



KPKB
KOMORA
PODNIKŮ
KOMERČNÍ
BEZPEČNOSTI
ČESKÉ REPUBLIKY

ČASOPIS KOMORY PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČR

DUBEN AŽ SRPEN/2025

BEZPEČNOST

S PROFESIONÁLY

MĚKKÉ CÍLE POD DROBNOHLEDEM

JAK TRÉNINK ZVYŠUJE NAŠI BEZPEČNOST

OCHRANA PROTI KINETICKÝM ÚTOKŮM

VOZIDLO UŽ NENÍ JEN DOPRAVNÍ PROSTŘEDEK

ZÁVAŽNÉ INCIDENTY

POD ŠIRÝM NEBEM A MOŽNOST PREVENCE

GUANLAN AI

NEJNOVĚJŠÍ TECHNOLOGIE PRO OCHRANU MĚKKÝCH CÍLŮ

PROSTOROVÝ ODPOSLECH

HISTORIE, SOUČASNOST A POUŽÍVÁNÍ SYSTÉMŮ

ISSN 2336-4793



9 772336 479003

WWW.KPKBCR.CZ



KPKB
KOMORA
PODNIKŮ
KOMERČNÍ
BEZPEČNOSTI
ČESKÉ REPUBLIKY

BEZPEČNOST

S PROFESIONÁLY

Šéfredaktor

Mgr. Bc. Kateřina Poludová, DiS.

Jazyková spolupráce

PhDr. Alena Hasáková

Redakční rada

Ing. Václav Jahodář

Mgr. Bc. Kateřina Poludová, DiS.

Ivo Kolář

PhDr. Barbora Vegrichová, Ph.D., MBA

Inzerce

sekretariat@kpkbcr.cz

Nesignované fotografie a články

Redakce

Vydavatel

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

Registrace

Bezpečnost s profesionály

MK ČR E 20140

ISSN 2336-4793

Tisk

Bittisk s r. o.

B. Němcové 53, 746 01 Opava

Rozšiřování zdarma

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

Na zadní straně obálky

členové KPKB ČR



ÚVODNÍ SLOVO

Vážení čtenáři,

ani uprostřed léta jsme nezaháleli a díky tomu máte před sebou další letošní číslo časopisu Bezpečnost s profesionály.

Naše Komora byla v letošním roce již po deváté spoluorganizátorem konference Ochrana měkkých cílů, která se uskutečnila 12. června 2025 v Konferenčním centru CITY v pražských Nuslích. Konference se již tradičně těší velkému zájmu odborné veřejnosti – letos se jí účastnilo na 260 registrovaných osob – a stala se významnou a osvědčenou platformou k získávání informací o novinkách a trendech v oblasti bezpečnosti. Tentokrát byla hlavním tématem ochrana veřejných prostranství. Zájem účastníků je pro nás závazkem a výzvou k pokračování tradice, proto se již nyní těšíme na jubilejní desátý ročník této konference, který plánujeme realizovat v roce 2026 opět v červnu.

Na stránkách tohoto čísla se můžete jako obvykle seznámit s řadou aktuálních informací a také s články našich odborných dopisovatelů na různá zajímavá témata – věříme, že si každý z Vás přijde na své.

Na podzim letošního roku nás čekají parlamentní volby. Nevíme sice zatím, jak dopadnou, ale máme naději, že otázky bezpečnosti v našem státě zůstanou i pro novou vládu prioritou a dočkáme se od ní aktivnějšího přístupu k řešení zákona o bezpečnostních činnostech.

Přeji vám poklidný zbytek léta a těším se na setkání u dalšího čísla našeho časopisu.

Ing. Václav Jahodář
prezident KPKB ČR

OBSAH

Tisková zpráva 3
ke konferenci OMC

Měkké cíle pod drobnohledem 4-5
jak trénink zvyšuje naši bezpečnost

Ochrana proti kinet. útokům 6-8
vozidlo už není jen dopravní prostředek

Závažné incidenty 10-13
pod širým nebem a možnost prevence

Inteligentní kamery 14-15
s detekcí zvuků

Dohledové centrum 16-17
na co se zaměřit při výběru

Guanlan AI 18-19
nejnovější technologie pro ochranu měkkých cílů

SŘBI 20-21
systém řízení bezpečnosti

Doporučení Úřadu 22-24
pro ochranu osobních údajů

Prostorový odposlech 25-27
historie, současnost a používání systémů

Nové motocykly 28-29
u pohotovostní motorizované jednotky

Dopady pandemie Covid 19 30-32
společenská odpovědnost a etické koncepce

Srdce Děkova 33
podpora spolku

Pozvánka 34
na mezinárodní konferenci obecních policí

TISKOVÁ ZPRÁVA KE KONFERENCI OCHRANA MĚKKÝCH CÍLŮ 2025

V Praze dne 23. června 2025

Vážení kolegové,

dne 12. června 2025 se uskutečnil již 9. ročník odborné konference „Ochrana měkkých cílů 2025“, který pořádala Komora podniků komerční bezpečnosti České republiky, z.s. společně s asociací kyberbezpečnosti AFCEA - českou pobočku za podpory Univerzity obrany, ČVUT - Fakultou biomedicínského inženýrství a Policejní akademii ČR v Konferenčním centru CITY Praha 4 – Pankrác.

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 nebyvale 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 300, přičemž konečné množství návštěvníků, kteří se konference zúčastnili, bylo cca 260.

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 pořádát **opět v červnu 2026**.

Veškeré informace týkající se našich konferencí jsou k dispozici na webo-

vých stránkách: <https://www.ochrana-mekkychcilu.eu/>

Jako příjemný bonus, nejen pro účastníky konference, ale i ty, kteří se jí nemohli zúčastnit, jsou od neděle 29. 6. 2025 postupně umísťovány záznamy jednotlivých přednášek na stránkách <https://youtube.com/channel/UCBU-xiqwV92hRxp9bKSZkrhg>

Několik konkrétních informací k 9. ročníku konference Ochrana měkkých cílů 2025:

- registrace byla kvůli kapacitě sálu otevřena pouze pro 300 posluchačů
- na konferenci přišlo 260 návštěvníků
- v auditoriu naslouchali reprezentanti: ústředních orgánů státní správy
- krajů a významných měst
- nemocnic
- vzdělávacích institucí včetně univerzit
- kulturních a církevních institucí
- provozovatelé kritické infrastruktury, zástupci policie a dalších složek IZS

Shrnutí dotazníkového šetření mezi účastníky konference:

- 99 % návštěvníků deklarovalo zájem přijít příští rok znovu
- 89 % účastníků vysoce kladně hodnotilo, že součástí konference je prostor pro setkávání, ocenilo možnost setkání s partnery a přejí si to tak i v dalším roce
- 97 % návštěvníků výrazně kladně ocenilo techniku konferenčního centra, zejména kvalitu zvuku a projekce v sále
- 70 % návštěvníků projevilo zájem o sborník nebo jinou formu publikace příspěvků z konference (i v letošním roce máte možnost zveřejnění PR článku v časopise Bezpečnost s profesionály)
- 90 % účastníků považuje letošní skladbu témat konference za vynikající. Hodnocení „nejpotřebnějších“ témat pro další ročníky se příliš nemění. Z „bodového hodnocení“ vycházejí jako vítězné témata: nová řešení, analýzy útoku, postupy a metodiky, vzdělávání / výcvik a pohled útočníka. Návštěvníci velmi pozitivně ohodnotili volbu jednotliho dominantního tématu letošního roční-

ku konference, tedy oblast bezpečnosti veřejných prostranství.

V úctě

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

Ing. Tomáš Müller
prezident ČP AFCEA



MĚKKÉ CÍLE POD DROBNOHLEDEM - JAK TRÉNINK ZVYŠUJE NAŠI BEZPEČNOST

V současném bezpečnostním prostředí představují tzv. měkké cíle – místa s vysokou koncentrací osob a nízkou úrovní zabezpečení – významnou výzvu pro ochranu obyvatelstva. Patří sem školy, nemocnice, kulturní a sportovní zařízení či obchodní centra. Reálná cvičení zaměřená na ochranu těchto cílů jsou nezbytným nástrojem pro zvyšování připravenosti a odolnosti vůči různým typům hrozeb, včetně teroristických útoků či útoků aktivního střelce.

Během uplynulého roku jsme se s týmem společnosti **Safe Technology Safete** aktivně podíleli na desítkách cvičení zaměřených na ochranu měkkých cílů, která považujeme za klíčová pro testování a zdokonalování tří základních pilířů bezpečnosti: lidí, procesů a technologií.

