přičemž několikrát se dostal do přestřelky s těžce vyzbrojenými útočníky.*

Jaromír Průša
předseda ASIS International ČR

VÝBĚR BEZPEČNOSTNÍ TECHNOLOGIE

Ochrana měkkých cílů, jako jsou veřejné budovy, školy, nákupní centra, dopravní uzly, masové veřejné akce apod., kde se soustředí velké množství lidí a které nejsou apriori chráněny proti možným teroristickým útokům, přestože jsou pro takové útoky lákavým potenciálním cílem, se v současné době stává klíčovou výzvou pro bezpečnostní specialisty. Vzhledem k narůstajícímu riziku teroristických útoků a jiných násilných činů je nezbytné správně vybrat a implementovat vhodné bezpečnostní technologie.

Tento článek se zaměřuje na obecné principy výběru bezpečnostních technologií a následně navrhuje konkrétní řešení, které je vhodné pro ochranu měkkých cílů, s ohledem na současné technologické možnosti.

Obecné principy výběru bezpečnostní technologie

Při výběru technologie pro ochranu měkkých cílů je klíčové postupovat systematicky a zohlednit několik základních principů. Tyto principy vycházejí z metodiky ochrany měkkých cílů a dalších strategických dokumentů a také z obecně přijímaných pravidel dobrého hospodáře, jež se uplatňují nejen ve veřejné správě, ale i v soukromém sektoru. Uvádím hlavní faktory, které by měly být zváženy:

Soulad se strategickými dokumenty

Každá technologie, kterou zvažujeme pro ochranu měkkých cílů, by měla být v souladu se strategickými bezpečnostními dokumenty a respektovat je. Nejvyšším takovým dokumentem v ČR je **Bezpečnostní strategie České republiky** – dokument pravidelně aktualizovaný Ministerstvem zahraničních věcí ČR a schvalovaný vládou ČR. Poslední aktualizace je z roku 2023 a mluví mj. o rostoucí hrozbě teroristických útoků a o nutnosti ochrany zejména kritické infrastruktury před potenciálními teroristickými útoky.

Mnohé měkké cíle jsou zároveň součástí kritické infrastruktury. Na několika místech se v ní technologie také zmiňují. Jednak je zde vyzdvihována potřeba využít moderní technologie pro prevenci a boj s teroristickými útoky a jednak se tu upozorňuje na problematičnost technologií dováže-ných z Ruska a Číny, které jsou zároveň označovány za geopolitickou hrozbu, jak o tom svědčí některé citace: *„Čína provádí kyberšpionáž, usiluje o kontrolu globálního datového provozu a využívá různých forem sociálně-ekonomického nátlaku a dalších nástrojů hybridního působení. Čínské firmy jsou fakticky propojeny se státem a připraveny sloužit jeho záměrům.“ […] „Rizikem jsou čínské investice do české a evropské kritické infrastruktury, dominance ve strategických dodavatelských řetězcích, kontrola klíčových komodit a rozvoj nastupujících a přelomových technologií, zejména umělé inteligence mimo etická pravidla a mezinárodní standardy. Čína usiluje o změnu těchto standardů. Vede dezinformační aktivity a mění narativ, který byl dosud v mezinárodním společenství vnímán jako konsenzuální. Čína nedostatečně chrání duševní vlastnictví a zneužívá instrumenty vědecké a akademické spolupráce.“*

Opustíme-li tuto nejvyšší strategickou úroveň, dostaneme se k úzce zaměřeným dokumentům týkajícím se tematiky ochrany měkkých cílů. Při výběru technologií je to určitě **Metodika ochrany měkkých cílů Ministerstva vnitra ČR**. Tento dokument se zabývá identifikací těchto míst, hodnocením rizik, a stanovuje opatření pro prevenci a minimalizaci možných útoků. Klíčovými prvky jsou spolupráce mezi státními orgány, soukromým sektorem a občanskou společností, stejně jako využití moderních technologií a bezpečnostních opatření k ochraně těchto zranitelných míst. Metodika klade důraz na včasnou detekci hrozeb, rychlou reakci na krizové situace a ochranu životů a zdraví obyvatel.

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČESKÉ REPUBLIKY

Integrace s bezpečnostními procesy

Vybraná technologie musí být schopna efektivně se integrovat s již nastavenými bezpečnostními procesy organizace. Samozřejmě to předpokládá, že organizace provozující měkký cíl má takové procesy nastaveny. Tento proces začíná důkladnou bezpečnostní analýzou hrozeb a rizik, která zároveň definuje potřebná opatření a metody. Zvolená technologie pak musí tato opatření respektovat, a navíc je propojit s ostatními kategoriemi bezpečnostních opatření podle Metodiky ochrany měkkých cílů, což je fyzická bezpečnost, elektronické prvky a mechanické prvky.

Často však bohužel vidíme, že to bývá opačně. Nepoučený a neznalý provozovatel měkkého cíle se mnohdy nechá výrobcem nebo jiným subjektem z dodavatelského řetězce (instalační firmou, distributorem atp.) přesvědčit, že nějaká konkrétní technologie je ta jediná a nejlepší pro jeho potřeby. Pořídí si ji a až potom přemýšlí, jak ji zasadit do svých procesů, případně tyto procesy dokonce podle pořízené technologie teprve vytváří. Nemluvě o tom, že provozovatel nezřídka pořídí jen různé komponenty bezpečnostních technologií (elektronické a mechanické prvky), které mezi sebou nejsou vzájemně kompatibilní a integrovatelné. Nastavení bezpečnostních procesů tím výrazně komplikuje, a hlavně pak celkové bezpečnostní řešení nesplňuje svůj hlavní účel a není ve smyslu ochrany před hrozbami a snižování rizik efektivní.

Efektivnost a hospodárnost řešení

Klíčovým faktorem je rovněž efektivnost a ekonomická stránka pořízení, a zejména pak následného provozování technologie. Před samotným nákupem by měl být proveden průzkum trhu, případně i předběžné tržní konzultace (PTK). V praxi se však namnoze setkávám s odporem majitelů a provozovatelů měkkých cílů k provádění předběžných tržních konzultací. Většina těchto subjektů přitom patří do veřejného sektoru a řídí se při pořizování technologií zákonem 134/2016 Sb., o zadávání veřejných zakázek, který v § 3 provádění předběžných tržních konzultací před samotným pořízením umožňuje a přímo doporučuje.

Vývoj technologií, zvlášť v posledních pár letech, je tak překotný, že není v kapacitách jedince znát aktuální trendy a možnosti všech oblastí, které dnes do hybridní bezpečnosti zasahují. Odborné znalosti bezpečnostních technologií platné před deseti nebo i pěti lety jsou už dnes zastaralé, pokud má řešení odpovídat svou efektivností a hospodárností aktuálním možnostem a trendům. Aktuálními trendy jsou otevřená, multimodální, integrovatelná řešení využívající v maximální míře automatizaci. Doporučuje se také testování technologií v pilotním provozu (Proof of Concept – PoC).

Každý měkký cíl má svá specifika a nemůže existovat univerzální řešení, které by se jen zapojilo do sítě a dělalo svou práci. Pro zajištění hospodárnosti zvoleného řešení je dobré podívat se na něj z pohledu kalkulace celkových nákladů na vlastnictví a provoz po předpokládanou dobu jeho fungování, což bývá v průměru 5–7 let. (Total Cost of Ownership – TCO). Platí zde více než jinde stará moudrost, že věci s levnou pořizovací cenou se v čase většinou prodraží. Důležité je také vyhnout se situacím, kdy by technologie mohla vést k tzv. vendor lock-in, tedy závislosti na jednom dodavateli. A to ať už z hlediska technologického „háčku" nebo právních kliček v uzavřených dodavatelských a servisních smlouvách. V obou případech se takové vendor lock-in řešení stává pro provozovatele měkkého cíle v budoucnu potenciální noční můrou a představuje budoucí nečekané náklady. Pravidlem je, že zvolená technologie a uzavřená smlouva s dodavatelem musí umožňovat jak snadné rozšiřování, tak i zužování nebo i ukončení jejího nasazení bez nějakých záludných technologických komplikací a smluvních pokut.

Soulad s legislativními regulačními požadavky

Při výběru technologie je nutno vzít v potaz také legislativu. Samozřejmě existuje spousta dílčích oborových norem a zákonů, o kterých tady nemáme prostor rozepisovat se. Rád bych ale upozornil na některé nové směrnice přicházející i do České republiky z Evropské unie. Patří sem například aktuálně transponovaný **zákon o kybernetické bezpečnosti** vycházející z nedávno schválené **směrnice NIS2** pro posílení opatření kybernetické bezpečnosti.

Moderní bezpečnostní technologie jsou z větší míry již „čistokrevná" IT síťová zařízení, a tak se jich jednoznačně týkají také doporučená a požadovaná technická a organizační opatření definovaná právě touto regulací. Moudrý provozovatel subjektu měkkého cíle bude při pořizování technologií brát toto vše v úvahu již nyní, přestože praktická účinnost tohoto nově vznikajícího zákona nastane zřejmě až počátkem roku 2025, a potom ještě poběží navíc zřejmě roční ochranná lhůta. Vždyť

bezpečnostní technologie se nepořizují na pouhé měsíce, ale na dlouhé roky, takže dobrý hospodář to v potaz vezme.

Další aktuálně transponovanou směrnicí, která ovlivní požadavky na bezpečnostní technologie alespoň u části měkkých cílů, zejména v dopravě a zdravotnictví, je **směrnice Critical Entity Resilience** (CER), která je aktuálně v gesci MV ČR a je transponovaná do zákona o odolnosti kritických subjektů (zkráceně zákona o kritické infrastruktuře). Cílem je zajistit, aby byly klíčové subjekty pro fungování společnosti schopny čelit bezpečnostním hrozbám, včetně teroristických útoků. Musí tak přijímat technická a organizační opatření k posílení své odolnosti, včetně vypracování krizových plánů a provádění cvičení pro zvládání mimořádných situací. Použité bezpečnostní technologie s tím budou významně souviset a ovlivňovat efektivnost takových opatření, jak jsem se již zmínil v předchozí podkapitole.

Dalšími regulačními požadavky jsou také dvě nařízení z EU. Tím prvním je starší (účinné od roku 2018), již víceméně známé **nařízení GDPR.** Bezpečnostní technologie, zejména kamerové systémy, významně zasahují do zpracování osobních údajů. Bude tedy velmi důležité pro majitele a správce měkkých cílů v rolích správců a zpracovatelů osobních údajů zajistit, aby pořízená technologie chránila soukromí a plnila soulad s tímto nařízením, a přitom co nejméně kompromitovala úroveň fyzicko-bezpečnostních opatření, která

se od těchto technologií očekávají především. Je to náročný úkol, ale technologie některých výrobců tohle již umožňují. Téma ochrany soukromí u kamerových systémů je aktuálně znovu velmi diskutované a sledované, zejména díky letos na jaře vydané **Metodice k návrhu a provozování kamerových systémů,** vydané Úřadem pro ochranu osobních údajů.