Jedním z hlavních cílů cvičení je posílení schopnosti jednotlivců reagovat na krizové situace. To zahrnuje nácvik postupů podle principu USB, tedy Uteč – Schovej se – Bojuj, který je obecně uznáván jako efektivní strategická reakce na útoky aktivního střelce. I když jsou tyto postupy obecně známé, jejich praktické osvojení a automatizace vyžadují pravidelný trénink.

Dalším aspektem je schopnost rozpoznat hrozbu. Například na konci roku 2024 proběhlo na Vysoké škole chemicko-technologické v Praze testování schopnosti identifikovat zvuky střelby z krátkých i dlouhých palných zbraní. Výsledky ukázaly, že pokud střelba neprobíhá v bezprostřední blízkosti, její detekce je pro většinu osob obtížná.

Cvičení také zdůrazňují význam rozpoznávání podezřelého chování a posilují komunikační dovednosti účastníků. Efektivní a rychlá komunikace, jak interní mezi zaměstnanci, tak externí směrem k integrovanému záchrannému systému (IZS), je pro zvládnutí krizových situací klíčová. Součástí tréninku

je i zvládnutí stresu a paniky, které v takových situacích nastávají.

V neposlední řadě pak cvičení slouží k praktickému ověření krizových scénářů a identifikaci potenciálních nedostatků v bezpečnostních plánech. Může odhalit třeba to, že evakuační cesty jsou blokovány nebo že některé unikové dveře jsou zamčené. Dále umožňují testovat spolupráci mezi interními týmy a složkami IZS, což je zásadní pro efektivní reakci na mimořádné události.

Technologie jako klíčový faktor úspěchu – proč je testování nezbytné?

Součástí většiny reálných cvičení zaměřených na ochranu měkkých cílů bývá také testování technologií. Přesto se stále setkáváme s mylným názorem, že technologie po nasazení „prostě fungují“ a není třeba jim věnovat zvláštní pozornost. Takový přístup je z hlediska krizové připravenosti zcela nepřijatelný. Stejně jako osobní dovednosti a procesní opatření, je nutno pravidelně testovat i technologická řešení, průběžně ladit a ověřovat jejich funkčnost v kontextu aktuálních hrozeb a provozních podmínek.

Z vlastních zkušeností víme, že bez pravidelného ověřování nedokážeme zajistit spolehlivou funkci ani u technologií, které byly původně implementovány jako „bezpečné a odolné“. Ve své praxi se zaměřujeme především na

testování komunikačních technologií, které tvoří páteř efektivního varování, svolávání a řízení krizové odezvy. Není výjimkou, že organizace při mimořádné události spustí hromadné hlasové volání směrem ke stovkám až tisícům osob, aniž by si uvědomila omezenou kapacitu mobilních sítí. Výsledkem bývá zahlcení místní sítě a neúměrné zpoždění při doručování zpráv.

Podobné komplikace nastávají i při využívání jediné GSM brány pro rozšiřování SMS zpráv – pokud odeslání každé zprávy trvá přibližně dvě vteřiny, odeslání 500 SMS zabere více než čtvrt hodiny. V případě rychle se vyvíjejících krizových scénářů, jako jsou útoky typu AMOK, je taková prodleva kritická – sdělení přichází příliš pozdě na to, aby mělo reálný přínos pro ochranu osob.

S rostoucím významem kybernetické bezpečnosti se do scénářů technologických cvičení stále častěji začleňují také simulace kybernetických útoků a výpadků infrastruktury (blackoutů). Organizace si začínají uvědomovat, že ani sebelepší plán nemá reálnou hodnotu, pokud nebyl ověřen v podmínkách simulujících narušení běžného provozu.

Výstupy z technologicky orientovaných cvičení generují velké množství dat, která je nutno systematicky vyhodnocovat. Pouze důslednou analýzou těchto poznatků lze dosáhnout zlepšení technologických procesů a zvýšení

jejich efektivitu v reálných krizových situacích. Odpovědné instituce by proto měly testování považovat za integrální součást své bezpečnostní kultury, nikoli za jednorázovou nebo formální aktivitu.

Integrovaný přístup jako základ efektivní krizové připravenosti

V oblasti ochrany měkkých cílů je klíčové chápat, že skutečná odolnost vůči krizovým situacím nevzniká izolovaným tréninkem jednotlivých složek, ale jejich koordinovaným a opakovaným testováním v reálných podmínkách. Pouze komplexní cvičení, která propojují lidský faktor, procesní rámce a technologickou infrastrukturu, umožňují odhalit slabá místa a zajistit hladký průběh krizové reakce.

Tři pilíře ochrany měkkých cílů

- Lidský faktor

Jednotlivci a týmy musí být schopni reagovat pod tlakem, rychle se rozhodovat a efektivně komunikovat. Trénink zaměřený na rozvoj těchto dovedností zvyšuje schopnost zvládat stresové situace a minimalizovat chyby.

- Procesní rámce

Jasně definované a nacvičené postupy jsou základem pro koordinovanou reakci. Bez nich může dojít k chaosu a zmatku, což zvyšuje riziko selhání.

- Technologická infrastruktura

Je nezbytné pravidelně testovat spolehlivost a funkčnost technologií podporujících komunikaci, monitorování a řízení krizových situací – jejich připravenost na různé scénáře.

Pouze integrace všech těchto tří složek do jednotného cvičení umožňuje spolehlivě a účinně simulovat reálné krizové situace a ověřit připravenost organizace na jejich zvládnutí. Takový přístup nejen zvyšuje efektivitu reakce, ale také posiluje důvěru zaměstnanců a veřejnosti ve schopnost organizace čelit mimořádným událostem.

Tedy jen prostřednictvím integrovaného a pravidelného cvičení všech klíčových složek lze dosáhnout vysoké úrovně krizové připravenosti, která minimalizuje škody na majetku, a co je nejdůležitější – chrání lidské životy.

Ing. Jan Burian

Generální ředitel

SAFE Technology Safete

Průběh vzniklé události



Rychlost varování při reálném požárním cvičení – Právnická fakulta UK



Požární cvičení na Univerzitě Karlově



Požární cvičení na Univerzitě Karlově

OCHRANA PROTI ZÁVAŽNÝM KINETICKÝM ÚTOKŮM

Motto:

Infrastruktura je dnes legálním cílem útoků.

Kinetický útok vozidlem je taktickou metodou jeho použití jako zbraně, při které tímto pachatel úmyslně najede na osoby či budovy s cílem způsobit jim ztráty, smrtelná zranění nebo jiné škody. Použitelným prvkem jsou všechny typy vozidel; jsou snadno dostupné, tvoří běžnou součást každodenního života, přičemž záměr do poslední chvíle nelze odhalit, jeho uskutečnění vyžaduje minimální finance, přípravu i schopnosti, a má potenciál způsobit velké ztráty na životech nebo infrastruktuře.

VYMEZENÍ POJMU KINETICKÝ ÚTOK

Pojem „Kinetický“ (z řeckého Κινητικός – kinētikós = uvedení do pohybu, kinetos = pohyblivý, kineo = pohybovat se) ve spojení kinetická energie = pohybová energie vyjadřuje proměnlivé děje a veličiny v časovém průběhu. Kinetický útok lze definovat jako „Pohybový útok, který způsobuje okamžitou škodu nebo újmu za použití zbraní nebo síly“.

Ve vojenské terminologii je užíván pro raketové útoky či nálety, anebo jako eufemismus pro armádní bojové operace; v názvosloví civilní obrany jako pojem pro záměrné použití automobilu jako zbraně k útoku, s cílem způsobit nárazem co největší materiální a lidské škody.

ROZHODUJE HMOTNOST A RYCHLOST TĚLESA

Kinetická energie (E_k [J]) je energie, kterou disponuje objekt v důsledku svého pohybu. Je základním pojmem

ve fyzice, hraje klíčovou roli při pochopení dynamiky pohybujících se objektů, a má význam při porozumění základním principům chování částic, vozidel nebo nebeských těles.

V případě vozidla závisí množství kinetické energie útočícího objektu na jeho hmotnosti a rychlosti.

- Hmotnost tělesa (m , mass [kg]) – roste úměrně.
- Rychlost pohybu tělesa (v , velocity [ms⁻¹]) – roste druhou mocninou rychlosti.
 - Pokud se rychlost zdvojnásobí, zvětší se pohybová energie 4x.
 - Pokud se rychlost zpětinásobí, zvětší se pohybová energie 25x.
 - Pokud se rychlost zesateronásobí, zvětší se pohybová energie 100x.

$$E_k = \frac{1}{2} mv^2$$

TESTY DEKRA NA PROTITERORISTICKÉ BETONOVÉ BLOKY



DEKRA – nadnárodní organizace se specializací na technické inspekce, testování, certifikaci a bezpečnost v oblasti dopravy – testovala volně ložené betonové silniční bloky 0,8 × 0,5 × 1,6 m o hmotnosti 2,5 tuny určené k zabránění teroristických útoků ve městech nákladními vozy. Ty se ukázaly jako neúčinné, když měly zastavit desetitu-

nový nákladní automobil v rychlosti 50 km/h. Pohybovou energii vozu jsou schopny absorbovat jenom sofistikované zádržné systémy.



DEKRA byla založena v roce 1925 v Berlíně jako Deutscher Kraftfahrzeug-Überwachungs-Verein (Německý svaz pro kontrolu motorových vozidel) a je špičkovou a renomovanou mezinárodní organizací poskytující expertní služby v oblasti bezpečnosti. Od svého vzniku přispívá důležitou měrou k prevenci nehod a ochraně životů. Podle DEKRA je problematické, že v současné době neexistují žádné právní požadavky na potřebné ochranné vlastnosti protiteroristických bariér



Detail zadržení nákladního vozu SCANIAT třídy N3 dle PAS 68 v kategorii

VOZIDLO UŽ NENÍ JEN DOPRAVNÍ PROSTŘEDEK

7.500 kg při rychlosti 50,1 km/h, použitý vůz na obrázku má hmotnost devět tun. V testu je názorně demonstrován jasný rozdíl mezi zadržením alternativním systémem pomocí tří pevnostních betonových bloků vzájemně propojených pevnostním ocelovým lanem (na výřezu obrázku bloky č. 2 a 3) v porovnání s předešlými testy se samostatně umístěnými volně ležícími protiteroristickými betonovými bloky běžně používanými na akcích, viz oba obrázky výše.

Je zřejmé, že pokud není bariéra řádně fixována, může být posunuta i při kinetickém útoku lehčím vozidlem.

Naopak, jestliže je bariéra pevně ukotvena do země, nebo jsou její prvky vzájemně pevnostně propojeny, dokáže bezpečně zadržet i těžký náraz, přičemž musí odolat vyšší kinetické energii.

Při volbě a užití bezpečnostních bariér je nutno zvažovat také zónu deformace útočícího vozidla, neboť při nárazu se část energie přemění na plastickou deformaci – absorbují ji podélníky, nosníky pod motorovým prostorem, rámové výztuhy, nárazníky s tlumícími prvky, kapota a blatníky. Dlouhá deformační zóna u osobního automobilu proto pohltí více energie, a na bariéru působí menší síla. Naopak těžké kamiony mají často krátké deformační zóny a tuhý rám, v důsledku čehož je směřováno více kinetické energie přímo do bezpečnostní bariéry; proto musí být tyto robustně fixovány.

CHARAKTERISTIKA ÚTOKU VOZEM S VÝBUŠNÝM NÁSTRAŽNÝM SYSTÉMEM



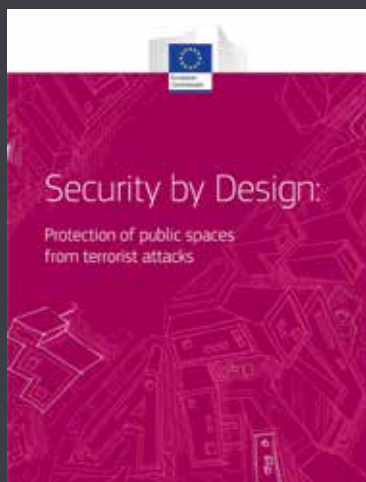
Rychlé a účinné dopravení velkého množství výbušnin na místo útoku, vozidlo užito jako jejich nosič; může být řízeno atentátníkem nebo zapar-

kované s nastaveným časovým spínačem. Cílem útoku je buď infrastruktura – mosty, silnice, kontrolní stanoviště, nebo budovy – vojenské základny, úřady, objekty KI, případně živá síla – davy lidí, vojenské nebo policejní hlídky. Primárním účinkem je silná exploze mající za následek rozsáhlé škody na majetku a zpravidla i vysoký počet lidských obětí, sekundárními efekty jsou pak požár, zřícení budovy, a dlouhodobý těžký psychologický dopad.

CHARAKTERISTIKA ÚTOKU KAMIONEM ČI JINÝM VOZIDLEM

Signifikanční jsou pro něj následující rysy: Náhlost a jednoduchost – útok bez varování, pachatel nepotřebuje zbraně, výbušniny, speciální výcvik. Vysoká smrtelnost – obrovská kinetická energie zabije desítky lidí během několika sekund. Veřejná místa – pěší zóny, festivaly, vánoční trhy, demonstrace, promenády. Vozidlo – kamion, dodávka, autobus, vozy s vysokou hmotností a schopností prorazit bariéry. Útočící – většinou jednotlivci, ale mohou být i součástí koordinovanějších útoků. Cíle – živá síla nebo kritická infrastruktura.

INSTITUTE OF BLAST & IMPACT PROOF CONCRETE, IBIPC



Firma IBIPC je český výrobce, konzultant a přední dodavatel v oblasti bezpečnostních řešení a ochranných prvků pro obranný průmysl, kritickou infrastrukturu a civilní obranu, které jsou realizovány z ultra vysokovýkonného drátkobetonu – patentovaného UHPFRC. IBIPC je katalogizovaný výrobce NATO Support and Procurement Agency (NSPA) s přiděleným NATO Commercial and Government Entity Code 8286G. Všechny výrobky jsou certifikovány Vojenským výzkumným ústavem dle normy NATO STANAG 2280:2016 na balistickou, výbuchovou a střepinovou odolnost. IBIPC spolupracuje s ČVUT Praha a Univerzitou obrany v Brně, a je členem Asociace obranného průmyslu a Security Bunkers Alliance. Výrobní program IBIPC obsahuje Bezpečnostní bariéry, Balistické stěny, Zadržné systémy, Zodolnění objektů, a Bunkry a kryty.

IBIPC navrhuje design ochrany moderních městských center, aniž by se podobala opevněným zónám, dle konceptu Evropské komise SECURITY BY DESIGN, tj. BEZPEČNÝ DÍKY NÁVRHU, kdy je prvek navržen od základu tak, aby byl jednoznačně bezpečný. Ochranná opatření harmonicky zapadají do okolního prostředí, nenarušují civilní vzhled místa a nejsou nepřiměřená. Kompletní realizace v čteně návrhu, instalace i dlouhodobého servisu.

S důrazem na kvalitu, certifikace NATO, špičkový výzkum a úzkou spolupráci s výzkumnými institucemi a armádními subjekty je IBIPC silným hráčem v oblasti bezpečnostní infrastruktury.

DOPORUČENÉ POSTUPY IBIPC PROTI KINETICKÉMU ÚTOKU VOZIDLEM

1. KONTROLA VSTUPNÍCH A VÝJEZDOVÝCH BODŮ. Instalace mobilních nebo pevně zapuštěných bezpečnostních prvků Osten či Květino-vý box u všech vstupů pro chodce a zásobování. Rozstup mezi prvky max. 1,2 metru k vytvoření místa pro chodce, nikoli pro vozidlo.
2. PERIMETR VEŘEJNÝCH PROSTOR. Obvodové zábrany maskované jako

mobiliář, tj. Květinové boxy s kotvenou betonovou základnou, nebo Balistické lavičky, či odpadkové koše z UHPFRC, případně nízké zídky či vodní prvky z UHPFRC - fontány s okrajem. Všechny prvky musí být pevně zakotveny a speciálně navrženy k zastavení těžkého vozidla při nárazu.

3. ÚPRAVA PŘÍSTUPOVÝCH CEST. Zkřívené a zúžené vjezdy – zabránění rozjezdu kamionu vysokou rychlostí. Zvýšené zpomalovací prahy u přístupových ulic.
4. MONITORING A DOHLED. Kamery s funkcí rozpoznávání registračních značek, mobilní hlídky městské policie zejména při konání akcí.
5. PŘECHODNÉ MOBILNÍ ZÁBRANY. Pro akce jako trhy, koncerty nebo demonstrace aplikovat prvky řady Osten v policejní či vojenské verzi, případně mobilní Květinové boxy, či speciální gabiony naplněné vodou, pískem, štěrkem. Parkovaná služební vozidla města, vhodně umístěná jako bariéra.