Druhým nařízením z EU, které bude v blízké budoucnosti také částečně promlouvat do výběru technologií, je nejčerstvější. Je platné od 2. 8. 2024, plná

účinnost se očekává postupně mezi 6 až 24 měsíci od schválení regulace, podle kritičnosti jednotlivých ustanovení. Jedná se o tzv. **AI Act,** plným názvem **Nařízení Evropského parlamentu a Rady,** kterým se stanoví harmonizovaná pravidla pro umělou inteligenci. Má za cíl stanovit právní rámec pro používání systémů umělé inteligence (AI) v EU. Tento akt je navržen tak, aby zajistil bezpečné a etické využívání AI technologií a současně podporoval inovace a konkurenceschopnost v této oblasti.

Snaží se chránit základní práva občanů EU, jako je právo na soukromí, nediskriminaci a ochranu osobních údajů. Zároveň se zaměřuje na zajištění bezpečnosti AI systémů. Vzhledem k tomu, že trend využití umělé inteligence proniká i do bezpečnostních technologií, včetně těch na ochranu měkkých cílů, bude moudré posuzovat plánované pořízení bezpečnostních technologií i z tohoto aspektu.

AI Act zavádí například klasifikaci AI systémů na základě míry rizika, které představují. Jako jednu z nejrizikovějších považuje biometrickou identifikaci na dálku v reálném čase ve veřejně přístupných prostorech, která může být součástí některých bezpečnostních řešení pro ochranu měkkých cílů před teroristickými útoky, například formou rozpoznávání obličejů (facial recognition). Takové systémy jsou dokonce klasifikovány jako „zakázané postupy v oblasti AI" a podléhají přísným regulačním požadavkům. AI Act sice i u této technologie připouští výjimky, ale jsou velice úzce a přesně stanoveny. Jde např. o prevenci konkrétního, závažného a bezprostředního ohrožení života nebo fyzické bezpečnosti osob nebo předvídatelného teroristického útoku a lokalizace nebo identifikace osoby podezřelé ze spáchání trestného činu.

Konkrétní bezpečnostní řešení pro ochranu měkkých cílů

V předchozí části článku byly vyjmenovány a popsány doporučené principy pro výběr bezpečnostních technologií a řešení vycházející z Metodiky ochrany měkkých cílů a dalších strategických dokumentů a také z obecně přijímaných pravidel dobrého hospodáře ve veřejné i soukromé sféře. Aby tento článek nezůstal jen teoretickým vodítkem, přináší ve své poslední části také konkrétní návrh bezpečnostního řešení, které je efektivní, hospodárné, v souladu s legislativou a snadno integrovatelné s existujícími bezpečnostními procesy pro většinu subjektů měkkých cílů.

Zde je potřeba zdůraznit, že pro pozitivní naplnění všech zmiňovaných principů je kriticky důležitý výběr výrobců jednotlivých komponent budoucího bezpečnostního řešení. Většina nových legislativních norem zmiňovaných v předchozí části o tom hovoří jako o posuzování dodavatelů nebo dodavatelského řetězce (NIS2, Metodika GDPR, CER). Důvodem je fakt, že pokud výrobce nevyjde dodavatelům vstříc již při navrhování a vývoji technologických prvků a zařízení, soulad s požadovanými principy při instalaci a implementaci již buď nebude možný, nebo bude možný jen za cenu zvýšeného úsilí, nákladů a kompromisů v efektivnosti.

Jedná se například o principy „security by design" a „privacy by design", podle nichž někteří zodpovědní výrobci začali své produkty vyvíjet a produkovat. Pokud budou vybrány produkty a technologie, které tyto vlastnosti a funkce nemají, nemůže být ani sebevíc zkušený a kompetentní dodavatel (integrátor nebo instalační firma) schopen tuto absenci nahradit. Pro navržené technologické řešení jsme proto pečlivě vybrali důvěryhodné výrobce všech jeho komponent. Jedná se o švédského výrobce kamer a síťových reproduktorů **Axis Communications,** českého výrobce dveřních interkomů **2N**, kanadského výrobce bezpečnostní softwarové platformy **Genetec** a českého výrobce aplikací pro detekci nebezpečných zvukových událostí **Jalud Embedded.**

Senzorová část – oči a uši systému

Kamery s vestavěnou analýzou obrazu a zvukových událostí – jsou vybaveny umělou inteligencí (AI), která umožňuje pokročilou analýzu obrazu a zvuku v reálném čase. Díky tomu je možné rychle identifikovat neobvyklé nebo podezřelé situace, což výrazně zvyšuje schopnost prevence a včasné detekce hrozeb. Není zde myšlena přímo biometrická identifikace, ale obecná objektová analýza obrazu.

Dveřní interkomy s kamerami – zajišťují kontrolu přístupu do chráněných prostor, přičemž integrují vizuální a zvukovou komunikaci. To umožňuje rychlé ověření identity osob a efektivní řízení přístupu.

Centrální vyhodnocovací část – mozek systému

Bezpečnostní integrační softwarová platforma – slouží jako centrální mozek celého bezpečnostního systému. Umožňuje integraci všech bezpečnostních prvků do jednoho celku, což

zjednodušuje řízení a monitorování. Platforma poskytuje přehled o všech událostech a umožňuje rychlou reakci na incidenty.

Aktivní část – ústa a ruce systému

Síťové reproduktory – jsou zodpovědné za šíření varovných hlášení a komunikaci s návštěvníky nebo zaměstnanci. Mohou být využity jak pro varování při krizových situacích, tak pro běžné informační účely.

Přístupový systém – umožňuje řízení přístupu do různých částí objektu, a to jak v běžném provozu, tak v krizových situacích, kdy může být nutné rychle uzamknout nebo odemknout určité prostory (evakuace, invakuace).

Výhody navrženého řešení

Navržené bezpečnostní řešení nabízí několik zásadních výhod, které jej činí ideálním pro ochranu měkkých cílů – a to jsou:

- **Multimodální analýza dat.** Kombinace analýzy obrazu a zvuku umožňuje větší přesnost detekce, a tím lepší prevenci hrozeb. Systém je schopný rozpoznat nebezpečné situace, které by jinak mohly zůstat nepovšimnuty, například křik nebo střelbu.
- **Otevřená technologie.** Řešení je založeno na otevřených technologiích, což zajišťuje snadnou integraci s dalšími bezpečnostními systémy a minimalizuje riziko vendor lock-in.
- **Flexibilita.** Systém je flexibilní a může být upraven podle specifických potřeb různých typů měkkých cílů. To zahrnuje možnost mobilního nasazení nebo rozšíření o další prvky.
- **Hospodárnost.** Řešení je založeno na produktech výrobců, kteří cílí na nízké celkové náklady na provoz (TCO) v horizontu 5–7 let.
- **Soulad s legislativou.** Výrobci tohoto řešení jsou v souladu a jejich produkty pomáhají být v souladu s technickými a organizačními požadavky nových směrnic a nařízení z EU (NIS2, CER, CSRD, AI Act, GDPR).
- **Respektování principu OORZ**. Řešení respektuje metodu OORZ (Odstrašit – Odhalit – Reagovat – Zmírnit dopad), která je klíčová pro efektivní ochranu měkkých cílů.

Výběr správné technologie pro ochranu měkkých cílů je klíčovým krokem k zajištění bezpečnosti osob a majetku. Je nezbytné postupovat podle osvědčených principů, které zahrnují respektování strategických dokumentů, integraci s bezpečnostními procesy, efektivitu a ekonomičnost řešení a splnění všech relevantních regulačních požadavků. Konkrétní bezpečnostní řešení, které bylo v tomto článku představeno, poskytuje komplexní ochranu měkkých cílů a může sloužit jako základ pro další rozvoj bezpečnostních technologií.

Výběr a implementace bezpečnostních technologií by měly být prováděny s náležitou pečlivostí a důrazem na kvalitu. Pouze tak lze zajistit, že budou chráněna ta nejcennější aktiva – zdraví a životy lidí.

Mgr. Dalibor Smažinka, MBA,
Expert na bezpečnostní technologie

ČESKÁ POŠTA SECURITY STŘEŽÍ VELKÉ FIRMY

Společnost OMEXOM GA Energo (součást holdingu VINCI Energies) v Plzni Bolevci je jednou z firem, které nově střeží Česká pošta Security (dále jen ČP Security). Služby vzdáleného bezpečnostního monitoringu hlavního sídla a poboček zajišťuje ČP Security ze svého dohledového centra za využití systému iVISEC.

Jak řešení vzdáleného dohledu za využití špičkových zařízení a systémů nové generace funguje, popisuje Karel Skokan, komerční ředitel společnosti Z.L.D., která je výrobcem a poskytovatelem zastřešujícího dohledového a řídicího systému iVISEC, jejž ČP Security ke střežení objektu využívá: *„Poskytované bezpečnostní služby GaaS* jsou realizovány na nejpokrokovějších technologiích. Zásadní roli má software iVISEC, který na jednotlivých lokalitách společnosti OMEXOM zajišťuje integraci dílčích provozních a bezpečnostních technologií a je využíván zaměstnanci společnosti OMEXOM pro každodenní potřeby. Zároveň však lokální instance iVISEC na pobočkách předávají v reálném čase informace o událostech do nadřízené instance iVISEC v hlavním sídle společnosti OMEXOM a souběžně také bezpečnostní události na multitenantní instanci iVISEC provozovanou na Dohledovém přijímacím a poplachovém centru (DPPC) České pošty Security."*

V případě výskytu nestandardní události jsou pracovníci DPPC okamžitě vizuálně i zvukově upozorněni, mají pohotově k dispozici videostreamy z místa události a mohou i nahlédnout do videozáznamů pro pochopení souvislostí, jak událost vznikla a co jí předcházelo. *„Operátoři DPPC tak získávají situační povědomí a kvalifikovaně rozhodují o dalším postupu. V případě zjištěného bezpečnostního incidentu vysílají na místo zásahovou jednotku,"* dodává Karel Skokan.