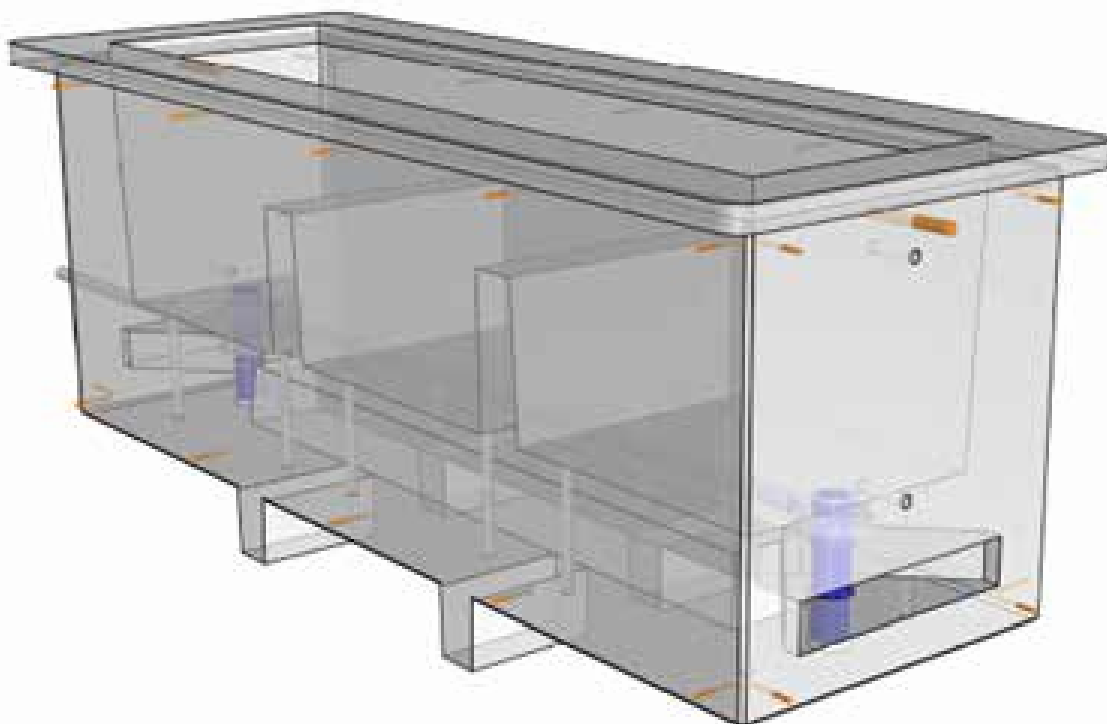
Pouze místa chráněná neprostupnou hradbou a nedostupná autům jsou před tímto typem útoku bezpečná.

DOPORUČENÁ SYSTÉMOVÁ OPATŘENÍ

1. FYZICKÉ ZÁBRANY. Betonové bloky, zahrazovací konstrukce, strategické parkování.
2. URBANISTICKÁ OPATŘENÍ. Zúžení ulic u vstupů na pěší zóny, konstrukční překážky, bezpečnostní design budov a veřejných prostranství, zóny s přirozenými překážkami, umístění pěších zón mimo hlavní silniční tahy.
3. PRÁVNÍ A PROVOZNĚ ORGANIZAČNÍ OPATŘENÍ. Zákazy vjezdu těžkých vozidel do center měst, místní vyhlášky o ochraně veřejného prostoru, plány krizového řízení obcí a krajů, předem schvalované trasy a časy zásobování, registrace a monitoring vjezdů kamerovými systémy, zvýšený dohled při akcích s velkým množstvím lidí.
4. LIDSKÉ FAKTORY A REAKCE. Školení bezpečnostního personálu a složek IZS, simulace krizových scénářů. Informovanost veřejnosti, co dělat při útoku vozidlem.



Ing. Pavel Bělohradský
CEO Institute of Blast & Impact Proof
Concrete
www.ibipc.com



Průhled mobilním ochranným prvkem Květinový Box. Při bližším pohledu je v dolní části vidět ocelové lano s okem zavěšené na ose čepu, kterým lze v případě potřeby modulárně propojit další prvky, a vytvořit tak pevný ale pružný řetěz z Květinových Boxů k zachycení kinetické energie útoku vozidlem.

Typ prvku je volně uložený na povrchu – nikoliv nasazený na zapuštěnou kotevní desku do země, která je rozšířenou fixní variantou k zadržení těžkých kamionů – a zachytí osobní vůz kategorie N1 dle PAS 68 při 50km/hod. Konstrukce na povrchu umístěného prvku umožňuje jeho propojení pevnostním ocelovým lanem s dalšími Květinovými boxy a jejich

postupné sesazení v linii jako článků řetězu; v takové konfiguraci odolá vytvořená bariéra nárazu nákladního vozu kategorie N3 dle PAS 68 při 50km/hod.

Základní provedení je připraveno k designovému opláštění IBIPC, anebo vizuálnímu řešení dle požadavků klienta.

CHRÁNÍME VÁS
JIŽ OD ROKU
1992



BEZPEČNOSTNÍ TECHNOLOGIE A SLABOPROUDÉ SYSTÉMY

ABAS IPS MANAGEMENT



WWW.ABASCO.CZ



ZÁVAŽNÉ INCIDENTY POD ŠIRÝM NEBEM A MOŽNOST JEJICH PREVENCE

(příspěvek vychází ze stejnojmenné přednášky, která zazněla v rámci konference Ochrana měkkých cílů 2025)

Násilná kriminalita, útoky nožem a dalšími chladnými zbraněmi

Útoky nožem nebo obecně chladnými improvizovanými zbraněmi, zejména na veřejných prostranstvích, představují emotivní téma pro společnost v celé řadě států. Autoři využili v této souvislosti zahraniční statistiky k tématu, zejména z Belgie, Portugalska a Rakouska. Další informace z otevřených zdrojů se týkají zejména Spojeného království. Nechybí přitom ani teoretické úvahy o příčinách útoků tohoto druhu.

Veřejný prostor jako „místo činu“

Incidenty na veřejných místech může představovat střelba, útoky nožem nebo vozidlem, ale i široké spektrum další eventualit. Úvahy o bezpečnosti ve veřejném prostoru naznačují nutnost mezioborového přístupu.

Prevenici (ve vztahu k bezpečnostním incidentům) je třeba vnímat jako neopomenutelnou součást funkce stavby nebo prostranství. Koncept integrované bezpečnosti začíná už v okamžiku zadávání projektového, respektive architektonického návrhu. Svou roli zde sehrávají nejen součásti bezpečnostního systému v užším smyslu slova, ale i další aktéři – architekti, obecní zastupitelé, nevládní, akademický a vědeckovýzkumný sektor, stejně jako externí poradci. Vedle úvah o primárním poslání budovy nebo areálu (park, obchodní centrum) je tedy zapotřebí sledovat bezpečnostní priority, například jak by

v rámci prostoru vypadal úkryt nebo útěk.

Jedná se přitom o časově nikdy neskončené zadání. Nikdy není možné tvrdit, že téma je vyřešeno jednou provždy a incident tohoto druhu je zcela vyloučen.

Belgie

K tématu se vztahuje statistika označená zde v tabulce a grafu jako Počet případů registrované kriminality, „Pobodání“ na veřejných prostranstvích nebo dalších veřejných místech. Definice trestného činu v těchto případech zní „zranění nebo zabití, při kterém pachatel způsobil nebo se pokusil zasadit (nožem) bodnutí do oběti“. V tabulce jsou uvedeny případy, kde je jako místo činu uvedeno „veřejné místo“ (veřejné komunikace, parky, ale může se jednat i o obchody, železniční stanice, restaurace či jiné veřejné provozovny). Termín „veřejné místo“ nebo „veřejná budova“ přitom může být interpretován velmi různorodě, a to i podle konkrétních policejních spádových regionů.

Obecně se pro veřejná místa v nejširším smyslu slova ve vztahu k útokům chladnými zbraněmi neplánují žádná konkrétní preventivní opatření. Policejní síly postrádají ve vztahu k tématu jednoznačné podklady či statistiku.

Rakousko

Související statistiku zajišťuje Spolkové ministerstvo vnitra. K tématu se vztahuje celá řada proměnných, zejména:

- prostředky trestného činu (použitá zbraň, například bodná zbraň),
- podezřelí (pohlaví, věk, občanství/národnost),
- oběť (pohlaví, věk, občanství/národnost),

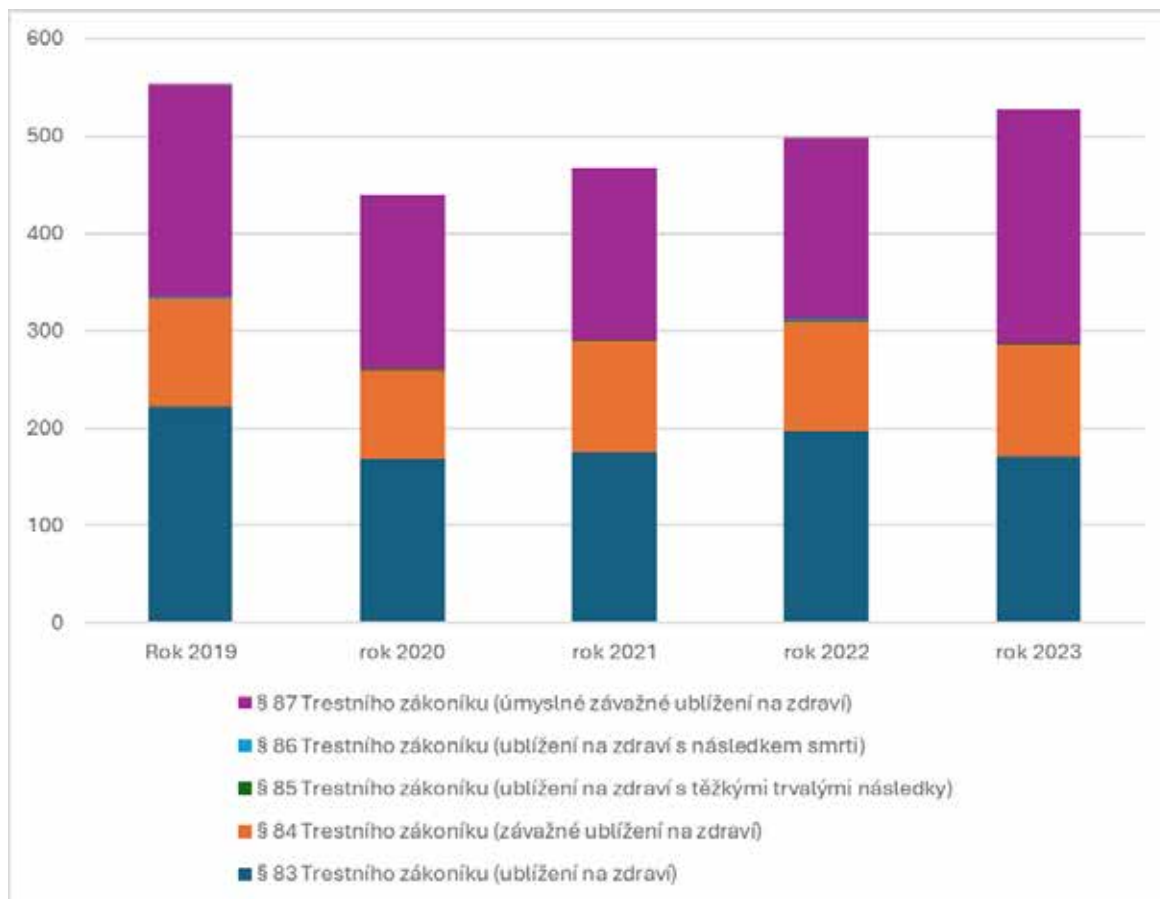
V řadě případů (jako pachatelé-podezřelí, anebo oběti) dominují občané Rakouska, což však mohou být i naturalizovaní přistěhovalci či osoby s přistěhovaleckými kořeny. Jinak jsou výrazně zastoupeny osoby původem z jihovýchodní Evropy, z postsovětského prostoru (Ruská federace, což mohou být nezřídkda Čečenci) nebo osoby mimo-evropského původu (Afghánistán, Sýrie, severní Afrika).

Nizozemsko

Policejní sbor je zapojen do různých preventivních iniciativ zaměřených na boj proti zneužívání bodných zbraní, jako jsou osvětové kampaně, spolupráce se školami (pomocí tzv. školních policistů) a s dalšími partnery. V rámci citlivých objektů probíhají preventivní prohlídky osob. Nizozemská policie rovněž natočila internetový film s cílem zvýšit povědomí o rizicích držení zbraní mezi mladými lidmi (získal cenu za nejlepší dokumentární film roku 2012; 22 minut, <https://vimeo.com/19722882>; heslo: ijzer).

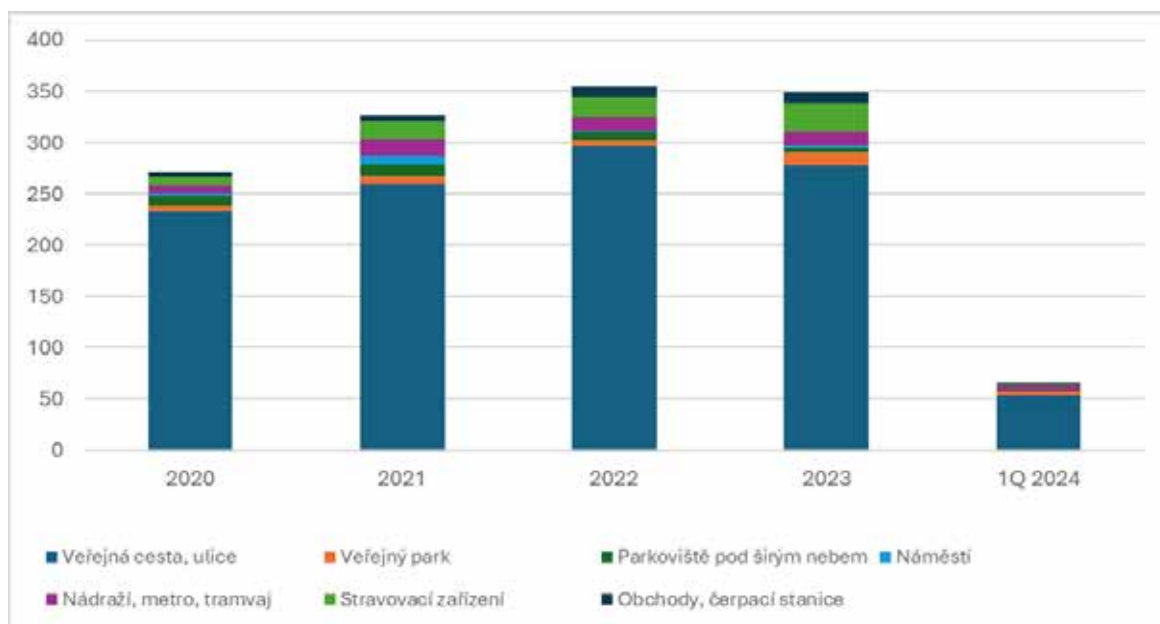
Tabulka a graf: Rakousko. Registrované trestné činy, při kterých byla použita bodná zbraň, § 83–87 trestního zákoníku, roky 2019 až 2023.

ÚTOK	2019	2020	2021	2022	2023
§ 83 trestního zákoníku (ubližení na zdraví)	222	168	175	197	170
§ 84 trestního zákoníku (závažné ubližení na zdraví)	111	92	115	113	116
§ 85 trestního zákoníku (ubližení na zdraví s těžkými trvalými následky)	~	1	1	1	1
§ 86 trestního zákoníku (ubližení na zdraví s následkem smrti)	1	~	~	1	~
§ 87 trestního zákoníku (úmyslné závažné ubližení na zdraví)	219	179	176	187	240
Celkem	553	440	467	499	527



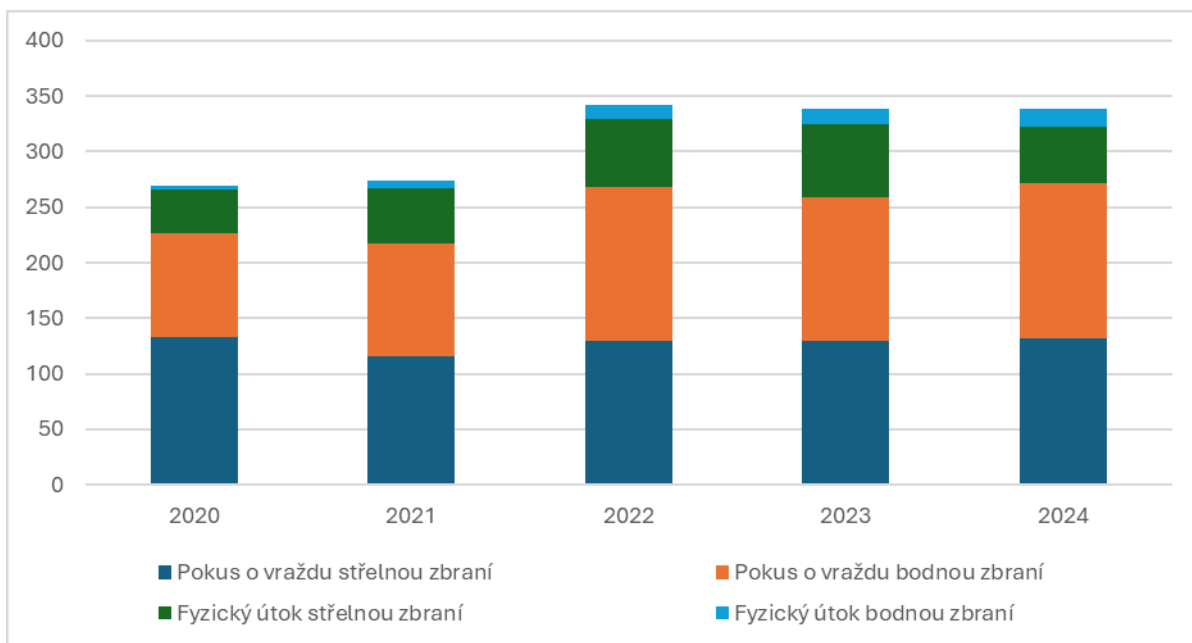
Tabulka a graf: Belgie. Počet případů registrované kriminality, „Pobodání“ na veřejných prostranstvích nebo místech.