DPPC je provozováno ČP Security a využívá výše uvedený systému iVISEC. Ten na základě přednastavených pravidel vyhodnocuje data přijímaná z již instalovaných technologií, které se v objektech společnosti OMEXOM nacházely. Jedná se především o video dohledový systém (VSS) a poplachový zabezpečovací a tísňový systém (PZTS). Využití umělé inteligence (AI) výrazně zlevnilo střežení, neboť ho lze provádět na dálku a není potřeba zajistit na místě fyzickou ostrahu.

„Projekt vzdáleného videodohledu, respektive služba 'střežení na dálku' prostřednictvím moderní zobrazovací a vyhodnocovací techniky bude nedílnou součástí všech řešení tohoto typu již v blízké budoucnosti. Progresivní zákazníci, jakým je společnost OMEXOM, jsou klíčoví pro rozvoj služeb s přidanou hodnotou, za což jim patří poděkování. Pro ČP Security je ctí s takovými klienty spolupracovat, díky nim se učit, a tak rozvíjet kvalitní služby," uzavírá Tomáš Hampl, jednatel společnosti ČP Security. *„Bezpečnostní služby ČP Security jsme začali využívat na jaře letošního roku na třech lokalitách v ČR a za první měsíce fungování mohu hodnotit službu jako kvalitní a spolehlivou. Systémy používané ČP Security bylo možné propojit s našimi stávajícími technologiemi, což je pro nás velkou výhodou. Díky propojení technologií je zajištěna vysoká úroveň zabezpečení majetku společnosti a bezpečnost našich zaměstnanců na pracovišti. Zároveň nám s ČP Security napomáhá k předcházení vzniku mimořádných a nežádoucích krizových situací,"* shrnuje Lenek Viduna, bezpečnostní manažer společnosti OMEXOM GA Energo.

OMEXOM GA Energo plánuje rozšířit služby GaaS na další pobočky, a navíc využít další možnosti, které celé řešení přináší, jako je např. včasná výstraha v případě poruch na infrastruktuře objektů apod.

Použité zkratky:
*GaaS – Guarding as a Service – bezpečnostní služba, kterou komerčně nabízí ČP Security, spočívá zejména ve vzdáleném bezpečnostním monitoringu areálu zákazníka.

V Plzni dne 1. června 2024

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČESKÉ REPUBLIKY

iVISEC OMEXOM Z.L.D. ČP SECURITY


CP SECURITY
DPPC
iVISEC
OMEXOM
Lokalita 1 (HQ)
iVISEC
VSS
PZTS
IP reproduktory
Serverové videoanalytiky
OMEXOM
Lokalita 2
iVISEC
VSS
PZTS
IP reproduktory
Serverové videoanalytiky
OMEXOM
Lokalita 3
iVISEC
VSS
PZTS
IP reproduktory
Kamerové videoanalytiky

PSYCHICKÁ ZÁTĚŽ A STŘELBA

V tomto čísle časopisu je uveřejněn článek policejního vyjednavače pana Zdeňka Orla o střelbě na FF UK v Praze. Článek se mi velmi líbí, je přehledný, stručně mapuje celou situaci, přičemž se v něm autor nepouští do doporučení a závěrů, které mu nepřísluší. Dovolím si doplnit tento článek o několik poznámek z pohledu psychologie.

Všichni účastníci zmíněné střelby prožívali především situaci nenadálého psychického zatížení.
Pro psychickou zátěž existuje celá řada vymezení, nejvýstižnější se mi jeví tato definice:

„Psychická zátěž je vždy vnitřně prožívaný individuální rozpor mezi vnějšími požadavky na člověka kladenými a jeho momentální připravenostíje řešit."

Toto vymezení obsahuje většinu základních znaků psychické zátěže. Problémem však vždy je, že vznik zátěže nelze dopředu předvídat. Proto hraje významnou roli při jejím řešení zmíněná momentální připravenost člověka. Účastníci střelby na FF UK nebyli pro tuto šílenou situaci připraveni, a proto se mnohdy chovali zmateně či neúčelně.

Psychická zátěž může mít pro člověka svůj význam, pozitivní i negativní. Pozitivum je v tom, že nás často motivuje, tzv. nabudí, i k nenadálým výkonům. Negativem je, že nás překvapí, a tudíž nás může tzv. ochromit, kdy nejsme schopni se rozumně rozhodovat a chovat. Toto se právě přihodilo některým účastníkům střelby. Celá situace byla tak naprosto mimořádná, že se nechci pouštět do hodnocení chování jejích účastníků.

Psychickou zátěž lze dělit různými způsoby. Např. na náhlou a postupně vznikající, komplexní a dílčí, trvalou nebo okamžitou apod. Nejlepším se mi jeví dělení na zátěž **běžnou, zvýšenou, hraniční a extrémní.**

Jedná se o klasifikaci z hlediska množství nároků kladených na jedince z vnějšku. To právě určuje smysluplnost a rozumnost jeho budoucí reakce. Nerozumně se však lidé často chovají i v situacích, na něž se lze včas, dopředu připravit. Potom se nelze divit jejich zmatku v případech vznikajících nečekaně, náhle.

Běžnou zátěží rozumíme události, které nás běžně potkávají. Reagujeme v nich běžnými, naučenými způsoby, tzv. schématy. I z těchto situací (např. nákup, cesta autobusem apod.) se ale může vyvinout zatížení vyššího typu.

Zvýšenou zátěž představují všechny nenadálé situace, jdoucí již nad rámec našeho běžného zatížení (např. nenadálé zatroubení auta, ať jsme chodec či řidič). A již zde se objevují zmatené lidské reakce (např. při nečekaném zatroubení skáčeme do vozovky, či prudce brzdíme a můžeme způsobit velkou dopravní kolizi). Existuje obrovské množství těchto podnětů, o nichž lze říct, že v nich situaci podléháme a zátěže neřešíme úspěšně. Většina rozumných lidí ovšem zvýšené zatížení s přehledem zvládá. Mezi tyto situace však v žádném případě nelze řadit střelbu na FF UK Praha.

Hraniční zátěží pro nás jsou události, které sice ještě zvládáme, ale přitom se již ocitáme na hranici svých sil a možností. Jedná se o případy, o nichž dodatečně konstatujeme, že bychom je už nikdy nechtěli zažít (např. náhlá a vážná nemoc někoho blízkého, závažná dopravní situace, z níž jsme se nakonec dostali, apod). Po vyřešení těchto událostí potřebujeme nějaký čas na regeneraci psychických a často i fyzických sil.

Extrémní zátěž již nezvládáme. Reagujeme extrémními způsoby, pláčem, křikem, nesmyslnými pohyby, apatií či depresí. Situace nás zcela pohltila, zvítězila nad námi. Proto označení extrémní.

Psychická zátěž má, jako celek, velkou dynamiku – pokud nás neochromí, uvádí nás do pohybu. Její zvládání je velmi individuální. To znamená, že pro někoho je určité zatížení jen zvýšené, jiný však tutéž situaci vnímá a řeší extrémně, např. prudkou a nesmyslnou emoční reakcí, afektem. Anebo naopak.

Střelba na FF UK představovala, z hlediska svého výskytu, pro většinu zúčastněných hraniční zátěž, s níž nikdo z nich nepočítal. Nebyla však extrémní zátěží. Všechny zapojené síly IZS chtěly zásah zdárně řešit, tudíž se pohybovaly v rovině hraničního zatížení, psychického i fyzického.

Lze tedy konstatovat, že všechna budoucí cvičení IZS by měla se vznikem podobné události, jako byla střelba, počítat a zařadit do svých výcvikových plánů i učení o psychické zátěži, s cílem její optimalizace a úspěšného zvládání.

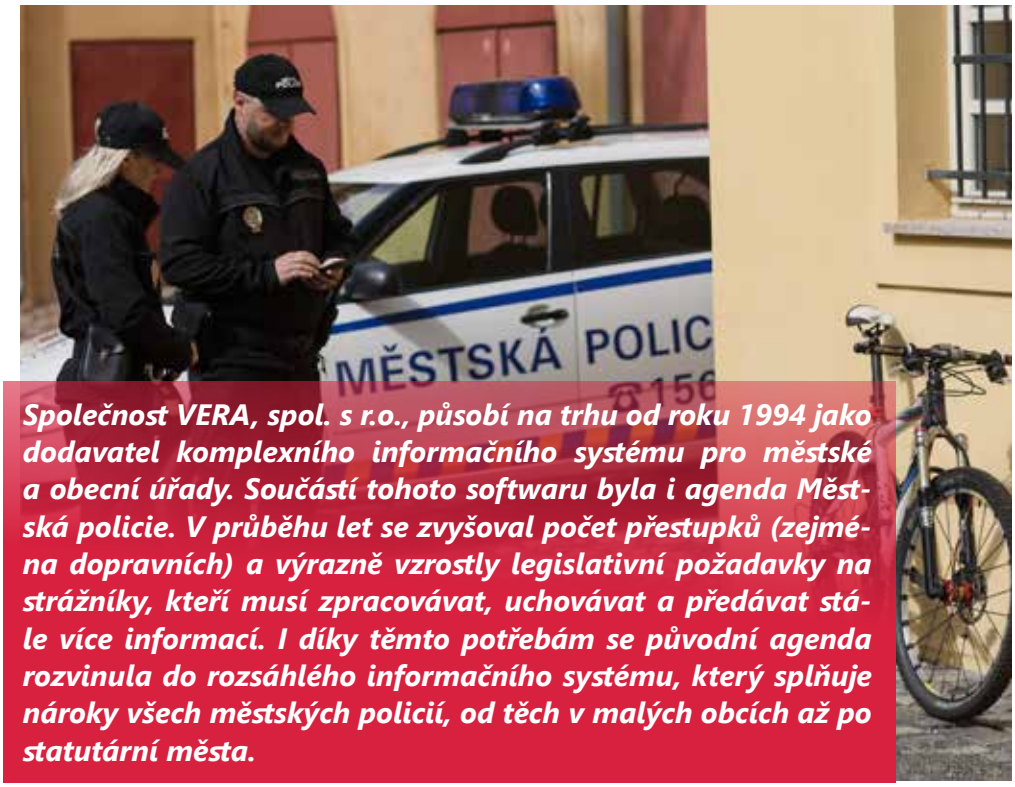
Poznatky uvedené v tomto příspěvku nejsou žádnou hlubokou psychologickou teorií. Jsou určeny především pro čtenáře z řad laické veřejnosti. Tito by se pak mohli, po přečtení příspěvku, pokusit uvedené informace zdárně aplikovat do svých životů.