„Místo činu“	2020	2021	2022	2023	1.Q 2024
Veřejná cesta	233	260	297	278	54
Veřejný park	6	8	5	13	4
Parkoviště pod širým nebem	9	11	9	3	1
Náměstí	2	8	1	4	0
Nádraží, metro, tramvaj	8	16	13	13	4
Stravovací zařízení	9	18	19	27	2
Obchody, čerpací stanice	4	6	11	11	1



Tabulka a graf: Portugalsko. Počet případů použití bodných a střelných zbraní (Justiční policie):

ÚTOK	2020	2021	2022	2023	2024	Celkem
Pokus o vraždu střelnou zbraní	133	116	130	130	132	641
Pokus o vraždu bodnou zbraní	94	101	138	129	140	602
Fyzický útok střelnou zbraní	39	50	62	66	50	267
Fyzický útok bodnou zbraní	3	7	12	14	17	53
Celkem	269	274	342	339	339	1 563



Sekundární studie k tématu

Útoky nožem na veřejnosti v Evropě jsou závažným problémem, který přitahuje značnou pozornost společnosti i médií. Téma vede i k politizaci problematiky, zejména pokud souvisí s pachateli z přistěhovalckého prostředí.

Studie „Celosvětový růst kriminality způsobené noži“ Roberta Kaisera se

zabývá kriminalitou spojenou s použitím nožů. Autor doporučuje v případě útoku útěk jako nejlepší obranu, pokud je to možné. I malá řezná rána může vést k rychlé ztrátě krve a následné smrti. Nicméně útěk není vždy možný, zejména v závislosti na prostředí. Proto studie zdůrazňuje potřebu lepší ochrany a výcviku pro pracovníky v první linii, kteří čelí těmto hrozbám – včetně personálu soukromých bezpeč-

nostních služeb.

Kriminalita spojená s noži přitom není omezena na konkrétní zemi nebo kulturu, ale představuje globální problém.

Útoky nožem (ale i jinými improvizovanými prostředky, včetně útoku automobilem) se mohou vyskytnout i ve společnostech, kde je držení střelných zbraní značně regulováno. To platí například

Ilustrace: Ve světovém srovnání je téma útoků nožem zdaleka nejviditelnější v Jihoafrické republice.



pro Čínskou lidovou republiku. Roku 2014 zde bylo 33 osob zabito a 130 dalších zraněno při koordinovaném útoku nožem na nádraží v provincii Jünan. Roku 2015 bylo nožem zabito 50 dělníků v uhelném dole. Roku 2016 bylo nožem 15 osob zavražděno a 45 dalších zraněno útočníkem v domě s pečovatelskou službou. Ve stejném roce pobodal útočník 10 dětí v provincii Chai-nan. Roku 2017 útočil muž nožem v obchodním domě v Pekingu, kde zabil 1 ženu a 12 dalších osob zranil.

Situace ve Spojeném království

Nože a ostré předměty jsou ve Spojeném království stěžejním nástrojem vražd, konkrétně u 41 %. Motivace útoků nožem jsou různorodé a zahrnují osobní konflikty, loupeže, psychické problémy či teroristické úmysly. Výjimkou nejsou ani útoky na uniformované policisty. Ve Spojeném království je nošení nožů s čepelí delší než 3 palce (7,62 cm) „bez dobrého důvodu“ (respektive bez povolení, například u kuchařů) trestným činem (knife crime), což činí související statistiku ještě složitější. Držení nože pro sebeobranu přitom výslovně není chápáno jako ospravedlňující důvod.

John McShane ve studii z roku 2010 srovnává vývoj ve vztahu k tématu ve Spojeném království za několik desetiletí. „Na rozdíl od případů v minulosti, kdy spory postupně eskalovaly „od nadávek po pěsti“, se dnes okamžitě objevují na scéně čepelí, a to i ve sporech mezi mládeží.“ Řada těchto případů je výsledkem nevládnutého okamžitého vzteku, stejně jako absence empatie. Bodání nožem, bití tupým předmětem nebo škrcení je „kontaktní způsob útoku“, který vyžaduje daleko vyšší míru odhodlání a angažování než použití střelné zbraně. Lidé jsou pod tlakem emocionálním, fy-

zickým nebo ekonomickým, a pokud se nenaučí „upouštět páru“ kultivovanějším způsobem, mohou „vybouchnout“ třeba v prostředku hromadné dopravy, nebo pokud do nich na ulici někdo omylem strčí.

Stěžejní roli může sehrávat několik aspektů, které výrazně přispívají k nárůstu násilných trestných činů způsobených noži a jinými ostrými zbraněmi (včetně rozbitých lahví):

1. Náboženský/politický extremismus

Pokud skutečně věříte, že ubližování druhým je absolutně jediný způsob, jak dosáhnout štěstí/naplnění nebo svého konečného cíle (ať už je to cokoli), pak je nepravděpodobné, že sami od sebe ve svém jednání přestanete.

2. Drogy

Výroba a obchodování s drogami vždy souvisely s násilím. Pokud je útočník navíc drogami ovlivněn, může to použití nože urychlit.

3. Sociální vyloučení

Nošení nožů je příznakem širšího společenského problému. „Kultura nožů“ je příznačná zejména pro nejchudší lokality. Chybějící „pocit sounáležitosti“ vede u řady osob k touze stát se členem gangu, což následně souvisí s nutností nosit a používat nůž.

4. Sociální média

Pozornost veřejnosti znamená pro členy gangů velmi mnoho. V minulosti mohlo docházet k situacím, kdy před střetem někdo ustoupil, ale nyní si je útočník vědom toho, že lidé okolo situaci natáčejí – a nechce vypadat jako slaboch. A naopak, pokud incident přinese miliony zhlédnutí, je to pro jedince z okraje společnosti úspěch, i když skončí za mřížemi.

5. Vážná duševní nemoc

U mnoha osob, odpovědných za vícenásobné zabití, byla diagnostikována

vážná duševní choroba. V nebezpečí jsou sociální pracovníci a zdravotníci, kteří v řadě případů vstupují sami do obydli duševně nemocných osob.

Shrnutí a doporučení

Zkušenosti z násilných incidentů posledních let naznačují, že toto téma rozhodně není ničím, co je v rámci České republiky možno vyloučit. Nemusí se přitom jednat nutně o teroristické útoky, ale i o jiné eventuality nebo motivace útočníka. Trvalou výzvu představuje napětí mezi otevřeností a bezpečím – respektive napětí mezi primárním účelem určitého objektu (například škola nebo obchodní centrum) a snahou o implementaci odpovídajícího spektra bezpečnostních prvků. Jedná se o komplexní téma, zahrnující bezpečnostní studia, architekturu, techniku, psychologii, respektive právo – nejenom s ohledem na ochranu soukromí a jiných lidských práv.

Ve vztahu ke konkrétním zákazníkům a dalším aktérům – kterými mohou být například obce nebo městské části – může dojít k využívání služeb externího bezpečnostního poradenství. Může se jednat o zpracování konkrétních bezpečnostních analýz a řešení, porovnání bezpečnostních technologií, mapování možností dalšího postupu nebo podporu při zpracování žádosti veřejné podpory. Konkrétně **Mezinárodní bezpečnostní institut z. ú.** je progresivní vědeckovýzkumnou institucí, věnující se problematice mezinárodních i domácích bezpečnostních výzev. Náš tým se zabývá širokým záběrem činností a v této souvislosti si dovoluujeme čtenářům nabídnout své služby (<https://mbi.expert>).