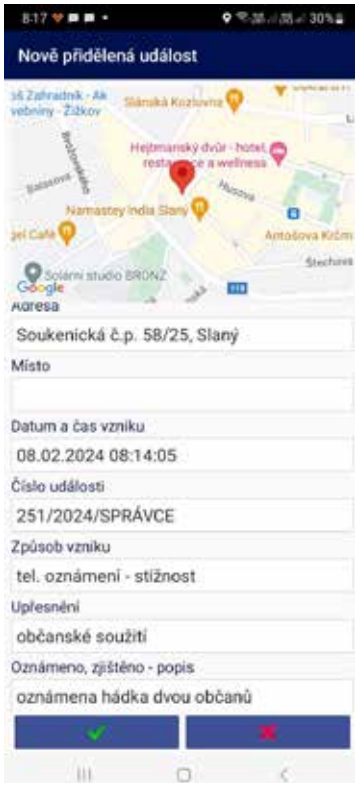
Mgr. Zoja Kalivodová, CSc.

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČESKÉ REPUBLIKY

ISMP VERA RADNICE

PROFESIONÁLNÍ INFORMAČNÍ SYSTÉM PRO MĚSTSKÉ POLICIE





Společnost VERA, spol. s r.o., působí na trhu od roku 1994 jako dodavatel komplexního informačního systému pro městské a obecní úřady. Součástí tohoto softwaru byla i agenda Městská policie. V průběhu let se zvyšoval počet přestupků (zejména dopravních) a výrazně vzrostly legislativní požadavky na strážníky, kteří musí zpracovávat, uchovávat a předávat stále více informací. I díky těmto potřebám se původní agenda rozvinula do rozsáhlého informačního systému, který splňuje nároky všech městských policií, od těch v malých obcích až po statutární města.

Informační systém městské policie VERA

Informační systém městské policie VERA se skládá z několika volitelných modulů: Přestupky a události, Velitel, Mobilní aplikace MP a Dispečink. Jeho nedílnou součástí jsou vazby na další agendy informačního systému města a integrace na software třetích stran. Samozřejmostí jsou statistiky, svodky, svodky v mapách a výkazy, včetně Výkazu činnosti MP pro Ministerstvo vnitra. Software komplexně zajišťuje přístup a ověřování ve všech registrech státní správy dle platné legislativy městské policie.

Vazby na informační systém města

V rámci vazeb je možné ISMP napojit zejména na příjmové agendy, pohledávky, evidence příkazových bloků a dalších cenin, skladové hospodářství města nebo lze využívat mapové vrstvy GIS (Geografický informační systém). Nedílnou součástí je plnohodnotná vazba na spisovou službu, a to jak VERA, tak na spisové služby třetích stran. Velkým usnadněním práce strážníků je automatizované předávání přestupků do správního řízení „jedním tlačítkem" nebo přímým zpracováním pokuty v mobilním platebním terminálu a následným automatickým zaúčtováním platby v ekonomických agendách. Samozřejmostí je i zjednodušené zpracování recidivních přestupků a jejich zápis do Registru přestupků – opět „jedním tlačítkem".

Propojujeme systémy

Bude-li řeč o integraci na software třetích stran, lze konstatovat, že integrací na různé aplikace a programy stále přibývá. Nejedná se jen o parkovací systémy (platby parkovného), ale disponujeme i automatickým odesíláním dat do Map kriminality, připojením na platební terminál GP Tom a připravujeme integraci na pult centralizované ochrany firmy NAM systém a Portál bezpečí.

Nejsme jenom dodavatel, jsme Váš partner

O zákazníky pečuje tým specialistů s dlouholetou praxí jak v přímém výkonu práce strážníků, tak i v jejich řízení a managementu městské policie. Se zákazníky jsme v denním kontaktu. Pečlivě naslouchámе požadavkům městských policií, nápadům strážníků, pořádáme pravidelné workshopy, kde vzniká mnoho podnětů k úpravám a novým funkcionalitám agendy. Tyto podněty analyzujeme, zapracováváme do aplikace a uvádíme je do praxe.

Generální partner mezinárodní konference městských policií

V roce 2023 se zúčastnil workshopu společnosti VERA v Chotěboři i ředitel Městské policie v Českém Těšíně Ing. Bc. Martin Látka, MBA. Setkání pana ředitele inspirovalo k uspořádání mezinárodní odborné konference, na jejímž zorganizování začal hned pracovat. VERA přijala roli generálního partnera konference a přispěje k jejímu průběhu mimo jiné i odbornými přednáškami, prezentacemi a workshopem. Jsme plně otevřeni diskusím i s účastníky, kteří nejsou našimi zákazníky. Věříme, že naše práce má smysl a pomáhá při udržování bezpečnosti v našich obcích a městech.

Pavel Štěpánek, DiS.
metodik
VERA, spol. s r.o.

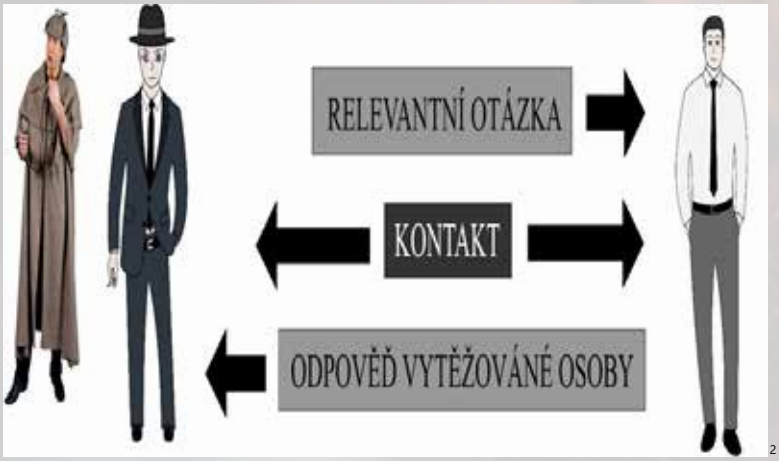
DETEKTIVNÍ OCHRANA SPORTOVNÍCH, KULTURNÍCH A SPOLEČENSKÝCH AKCÍ – OCHRANA MĚKKÝCH CÍLŮ

2. ČÁST

Detektivní činnosti zpravidla začínají vytěžením informací z tzv. otevřených zdrojů. To znamená získání informací z dostupných databází (velmi významnou je ANOPRES), z evidencí, registrací a archivů. Tím se realizují metody detektivního vyhodnocování databází a detektivní vyhodnocování dokumentů.

I u těchto metod, zejména při vyhledávání přístupu k databázím, kryjí detektiv nebo zpravodajec svou činnost vhodně zvolenou legendou. Otevřené zdroje je možno vytěžovat také pomocí speciálních softwarů.

DETEKTIVNÍ VYTĚŽOVÁNÍ [1]



2

Velmi významnou metodou při provádění detektivního průzkumu v souvislosti se sportovními, kulturními a společenskými akcemi je detektivní vytěžování. Tato metoda se podobně jako další neobejde bez správně zvolené legendy, která kryje skutečný záměr detektiva, zpravodajce. V podstatě se jedná o řízený rozhovor směřující k získání potřebných informací. Zpravidla velmi obtížná je fáze navázání kontaktu, kdy je třeba nejen správně zvolit legendu, ale důležitá je i otázka znalosti slangu, který členové zájmového prostředí používají. Důležitá je rovněž věková přiměřenost.

3

DETEKTIVNÍ POZOROVÁNÍ (SLEDOVÁNÍ)

a) *Statické* – připadá v úvahu v souvislosti s detektivním průzkumem před konáním nebo v průběhu konání sportovních, kulturních nebo společenských akcí. Je však třeba zdůraznit, že není o nic snadnější než dynamické pozorování (sledování). Cílem statického detektivního pozorování je získat informace o situaci v prostředí závadových skupin, u nichž je předpoklad narušování uvedených akcí.

b) *Dynamické* – připadá v úvahu zejména při realizaci metody detektivní kombinace nebo k získání informací o organizátorech narušujících předmětné akce, případně při realizaci formy činnosti detektivního rozkrývání latentních protiprávních jednání souvisejících se sportovními, kulturními nebo společenskými akcemi.

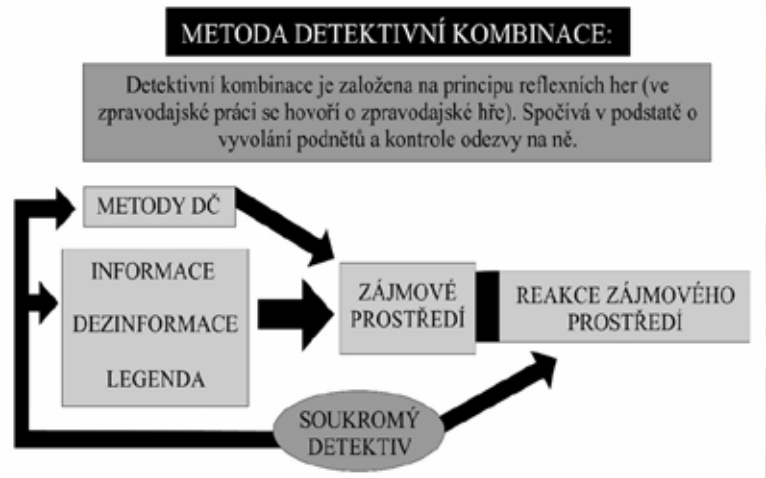
DETEKTIVNÍ KOMBINACE

Tato detektivní metoda již vyžaduje od detektiva jistý um a jisté praktické zkušenosti. Lze ji přirovnat k jakési zpravodajské hře (reflexní hře). Významnou roli v ní hraje detektivní legenda. Je použitelná v rámci detektivního – zpravodajského průzkumu v souvislosti se sportovní, kulturní nebo společenskou akcí. Jejím cílem je vyvolat pomocí některé z metod reakci zájmového prostředí a pomocí dalších metod zajistit sledování průběhu reakce (odezvy).

DETEKTIVNÍ INFORMAČNÍ ZDROJ – INFORMÁTOR [5]

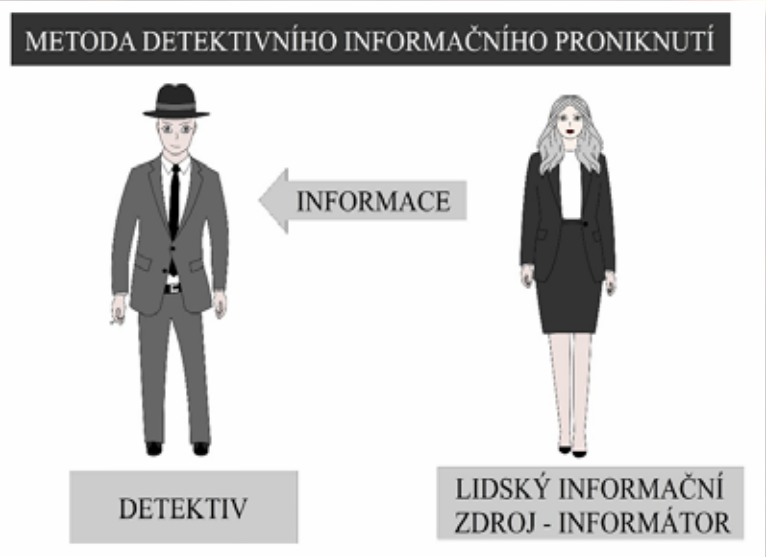
Lidské informační zdroje (informátoři) nebo technické informační zdroje představují v detektivním procesu významný prvek. Využití lidských informačních zdrojů (informátorů) vyžaduje

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI
ČESKÉ REPUBLIKY



4

zkušeného detektiva, neboť práce s těmito zdroji je odborně náročná.
V souvislosti s průzkumem v rámci zajišťování bezpečnosti sportovních, kulturních nebo společenských akcí je využití informátora možné v případě, že:
- v daném prostředí již informátora máme,
- máme informátora, kterého lze do zájmového prostředí nebo k zájmové osobě vhodně infiltrovat,



6

- jde o dlouhodobé nebo opakované akce.
V rámci soukromé detektivní činnosti se jeví jako pravděpodobné získání a využívání lidských informačních zdrojů (informátorů) na finanční bázi (SKPV má další možnosti).
Informátoři mohou být budováni jako:
- informační zdroje cílené – jedná se o informační zdroje získané a využívané ke konkrétní osobě a zpravidla ke konkrétnímu případu,
- informační zdroje poziční – jedná se o informační zdroje z určitého prostředí.

DETEKTIVNÍ DOKUMENTOVÁNÍ [7]

Průběh veškeré detektivní činnosti a prostřednictvím ní zjištěné informace, informace o důkazech a důkazy je třeba dokumentovat – to znamená zajistit je pro další zpracování v procesu detektivní, investigativní analýzy. Detektivní dokumentování prolíná všemi detektivními formami, metodami i využitím technických prostředků.
Je to metoda detektivní činnosti, jejímž cílem je informace získané detektivní činností legalizovat, zachovat, zpřístupnit (podávat ve srozumitelné podobě) a umožnit klientovi je využít pro jím plánované postupy v různých, i soudních kauzách. V procesu detektivního dokumentování využije soukromý detektiv řady kriminalistických taktických i technických metod a rovněž celé řady dalších obecných metod.

Druhy dokumentace:

a) <u>písemná dokumentace</u>
- pořízení fotokopií různých dokumentů,
- pořízení nových písemností, např. čestná prohlášení (s úředně ověřeným podpisem),
- znalecké posudky apod.
U písemností je vhodné, aby byly úředně ověřeny.

b) <u>fotodokumentace</u>
- událostí,
- jevů,
- kriminalistických stop,
- činnosti osob,
- archiválií apod.

Jedná se o dokumentování významných skutečností a jevů v podobě fotografií, ať jednotlivých, či zpracovaných do fotodokumentace (fotodokumentačních svazků). Pro další využití je třeba, aby k fotografiím či fotodokumentačním svazkům byla pořízena legenda obsahující zejména následující údaje:
- datum a čas pořízení,
- místo pořízení,
- vysvětlení, co fotografie zachycuje,
- kdo fotografii pořídil a proč.
U důležité fotodokumentace je vhodné uvést svědky události či jevu a svědky vlastního pořízení fotodokumentace. Je vhodné fotodokumentaci doplnit i čestnými prohlášeními svědků.

c) <u>audiodokumentace</u>
Jedná se o pořízení zvukových záznamů na audiomédia (magnetofonové pásky, CD, DVD nosiče). Z hlediska dalšího využití je vhodné obsah záznamu nebo alespoň jeho nejdůležitější pasáže pojistit i záznamem písemným, neboť je již v praxi ověřeno, že zejména nové nosiče jsou schopny uchovat záznam jen po dobu několika let, na rozdíl od magnetofonových pásků, které neztrácejí svou záznamovou hodnotu ani po 30 letech.

d) <u>video či filmová dokumentace</u>
Jedná se o dokumentování významných skutečností, především dějového charakteru, na filmová či video média. Zejména u detektivní dokumentace bez návaznosti na jiné formy detektivní činnosti může jít o zpracování různých filmových či video sestřihů významných událostí, skutečností. Rovněž v souvislosti s video či filmovou dokumentací se doporučuje zpracovat písemné legendy a písemné popisy natočených skutečností, událostí a dějů a doplnit je čestnými prohlášeními svědků událostí či dějů. Videozáznam je používán zejména tam, kde nejsou vhodné světelné podmínky pro fotodokumentaci. Je známo, že rozlišovací schopnost těchto záznamů je i vyšší.

e) <u>věcná dokumentace</u>
Jedná se o zajištění předmětů a stop (např. sádrových odlitků, daktyloskopických otisků apod.) pro potřeby dokazování v soudních kauzách či ve správních řízeních. Rovněž v těchto případech je vhodné doplnit tyto věcné důkazy a stopy čestnými prohlášeními svědků s úředně ověřenými podpisy.

8

To, co je u dokumentací pořizovaných orgány činnými v trestním řízení poměrně jednoduché a je dáno kriminalistickou metodikou a zásadami trestního řízení, vyžaduje u detektivního dokumentování značnou vynalézavost, aby bylo možno v procesních řízeních převést tyto dokumentace do podoby soudních důkazů.

DETEKTIVNÍ (INVESTIGATIVNÍ) ANALÝZA

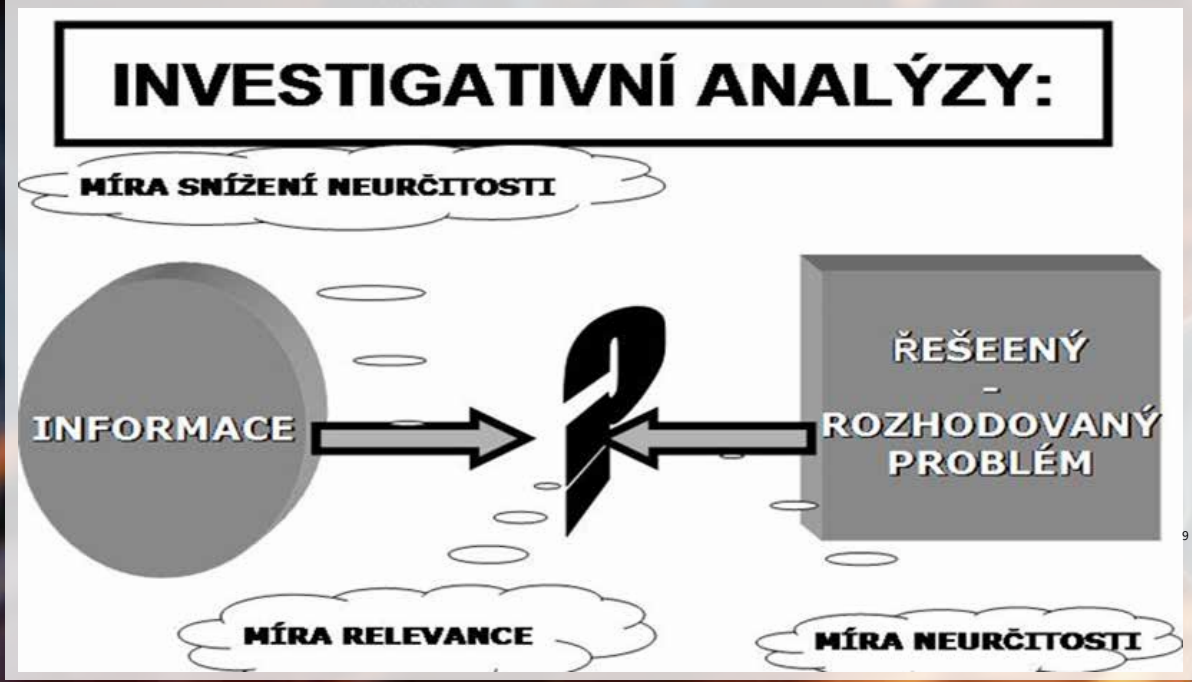
Stejně jako detektivní – zpravodajská legenda prolíná i detektivní analýza celým detektivním procesem. Je uplatňována při realizaci všech detektivních forem i metod. Detektivní (investigativní) analýza převádí míru neurčitosti na míru určitosti a zpracovává získané informace na relevantní.

Cílem investigativní analýzy je interpretace shromážděných informací v kontextu zadaných cílů detektivního průzkumu.

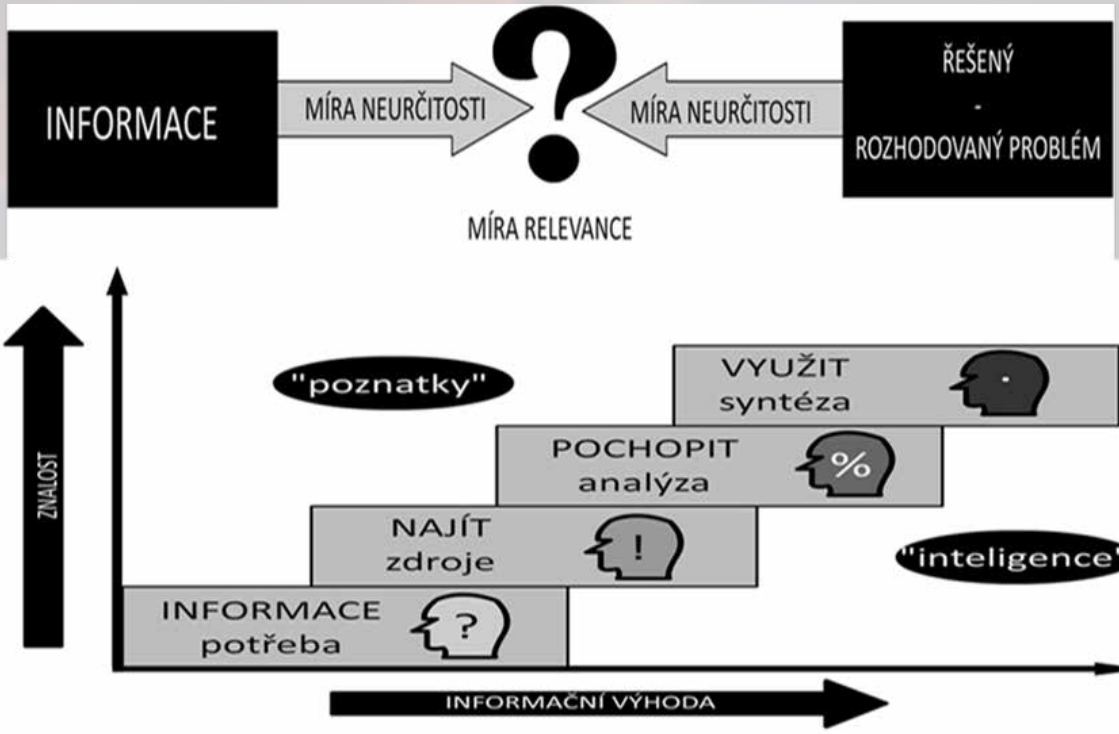
Základem analýzy je porozumění významu shromážděných informací (vytvoření mentálního modelu v mozku analytika). Interpretace informací spočívá v jejich intelektuálním zpracování (čtení), na jehož základě se extrahují důležité entity (lidé, organizace, věci, místa, události) a jejich vazby reprezentující smysl obsahu informací.