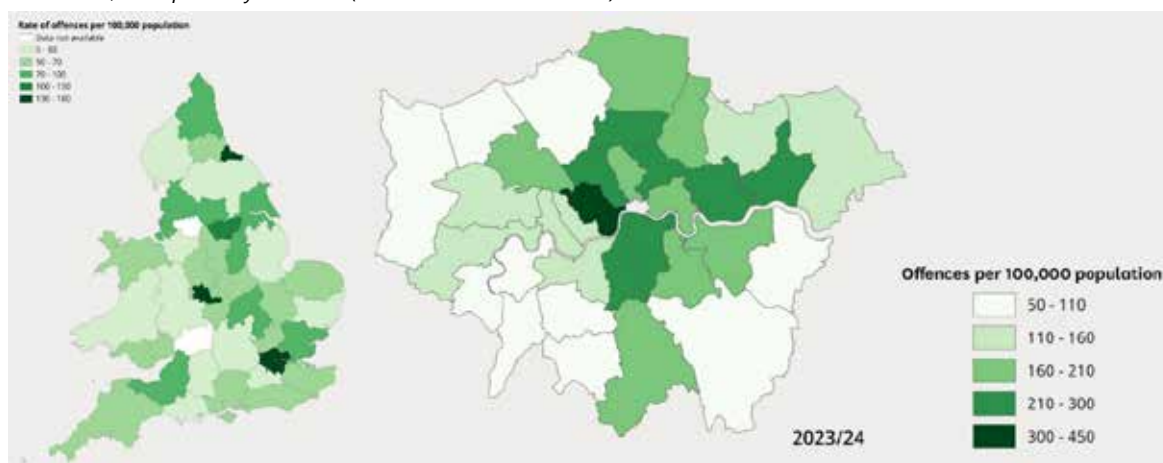
doc. Mgr. Oldřich Krulík, Ph.D.

Mgr. Filip Gundza, MBA

JUDr. Tomáš Koniček

Mezinárodní bezpečnostní institut, z. ú.

Ilustrace: Mapa výskytu případů za využití nože a jiných ostrých předmětů pro Anglii a Wales, s výjimkou policejní síly Greater Manchester, která podklady nedodala (březen 2023 až březen 2024).



Použité podklady

- A Surge in Mass Attacks Has Killed Dozens in China in Recent Months. Associated Press. 19. XI. 2024. <https://1url.cz/4JEoM>
- ALLEN, Grahame; WONG, Helen. Knife Crime Statistics: England and Wales. House of Commons Library, 27. I. 2025. <https://1url.cz/AJEoK>
- European Report on Preventing Violence and Knife Crime among Young People. World Health Organization, 2010. <https://iris.who.int/handle/10665/326377>
- KAISER, Robert. The Global Rise of Knife Crime – Why? Personal Protection on Specialized Solutions, 10. VI. 2024. <https://www.ppss-group.com>
- Knife Crime Statistics England and Wales. House of Commons Library, 27. I. 2025. <https://commonslibrary.parliament.uk/research-briefings/sn04304/>

- Knife Crime Statistics. Ben Kinsella Trust. <https://benkinsella.org.uk/knife-crime-statistics/>
- Knife Crimes per 100 000 People by Country and the Top 10 Ranking for the Same. Reddit. <https://1url.cz/CJEor>
- MCSHANE, John. Knife Crime: The Law of the Blade. Quercus, 2010. ISBN 978-1847249791.
- Personal Protection Specialized Solutions. <https://www.ppss-group.com/>
- Stabbing Deaths by Country. World Population Review, 2022. <https://1url.cz/JJEou>
- Statistiek. Politie. <https://www.politie.be/statistieken/nl/>

INTELIGENTNÍ KAMERY S DETEKCÍ ZVUKŮ

EXPERIMENT NA PRAŽSKÉM LETIŠTI (AŽ O 97 % RYCHLEJŠÍ REAKCE SLOŽEK IZS)

Útoky aktivního střelce jsou dnes bohužel častou hrozbou zejména v objektech typu letišť, nádraží, obchodních center nebo škol. V podobných krizových situacích rozhodují sekundy – čím dříve bezpečnostní složky zasáhnou, tím větší šanci mají ohrožení lidé přežít. Přitom tradiční způsoby hlášení incidentů bývají často pomalé, nepřesné a příliš závislé na lidském faktoru.

V tomto článku přiblížíme praktické výsledky nedávné studie ve formě experimentu na Letišti Václava Havla v Praze, který ukázal, jak dramaticky lze zkrátit reakční dobu bezpečnostních složek pomocí inteligentních kamer Axis Communications vybavených aplikací pro akustickou detekci Jalud Embedded (SED – Sound Event Detector).

O experimentu

Experiment proběhl během pravidelného cvičení Integrovaného záchranného systému (IZS), konkrétně v modelové situaci STČ-14/IZS – simulovaném útoku aktivního střelce v administrativní budově letiště Václava Havla v Praze. Tato budova byla vybrána pro její komplexní architekturu a realistické prostředí, ideální pro simulaci krizových situací. Samotná metodologie experimentu byla navržena tak, aby bylo možno objektivně a systematicky změřit účinnost technologie detekce zvuků v realistických podmínkách. Pro účely experimentu byly definovány čtyři různé scénáře útoku, které pokrývaly širokou škálu možných incidentů – od méně závažných až po kritické.

Scénář 1

Verbální konflikt bez výrazného zvukového projevu, který testoval základní schopnost technologie ignorovat běžnou konverzaci.

Scénář 2

Hádka s agresivním křikem, simulující situaci, kdy konflikt začíná eskalovat do potenciálně nebezpečného incidentu.

Scénář 3

Aktivní střelec pohybující se a střelící na více místech v budově, simulující velmi závažnou hrozbu.

Scénář 4

Opakovaná intenzivní střelba v omeze-

ném prostoru, která testovala schopnost systému detekovat a okamžitě upozornit na akutní a extrémně nebezpečnou situaci.

K provedení scénářů byli použiti figuranti z řad Policie ČR, kteří simulovali chování útočníků, a zaměstnanci letiště, kteří reagovali realisticky, tedy utíkali, schovávali se a snažili se ohlásit incident. Každá simulovaná situace byla detailně připravena a koordinována podle standardizovaných postupů pro krizová cvičení.

Z technologického hlediska byly v budově rozmístěny čtyři mobilní jednotky vybavené inteligentními IP kamerami Axis Communications (model AXIS P1387 Box Camera), které byly osazeny aplikací Jalud Embedded pro detekci zvukových událostí. Každá jednotka byla navíc doplněna mikrofonem a routerem, které zajišťovaly bezdrátovou komunikaci s centrálním dispečerským stanovištěm letiště. Tyto jednotky byly strategicky rozmístěny v klíčových lokalitách – dvě v přízemí u hlavního vstupu a recepce a dvě v patrech administrativní budovy.



Kamery Axis vybavené aplikací Jalud SED dokázaly díky integrovaným algoritmům umělé inteligence v reálném čase detekovat zvukové signály charakteristické pro krizové situace, jako jsou výstřely, agresivní křik nebo rozbití skla. Okamžitě po detekci byl automaticky generován alarm, který byl bez prodlení přenášen do bezpečnostního centra letiště. Tam mohli operátoři prostřednictvím živého videa z kamer situaci ihned verifikovat a bez prodlevy aktivovat krizový plán, včetně vyslání závažných jednotek na místo incidentu.

Při vyhodnocování experimentu byly přesně měřeny a zaznamenávány časy od začátku incidentu až po okamžik, kdy byla informace o incidentu předána složkám IZS – jak tradičními metodami (telefonát na tísňovou linku), tak automatickou notifikací pomocí akustické detekce v kamerách Axis.

Díky detailnímu a pečlivému provedení experimentu bylo možno přesně kvantifikovat rozdíly v rychlosti reakce mezi automatizovanou detekcí a tradičními metodami. Výsledky tak poskytují silné argumenty pro širší nasazení této technologie v bezpečnostní praxi.



Výsledky experimentu

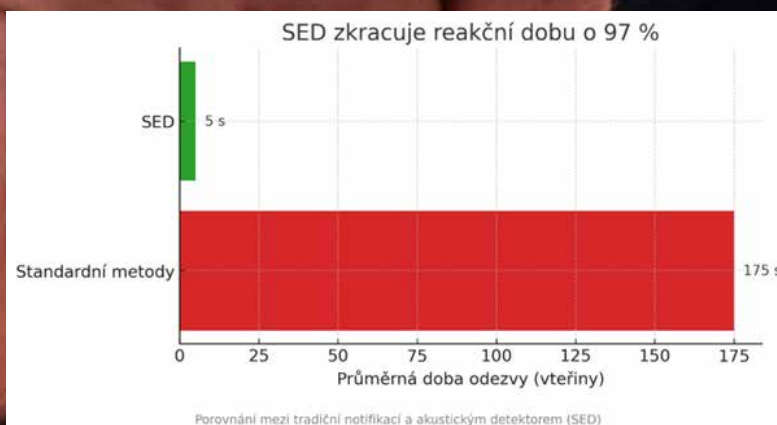
Experiment zahrnoval čtyři scénáře – od verbálního konfliktu až po střelbu

ve více patrech. Akustická detekce incidentů kamerami Axis s aplikací Jalud SED zkrátila dobu první notifikace

z průměrných 175 sekund na pouhých 5 sekund, což znamená zrychlení reakce složek IZS o neuvěřitelných 97 %.