Detektivní (investigativní) analýzy lze rozdělit na:

a) vztahové – jsou metodou zobrazo-



9



10

vání velkého množství informací v organizované, jasné formě, s ohledem na vztahy mezi prvky, jako jsou osoby, organizace, dopravní prostředky, telefony, místa atd.; vztahové diagramy jsou formou zobrazení určité části zpravodajství nebo vyšetřovacích zpráv a jejich hlavním cílem je zobrazení vztahů v grafické formě;

b) komoditní – ilustrují toky zboží, peněz a dalších komodit, na základě nichž lze ukázat vztahy mezi subjekty a pochopit způsob provádění jejich aktivit (klíčové osoby);

c) kauzální – znázorňují souslednost událostí a mohou odhalit vztahy mezi nimi – účelem je zobrazit spletité a mnohdy velké množství dat jasným a stručným způsobem; tyto grafy mohou znázorňovat pouhou souslednost jevů nebo ji promítnout na časovou osu;

d) postupové – znázorňují průběh procesů, resp. pořadí událostí vedoucích k určitému výsledku nebo stavu, pokud musí být provedena jedna nebo více činností, než může nastat jiná aktivita.

Postup při analýze informací:

a) *porovnávání a třídění informací*

Pokud máme co do činění s objemem informací přesahujícím několik desítek záznamů, je pro jejich další rozbor naprosto nezbytné uložit je takovým způsobem, aby je bylo snadné prohledávat a třídit podle nejrůznějších (často předem neznámých) kritérií.

Jednotlivé shromážděné informace je proto vhodné převést do elektronické podoby a uložit do nějaké fulltextové, případně relační databáze. Tento krok připravuje shromážděné informace pro následnou analýzu a distribuci tak, aby bylo možné:

- cokoli vyhledat podle čehokoli,
- nalézat společný kontext různých informací,
- zjišťovat různé kontexty jednotlivých faktů,
- třídit informace podle společných atributů,
- vytvářet dokumentaci k jednotlivým zadáním.

b) *vlastní analýza*

Kvalitativně odlišuje detektivní prověrku od prostého monitoringu (sledování) informací. U monitoringu dochází k pouhé selektivní distribuci shromážděných informací koncovým uživatelům, zatímco v případě detektivní prověrky dostává koncový uživatel (klient) interpretovaný význam shromážděných informací až soukromým detektivem – analytikem.

Analýza je kreativní intelektuální proces, kdy se informace přeměňují ve znalosti potřebné pro konkrétní rozhodnutí.

JUDr. František BRABEC
čestný prezident ČKDS
výkonný ředitel ČS ESBOC

Poznámky pod čarou:

1/ Srov. KAMENÍK, Jiří; BRABEC, František a kol. KOMERČNÍ BEZPEČNOST 2, Praha 2019, vydavatel Wolters Kluwer ČR, ISBN 978-80-7598-303-9, str. 279–282. & Srov. BRABEC František a kol. SOUKROMÉ DETEKTIVNÍ SLUŽBY, Praha 1995, Eurounion, ISBN 80-85858-16-8, str. 170–179.
2/ BRABEC, František. DETEKTIVNÍ – ZPRAVODAJSKÉ VYTĚŽOVÁNÍ, PRAHA 2023, složeno z komponentů grafiky ZAPLETAL, Karel a internetu.
3/ BRABEC, František. METODA DETEKTIVNÍ POZOROVÁNÍ, Praha 2001.
4/ BRABEC, František. DETEKTIVNÍ – ZPRAVODAJSKÁ KOMBINACE, Praha 2001, nové grafické vyjádření, ZAPLETAL, Karel, 2021.
5/ Srov. KAMENÍK, Jiří; BRABEC, František a kol. KOMERČNÍ BEZPEČNOST 2, Praha 2019, vydavatel Wolters Kluwer ČR, ISBN 978-80-7598-303-9, str. 280–284. & Srov. BRABEC, František a kol. SOUKROMÉ DETEKTIVNÍ SLUŽBY, Praha 1995, Eurounion, ISBN 80-85858-16-8, str. 158–159.
6/ BRABEC, František. GRAFICKÉ VYJÁDŘENÍ METODY DETEKTIVNÍ INFORMAČNÍ PRONIKNUTÍ, Praha 2001, úprava 2023, nová grafická úprava, ZAPLETAL, Karel, 2021.
7/ Srov. KAMENÍK, Jiří; BRABEC, František a kol. KOMERČNÍ BEZPEČNOST 2, Praha 2019, vydavatel Wolters Kluwer ČR, ISBN 978-80-7598-303-9, str. 299–302; & Srov. BRABEC, František a kol. SOUKROMÉ DETEKTIVNÍ SLUŽBY, Praha 1995, Eurounion, ISBN 80-85858-16-8, str. 146–147.
8/ BRABEC, František. METODY DETEKTIVNÍ DOKUMENTOVÁNÍ, Praha 2020, grafické vyjádření.
9/ BRABEC, František, Praha.
10/ BRABEC, František. DETEKTIVNÍ ANALÝZA, Praha 2023, obrázek je složen z komponentů převzatých z grafiky ZAPLETAL, Karel a grafiky VEJLUPEK, Tomáš.

KAMEROVÝ SYSTÉM V AME

ANEB CO JE POTŘEBA SPLNIT

Kamerový systém ve zdravotnictví, a to i v ambulantní sféře, musí splňovat požadavky obecného nařízení o ochraně osobních údajů (GDPR). I kamery v čekárně ordinace praktického lékaře musí splňovat legislativní požadavky.

Dozorový orgán Úřad pro ochranu osobních údajů vypracoval „Metodiku k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů", která je k dispozici na webových stránkách: www.uoou.cz.

Kamerový systém zasahuje také do pracovního práva, kde jsou dozorovým orgánem oblastní inspektoráty práce Státního úřadu inspekce práce (dodržení ustanovení § 316 zákoníku práce).

Účely zpracování

Přestože pojem kamerový systém je v podstatě pouze jeden, existuje celá řada právních účelů zpracování osobních údajů dle GDPR. Za primární kamerový systém lze považovat ten, který představuje použití pro bezpečnostní účely. Dalším účelem zpracování osobních údajů ve zdravotnictví je co do významu neméně důležitý kamerový systém pro zdravotnické účely.

Kamerové systémy pro bezpečnostní účely rozlišujeme zejména:

a) k ochraně osob a majetku (prevence kriminality, prevence před požárem, ochrana zdraví a života osob, ochrana osobních údajů a další),
b) k zajištění plynulosti na vjezdu/výjezdu do zdravotnického zařízení.

Kamerové systémy nebo jednotlivé kamery pro zdravotnické účely

dělíme podle charakteru poskytované zdravotnické péče zejména na:
a) kamery ze zdravotnických přístrojů (prostředků),

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI
ČESKÉ REPUBLIKY

BULANTNÍ SFÉŘE DLE GDPR

b) výukové kamery (pro edukativní účely) – např. v operačních sálech,
c) dohledové kamery (slouží k zajištění ochrany života a zdraví pacienta nebo personálu v ohrožující situaci).

Právní tituly zpracování osobních údajů

Právní titul je zákonnou podmínkou zpracování osobních údajů dle GDPR. Ke zpracování může dojít pouze v odpovídajícím rozsahu.

Zpracování osobních údajů kamerovým systémem je ve většině případů **oprávněným zájmem správce** nebo třetí strany (čl. 6 odst. písm. f) GDPR). K takovému zpracování osobních údajů není třeba souhlasu zaměstnanců zdravotnického zařízení ani pacientů, protože se jedná o jiný právní titul než souhlas.

Nejde tedy o jediný možný právní titul zpracování osobních údajů kamerovým systémem. Teoreticky je možné např. i zpracování založené na souhlasu subjektu údajů (čl. 6 odst. 1 písm. a) GDPR), ale vzhledem k tomu, že takový souhlas může být kdykoli odvolán, je tento právní titul přinejmenším nepraktický. Navíc subjekt údajů musí být poučen o právu tento souhlas kdykoli odvolat a o svých dalších právech dle GDPR, včetně práva podat stížnost k dozorovému orgánu. Dále je povinností správce tento souhlas doložit dozorovému orgánu. Problematické zde je i dodržení recitálu 32 GDPR: *„Souhlas by měl být dán jednoznačným potvrzením, které je vyjádřením svobodného, konkrétního, informovaného a jednoznačného svolení subjektu údajů ke zpracování osobních údajů."* Souhlas by měl být udělen vždy ke konkrétnímu účelu. *„Jestliže má zpracování několik účelů, měl by být souhlas udělen pro všechny,"* uvádí zmíněný recitál. Souhlas se zpracováním osobních údajů dle GDPR nelze zaměňovat s informovaným souhlasem s poskytnutím zdravotní služby dle zákona o zdravotních službách. [1]

Nákup a servis kamerového systému – dodavatelské vztahy

Pro zpracování osobních údajů kamerovým systémem je u dodavatelů podstatné především to, jakým způsobem jsou zpřístupněny kamerové záběry a zda vůbec. Jde zejména o stálé zpřístupnění online záběrů *(pozn.: např. soukromé bezpečnostní službě)* nebo nepravidelné zpřístupnění pomocí vzdáleného přístupu, tzv. VPN *(pozn.: např. servisní firmě, zpravidla dodavateli, z důvodu zajištění servisních služeb dle smlouvy)*.
Vždy se musí jednat o smluvní vztah s písemným ujednáním dle **čl. 28 GDPR.** Tato opatření musí být uvedena např. už v kupní smlouvě, servisní smlouvě nebo pak v samostatné zpracovatelské smlouvě. Obsahem opatření k ochraně osobních údajů musí být především závazek mlčenlivosti a stanovení povinností a postupu zpracovatele při porušení zabezpečení osobních údajů atd. Mezi povinnosti zpracovatele patří vedení záznamů o všech kategoriích činností zpracování prováděných pro správce (čl. 30 odst. 2 GDPR). *Pozn.: za podmínek uvedených v čl. 30 odst. 5 GDPR.*

Vnitřní předpis ke kamerovému systému

Důležitým dokumentem je vnitřní předpis ke kamerovému systému. Zaměstnanec musí být s vnitřním předpisem řádně seznámen a je jeho povinností vnitřní předpis dodržovat.[2] Účelem vnitřního předpisu je především ochrana práv zaměstnavatele vůči možným následkům a sankcím[3] při jeho porušení zaměstnancem (např. osobní selhání jedince).

Vnitřní předpis k ochraně osobních údajů by měl obsahovat přinejmenším tato ustanovení:

- zásady zpracování osobních údajů,
- seznam a popis přijatých technických a organizačních opatření,
- způsob zabezpečení komunikace a nakládání s daty,
- ochrana osobních údajů kamerového systému,
- zajištění vztahů s dodavateli – zpracovateli osobních údajů,
- způsob poskytování informací o zpracování osobních údajů,
- způsob uplatnění práv dle GDPR,
- úkoly a postavení pověřence (byl-li jmenován).

Provozní kniha kamerového systému

Provozní kniha *(pozn.: případně deník)* představuje dokumentaci pro předávání kamerových záznamů oprávněným subjektům:

a) Subjekty, které žádají správce o poskytnutí záznamu z kamerového systému, by měly správci zaslat žádost obsahující specifikaci rozsahu požadovaného záznamu, zdůvodnění žádosti a v případě subjektů, kterým je správce povinen předat záznamy z kamerového systému na základě zákona, také termín pro poskytnutí záznamu.

b) Správce může poskytnout kamerové záznamy orgánům činným v trestním řízení nebo správním orgánům pro vedení přestupkového řízení, případně pojišťovnám, i z vlastního rozhodnutí, a to v případě, že má podezření na

spáchání trestného činu nebo přestupku nebo vzniku pojistné události, které jsou na záznamu zachyceny.

c) Pro vyřizování žádostí o poskytnutí záznamů z kamerových systémů, i pro poskytnutí kamerových záznamů z vlastního rozhodnutí správce, vytvoří správce postupy, které stanoví a budou obsahovat:
- kontaktní osoby správce pro předávání žádostí o poskytnutí dat,
- posouzení oprávněnosti předání dat,
- postup pro zpracování kopie záznamu, včetně stanovení osoby, která zajistí zpracování kopie,
- určení osoby správce, která zajistí předání kopie kamerového záznamu žadateli nebo orgánům činným v trestním řízení nebo správním orgánům pro účely přestupkového řízení,
- pokyny pro zpracování dokumentu o předání kopie kamerového záznamu, které zohlední následující doporučení:

- protokol o předání kamerových záznamů, připravený orgány činnými v trestním řízení nebo správními orgány pro účely přestupkového řízení, lze použít bez nutnosti zpracování dalších dokumentů,
- pokud dokument o předání zajišťuje přímo správce, doporučuje se zpracovat předávací protokol nebo záznam v rámci vedení provozního deníku, který bude obsahovat:

- datum poskytnutí záznamu,
- zdůvodnění poskytnutí záznamu (zejména právní důvod[4]):

- v případě žádosti policie může jít o právní důvod plnění právní povinnosti[5]
- v případě pojistné události nebo podezření správce na trestný čin nebo přestupek, kdy dochází k předání záznamu příslušným orgánům či pojišťovně na základě podezření správce či vzniklé škody, jde o předání na základě ochrany oprávněných zájmů správce, u třetích osob rovněž na základě prokázaných oprávněných zájmů těchto osob[6]
- v ostatních případech, jako je přístup (např. individuální), šíření (on-line) nebo jakékoli jiné zpřístupnění kamerových záznamů jiným subjektům, jde o předání na základě souhlasu subjektu údajů[7]

- identifikaci žadatele o záznam (v případě žádosti oprávněných orgánů včetně čísla jednacího příslušného řízení nebo jiné specifikace příslušného řízení) nebo subjektu, kterému je záznam předáván z vlastního podnětu,
- specifikaci poskytnutých záznamů (datum pořízeného záznamu, uvedení času odkdy – dokdy),
- jméno a příjmení předávající osoby, včetně jejího podpisu,
- jméno a příjmení přejímající osoby, včetně jejího podpisu.

d) Pro účely poskytnutí záznamů z kamerového systému se za rozhodný den považuje den obdržení žádosti; jako přiměřená doba pro poskytnutí záznamu se považuje lhůta do jednoho měsíce od obdržení žádosti nebo je třeba respektovat termíny určené orgány činnými v trestním řízení.[8]

Pravidla provozování kamerového systému

- Zpracování osobních údajů provozováním kamerového systému je zákonné, pouze pokud je prováděno v odpovídajícím rozsahu v rámci některého z přípustných právních titulů zpracování osobních údajů (zpravidla oprávněný zájem).
- Kamerovým systémem nelze soustavně sledovat zaměstnance nebo je tímto způsobem kontrolovat při plnění pracovních úkolů (provoz kamer a využití záznamu musí být v souladu s pracovněprávními předpisy, zejména § 316 zákoníku práce).
- Je vyloučeno užití kamerového systému v prostorách určených k ryze soukromým úkonům (např. toalety, sprchy). Pro sledování je třeba vymezit určitý prostor daný účelem zpracování.
- Kamerový systém je možno použít zásadně v případě, kdy sledovaného účelu nelze účinně dosáhnout jinou cestou (např. lepším zabezpečením majetku).
- Je třeba předem jednoznačně stanovit účel pořizování záznamů, který musí korespondovat s důležitými, právem chráněnými zájmy správce (např. ochranou majetku před krádeží). Záznamy tak mohou být využity pouze v souvislosti se zjištěním události, která poškozuje tyto důležité, právem chráněné zájmy správce. Přípustnost využití záznamů pro jiný účel musí být omezena na významný veřejný zájem, např. potírání další kriminality.
- Je nezbytné stanovit lhůtu pro uchovávání záznamů. Doba uchovávání dat by neměla přesáhnout časový limit maximálně přípustný pro naplnění účelu provozování kamerového systému. Metodika ÚOOÚ doporučuje **základní lhůtu 72 h**[9] s tím, že delší lhůta musí být řádně zdůvodněna (nezbytnost delšího uchování).
- Je nutné řádně zajistit ochranu snímacích zařízení, přenosových cest a datových nosičů, na nichž jsou uloženy záznamy, před neoprávněným nebo nahodilým přístupem, změnou, zničením či ztrátou nebo jiným neoprávněným zpracováním. Záběry z kamer se musí zabezpečit proti přístupu neoprávněných osob (vhodná instalace monitorů apod.).
- Dokumentují se a řeší veškeré případy porušení zabezpečení osobních údajů.
- Subjekt údajů musí být o užití kamerového systému vhodným způsobem informován (cedule, samolepka, webové stránky apod.) a musí mu být umožněn výkon dalších práv dle GDPR.

Školení zaměstnanců z ochrany osobních údajů

Školení z ochrany osobních údajů (včetně zpracování kamerovým systémem) představuje splnění základní povinnosti správce přijmout vhodné organizační opatření.

V ambulantní sféře lze postupovat dle Metodického pokynu Ministerstva zdravotnictví ČR, kde se uvádí potřeba mít zdokladováno, že osoby, které mají přístup k osobním údajům a pracují s nimi, byly řádně poučeny – co dělat mají a co nesmí. Ideální je nechat toto poučení danými pracovníky podepsat – zejména tam, kde je takových osob více a může hrozit selhání lidského faktoru. Školení v ambulantní sféře se doporučuje provádět alespoň jednou ročně nebo dle potřeby v případě změn (např. při nástupu nového zaměstnance, při změně dodavatele, při změnách legislativy apod.). [10]

Mgr. Bc. Milan Bláha
lektor FES ÚSII Univerzity Pardubice

MUDr. Bohumil Skála, Ph.D., LL.M

Poznámky pod čarou:

1/ § 28 odst. 1, zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), v platném znění

2/ § 106 odst. 4 písm. c) zákona č. 262/2006 Sb., zákoník práce, v platném znění

3/ HLAVA VI, Přestupky, § 61 až § 64, zákon č. 110/2019 Sb., o zpracování osobních údajů, v platném znění

4/ kapitola 4, Pokyny EDPB 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky ze dne 29. ledna 2020

5/ čl. 6 odst. 1 písm. c) GDPR

6/ čl. 6 odst. 1 písm. f) GDPR

7/ čl. 6 odst. 1 písm. a) GDPR

8/ METODIKA K NÁVRHU A PROVOZOVÁNÍ KAMEROVÝCH SYSTÉMŮ Z HLEDISKA ZPRACOVÁNÍ A OCHRANY OSOBNÍCH ÚDAJŮ (Úřad pro ochranu osobních údajů, 2024, str. 18 - 19)

9/ METODIKA K NÁVRHU A PROVOZOVÁNÍ KAMEROVÝCH SYSTÉMŮ... (ÚOOÚ, 2024, str. 11)

10/ Metodický pokyn Ministerstva zdravotnictví ČR „Jak implementovat v ambulantní sféře NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) do rezortu zdravotnictví (na co si dát pozor v ambulantní sféře)," ze dne 31. března 2018, čl. 3.5, 3.10 a 6.11

MEZINÁRODNÍ KONFERENCE OBECNÍCH POLICIÍ V ČESKÉM TĚŠÍNĚ

Přijměte pozvání na Mezinárodní konferenci městských policií, která se uskuteční ve dnech 23.–25. října 2024 v Kulturním a společenském středisku Střelnice v Českém Těšíně. Budou tu probírány radosti i strasti profesionální práce strážníků obecních policií v Evropě, dojde tu k výměně zkušeností, jejímž hlavním cílem bude přispět ke zkvalitnění práce městských policií nejen v ČR. A co konkrétního se o konferenci dozvěděla od jejích organizátorů redakce našeho časopisu?

Proč se bude konat Mezinárodní konference městských policií právě v Českém Těšíně?

Otcem myšlenky se stal Ing. Bc. Martin Látka, MBA, ředitel místní městské policie a člověk s řadou zkušeností v oboru bezpečnostní problematiky. V minulosti byl důstojníkem AČR, studoval na vojenského pilota, byl účastníkem čtyř zahraničních misí UNPROFOR (United Nations Mission in Kosovo – mírové mise OSN na území zemí bývalé Jugoslávie v letech 1992–1995), velel výsadkové rádiové četě u 4. brigády rychlého nasazení, kde pracoval i jako instruktor pro boj zblízka MUSADO (moderní způsob sebeobranného boje, který kombinuje techniky starých korejských bojových umění – volně přeloženo „Cesta válečníka“). Dále pracoval jako instruktor a inspektor ŘLP (řízení letového provozu) a jako vedoucí směny ŘLP u 21. základny vojenského letectva v Čáslavi. Kariéru ukončil s diplomatickým pasem jako styčný důstojník dvou mezinárodních misí UNMIK (United Nations Mission in Kosovo) na území Kosova a FYROM (Former Yugoslav Republic of Macedonia) na území bývalé jugoslávské republiky Makedonie. Vystudoval ekonomii a poté pracoval na vedoucích pozicích v různých soukromých společnostech v ČR i v zahraničí, měl na starosti především vedení společností, obchodních týmů, zahraniční obchod a finance. Je ženatý, miluje svou rodinu a má rád nové výzvy. Proto začal ihned po uvedení do funkce ředitele MP v Českém Těšíně pracovat na zkvalitnění činnosti zdejšího útvaru a ruku v ruce s tím na zviditelnění a propagaci města.

Kdy vlastně myšlenka uspořádání konference v Českém Těšíně vznikla?

Myšlenka uspořádání konference se zrodila právě v hlavě nového ředitele Městské policie v Českém Těšíně – Ing. Bc. Martina Látky – na sklonku loňského roku. V prosinci 2023 začal jednat s ředitelem Odboru prevence kriminality MV ČR JUDr. Michalem Barboříkem o možnosti uspořádat mezinárodní konferenci obecních policií také ve Slezsku a Český Těšín, který leží na hranici s Polskem a nedaleko hranic slovenských, doporučil jako ideální místo pro její konání. Když dostal „zelenou“, okamžitě začal pracovat na její přípravě.

Co je cílem této konference?

Především nabídnout účastníkům odborný, profesionální, ale i kulturní zážitek, který prohloubí jejich profesní znalosti, rozšíří obzor v oblasti využití moderních technologií, poskytne příležitost pro vznik nových přátelství a pro rozšíření užitečných kontaktů, jež mohou být nápomocny při zdolávání složité a namáhavé každodenní práce obecních strážníků.

A co na tuto zajímavou aktivitu říká starosta Českého Těšína Karel Kula?

Starosta města, který má městskou policii ve své gesci, myšlenku uspořádání konference tak velkého významu s radostí uvítal a je jí od počátku nakloněn. Vnímá ji jako cestu k pozitivnímu zviditelnění města v mezinárodním měřítku a příležitost k pozvednutí prestiže nejen města samotného, ale i zdejší městské policie. Za podporu při organizování konference mu patří velký dík, stejně jako celému vedení města, odborům MěÚ, které se do přípravy akce zapojily, vedení a zaměstnancům Kulturního a společenského střediska Střelnice a v neposlední řadě celému realizačnímu týmu Městské policie v Českém Těšíně.

Jaká témata budou na konferenci diskutována?

Oficiální výčet témat podzimní Mezinárodní konference městských policií v Českém Těšíně je následující:

- NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost) – školení NIS2 (o směrnici k zajištění vysoké společné úrovně kybernetické bezpečnosti)
- Umělá inteligence, bezpečnost
- Praktické využívání kamerových systémů pro bezpečnost ve městě
- GDPR (General Data Protection Regulation – Obecné nařízení o ochraně osobních údajů)
- Kyberbezpečnost
- Problematika uprchlíků v centrální Evropě
- Moderní řízení městské policie – dispečink
- PCO (Pult centrální ochrany), informace přes dispečink – krizové řízení

Ovšem kuloárně bude možno diskutovat i o mnoha dalších problémech, které obecní a městské policie tíží.

Proč vznikla potřeba uspořádat konferenci právě s takovým zaměřením?

Obecní policie za více než 30 let své existence prošly velikou obměnou svých povinností a pravomocí. Proble-

matika jejich činnosti se liší – jednak se odvíjí od velikosti obcí či měst a jednak od jejich lokalizace, tedy zda leží ve vnitrozemí, či zda se nacházejí přímo na státní hranici.
Strážníci jsou přímo závislí na úkolech daných obcím, které jsou povinny ze zákona zajistit pro své občany bezpečný život. Zároveň jsou závislí na možnostech přístupů do různých registrů, jež musejí ze zákona procházet při každodenní práci s přestupky občanů ČR, ale i cizinců.

Proč se generálním partnerem konference stala společnost VERA, spol. s r.o.?

Jak vyplývá z výše uvedeného, je pro práci strážníků městských policií nezbytné mít možnost využívat k podpoře vlastní práce aplikací a systémů, jež jim náročnou činnost usnadňují. A tuto možnost nabízí mimo jiné právě společnost VERA. Koneckonců si tuto společnost a její aplikační systémy vybrala pro zkvalitnění své práce Městská policie Český Těšín už v 90. letech minulého století, jako první z obecních policií u nás. Dnes již aplikace této společnosti využívají ke své každodenní práci nejen obecní policie, ale i odbory obecních a městských úřadů. Proto bylo rozhodnutí ředitele Ing. Bc. Martina Látky celkem jednoznačné – oslovil v první řadě právě společnost VERA, aby se stala generálním partnerem těšínské mezinárodní konference, a ta po vzájemném jednání nabídku přijala.

Čím je činnost městských a obecních policií v České republice nejčastěji determinována?

Dílčí charakteristiku územně příslušné obecní policie vytvářejí typické a nejčastěji vykonávané preventivní služební činnosti. Do obecného povědomí vstupují nejvíce frekventované úkony a zákroky strážníků, jejichž činnost je v zásadě ovlivněna následujícími faktory:
• zda jde o policii obecní či městskou,
• zda jde o sbor s vysokým či nízkým počtem strážníků,
• jaká je rozloha obce či města a dosažitelnost místních částí,
• jaký je počet obyvatel,
• jaká je sociální struktura obyvatelstva,
• jaký je nápad trestné činnosti.

Velice důležitou roli hraje též délka doby, po kterou sbor v obci/městě působí, i délka praxe jednotlivých strážníků, jelikož faktor času a délka praxe má nesporný vliv na úroveň zkušeností a erudici strážníků. Jednotlivé obecní policie se od sebe mohou odlišovat i formami a způsoby výkonu služby, jež jsou odvislé od jejich materiálně technického vybavení. Zde mnohdy nejde ani tak o optimální potřeby vycházející z místních podmínek a stavu veřejného pořádku, jako o výši finančních zdrojů, které bývají pro rozsah služeb poskytovaných konkrétní obecní policií limitujícím faktorem.

Je třeba přitom mít na paměti, že plnění úkolů v oblasti vnitřního pořádku a bezpečnosti spadá především do kompetence Policie ČR. Jedná se o plnění úkolů, které jsou vlastní každému demokratickému státu. Jejich zajišťováním jsou vytvářeny podmínky pro běžnou činnost a fungování všech složek, orgánů, organizací a institucí státu, jakož i pro každodenní život občanské společnosti.

Nicméně Policie ČR není jediným subjektem zodpovědným za ochranu společenských vztahů v uvedené oblasti. Historicky přibyla řada dalších subjektů, které se spolupodílejí na ochraně života a zdraví občanů, majetku, veřejného pořádku a dalších zájmů a hodnot společnosti i jedince. Toto znásobení počtu subjektů k zabezpečení bezproblémového života občanů si vyžádala složitost a náročnost úkolů, které je nutno pro klidný a bezporuchový chod společnosti (obce/města) zajišťovat.

Zvláště v posledních letech lze pozorovat trend vytváření místních policejních orgánů, které se blíže přimykají k potřebám plnění úkolů jednotlivých obcí a měst. Posláním místních policejních orgánů je v řadě případů plnění stejných či obdobných úkolů, které ze zákona přísluší Policii ČR. Nejde však přitom v žádném případě o nahrazování činnosti Policie ČR. Místní policejní orgány, ale i soukromé bezpečnostní služby a jiné subjekty, vyvíjející bezpečnostní činnost na komerčním základě, při plnění uvedených úkolů spolupůsobí a činnost Policie ČR doplňují. To samozřejmě neznamená nadřazování Policie ČR ve vztahu ke kterémukoli z uvedených subjektů. Jedná se pouze o věcné kompetence a vzájemné rozdělení pravomocí na místní úrovni.

Jaké problémy v současnosti obecní/městské policie nejvíce trápí?

Obecní policie se v praxi osvědčily a vybudovaly si své nezastupitelné místo v soustavě orgánů ochrany veřejného pořádku. Proto Policie ČR upouští od výkonu některých úseků ochrany veřejného pořádku a dominantní aktivitu zde jim přenechává. Zejména ve statutárních městech však praxe ukázala nedostatečnost stávající právní úpravy. Práci strážníků obecní policie komplikuje buď úplná absence řešení některých důležitých problémů, nebo celá řada nejasností ve znění konkrétních ustanovení zákona o obecní policii, které otvírají cestu k mnohým, nezřídka chybným výkladům. Dále je velikým problémem skutečnost, že obecní policie doposud nefigurují v seznamu Integrovaného záchranného systému (IZS), byť legislativci ji nyní rozhodli přiřadit alespoň k tzv. ostatním složkám IZS.

Hojně diskutovaná je dnes také otázka výsluh strážníků, kteří bojují za jejich zakotvení v zákonech ČR, jak je tomu již například na Slovensku. Aktuálně o to usilují za všechny strážníky především Svaz obecních a městských policií České republiky z. s. a Kolegium ředitelů MP statutárních měst a hl. m. Prahy.

Problémů, které strážníky trápí, včetně stále více palčivých otázek týkajících se bezdomovectví, je skutečně mnoho. Pojďme je tedy diskutovat a zkusit řešit na těšínské konferenci ve dnech 23.–25. října 2024.

Mgr. Bc. Kateřina Poludová, DiS.
tajemnice KPKB ČR
šéfredaktorka časopisu
Bezpečnost s profesionály


Karel Kula


Martin Látka

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČESKÉ REPUBLIKY

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

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

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

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

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

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

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 Zdiby
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.
Jeřábová 419
250 73 Radonice
www.solidita.cz

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

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

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

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

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

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

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

Ing. Martin Neuschl
Šachetní 391
261 01 Příbram