Scénář	Detekce SED (Axis + Jalud)	Tradiční metoda	Rozdíl
Hádka s křikem	5 sekund	30 sekund	25 sekund
Střelba ve více patrech	5 sekund	6 min 50 s	6 min 45 s
Opakovaná střelba	5 sekund	1 min 27 s	1 min 22 s

Čísla mluví jasně: při skutečné krizové situaci by takový rozdíl mohl znamenat záchranu mnoha životů.



Výhody a limity řešení

Silnou stránkou použitého řešení je nejen rychlost a přesnost detekce, ale i snadná integrace do existujících systémů. Pokud již máte instalované IP kamery Axis, stačí nainstalovat aplikaci Jalud SED – není potřeba další HW. Tato integrace je nejen efektivní, ale především ekonomicky výhodná.

Limitem technologie je logicky její orientace na slyšitelné incidenty – střelbu, výbuchy nebo křik. Proto je ideální kombinace s videoanalýzou, což Axis kamery rovněž umožňují. Dále je nutné pečlivě vyladění systému, aby se předešlo falešným poplachům způsobeným běžnými zvuky v rušném prostředí.

Doporučení pro bezpečnostní praxi

Vzhledem k výsledkům experimentu

jednoznačně doporučujeme toto řešení prioritně implementovat na riziková místa, jako jsou letiště, školy či nádraží. Díky stávající infrastruktuře kamer Axis je zavedení této technologie rychlé, snadné a levné.

Důležitým krokem je také pravidelné školení personálu a pravidelná kontrola funkčnosti technologie prostřednictvím praktických cvičení. Tím zajistíte, že systém bude připraven v kritických chvílích okamžitě a správně reagovat.

Experiment jasně prokázal, že využití IP kamer Axis s aplikací Jalud Embedded pro detekci zvuků může významně zvýšit úroveň bezpečnosti měkkých cílů. To vše bez nutnosti významných investic do další infrastruktury. Výsledky tohoto experimentu byly podrobně

publikovány v prestižním mezinárodním recenzovaném časopise International Journal of Safety and Security Engineering, což potvrzuje jejich vědeckou relevanci a praktickou použitelnost.

Je načase využít existující technologie efektivně a zajistit tak rychlejší a účinnější reakci na hrozby, které nás bohužel mohou kdykoli potkat.

Mgr. Dalibor Smažinka, MBA, LL.M. specialista na bezpečnostní technologie Axis Communications Fakulta bezpečnostního inženýrství VŠB-TUO

O autorovi:

Mgr. Dalibor Smažinka, MBA, LL.M., je specialistou na bezpečnostní technologie s více než 20 lety praxe v oboru. Dlouhodobě spolupracuje se švédským výrobcem bezpečnostních technologií Axis Communications a v současné době se připravuje na doktorát na Fakultě bezpečnostního inženýrství VŠB-TU Ostrava, kde se zaměřuje na inteligentní bezpečnostní technologie a jejich propojení s fyzickou bezpečností, kyberbezpečností a ochranou dat.

NA CO SE ZAMĚŘIT, KDYŽ VYBÍRÁTE DOHLEDOVÉ CENTRUM?

Na zařízení pro dohledová centra jsou kladeny specifické nároky, a tedy i výrobky musí splňovat specifické parametry.

Na trhu je řada výrobců zobrazovačů (ať už LED nebo LCD), ale pouze naprosté minimum z nich se primárně zaměřuje na dohledová centra.

Na straně LED používají výrobci svoje standardní řady, které „mimochodem“ nabízejí jako vhodné rovněž pro dohledová centra.

Na straně LCD je situace jednodušší, neboť výrobci bezrámečkových displejů je velmi málo, ale existují dodavatelé, kteří videostěny skládají z displejů pro toto využití zcela nevhodných (např. z řad signage, nebo dokonce běžných TV).

Životnost

- Standardně udávaná životnost LED modulů se pohybuje okolo 100 000 hodin, je však třeba dodat, že tento údaj platí většinou pro provoz při 50% jasu. Z tohoto pohledu (a v zásadě pouze z tohoto pohledu) je pak důležitý maximální jas videostěny. V dohledových centrech přitom jas videostěny většinou nepřesahuje cca 250 nit, tzn. že minimální požadovaný jas by měl být alespoň 500 nit.

Servisovatelnost, záruka, dostupnost náhradních dílů

- **Jak velký modul je třeba v případě poruchy měnit a jak rychle ho lze vyměnit?**
LED stěny pro dohledová centra mají výměnu řešenou tak, že se mění pouze malé části, bez nutnosti rozebírat větší část, a to takovým způsobem, že to zvládne i vyškolený pracovník centra.
- **Jak velká část stěny vypadne při poruše/výměně modulu?**
U LED videostěn pro dohledová centra vypadne v případě poruchy/výměny většinou pouze malá část obrazu, zbytek stěny funguje nadále.
- **Jak dlouho výrobce produkt podporuje, např. i nad rámec záruky?**
Řešení pro dohledová centra mají jasně deklarovaný cyklus – tzv.

End of Life a End of Service. Po oznámeném End of Life následuje většinou tříleté období, kdy produkt nelze koupit, ale jsou dostupné náhradní díly. Výrobci také drží náhradní díly pro všechny produkty, které jsou kryté zárukou.

• Jakou záruku lze na stěnu pořídit?

Pro řešení určená pro dohledová centra lze pořídit až desetiletou záruku; s ohledem na výši investice doporučujeme minimálně pětiletou.

Automatická kalibrace, včetně kalibrace případných náhradních modulů

- Videostěna musí být barevně a jasově jednotná bez nutných servisních zásahů a bez ohledu na provoz.
- V případě výměny modulu se tento musí zařadit do videostěny tak, aby byl nerozeznatelný.

Barevné podání, věrnost a kontrast i při nízkém jasu

- Kvalitní výrobci LED videostěn pro ně vyrábějí také vlastní video-processory a mají tak kompletní kontrolu nad zobrazením. Levné varianty jsou složené z „nějakých“ modulů (které jsou zrovna skladem) a z „nějakého“ procesoru (většinou čínské produkce) a nikdy nebudou schopny přesně zobrazit např. definovanou bílou. Špičkové procesory zaručují optimální škálování obrazu bez rozmazání.
- Bez vlastního kvalitního procesoru dochází často k barevným posunům anebo ke ztrátě detailů především při nízkých jasech – přesně takových, jaké se využívají v dohledových centrech.

Ukázka špatného barevného podání při špatném processingu.



Technologie proti únavě očí a komfort uživatelů

- Pracovníci dohledového centra se na některých pracovištích dívají na videostěnu až 70 % času z 8 nebo 12hodinové směny, je proto extrémně důležité, aby zobrazovače obsahovaly technologie, jež bojují proti únavě očí a případným bolestem hlavy.
- Diskomfort uživatelů vzniká obnovováním zobrazení po řádcích, v tzv. scan lines, a příliš nezáleží, jak je vysoká obnovovací frekvence. Špičkoví výrobci tento problém řeší buď nahodilou obnovovací frekvencí pro jednotlivé pixely, nebo obnovováním nikoli v řádcích, ale ve sloupcích.

Redundance

- Signálová – vícero tras v samotné LED pro případ poškození kabelu nebo výpadku na trase (např. vadný modul), videostěny pro dohledová centra by ji měly mít minimálně dvojitou, ideálně čtyřcestnou.
- Procesorová – zdvojení videoprocessorů LED stěny (a jejich kabeláže do videostěny) pro případ poruchy.
- Napájení – zdvojení napájecích zdrojů nebo vzdálené napájení z racku.

Bezpečnost

- Kontrola nad celým signálovým řetězcem – šifrování celého řetězce tak, aby v žádném případě nemohlo dojít k odposlechu.
- Žádné komponenty čínské výroby (kromě obrazových pixelů samotných).



KPKB
KOMORA
PODNIKŮ
KOMERČNÍ
BEZPEČNOSTI
ČESKÉ REPUBLIKY



Příklad zapojení systému KVM over IP.



Na co se zaměřit při výběru řídicího systému?

Jednoznačným trendem v distribuci signálu je přechod na KVM/AV over IP (Keyboard-Video-Mouse/Audio-Video) – to znamená využití standardní ethernetové sítě pro posílání (ideálně) zašifrovaných dat od jejich zdroje k zobrazovači.

Toto řešení má řadu výhod:

- **Flexibilita** – signály lze poslat na více míst, a to pouze za použití standardní, většinou již existující infrastruktury. Kromě hlavního dohledového centra např. do zasedací místnosti nebo krizového centra.
- **Robustnost** – výpadek jednoho ze zařízení znamená ztrátu pouze té části zobrazení, za kterou bylo odpovědné.
- **Škálovatelnost** – systém lze snadno rozšiřovat o další zdroje či výstupy.
- **Přesun technologií z pracovišť** – na pracovištích operátorů jsou pouze „tenci“ klienti, zdroje jsou

soustředěny bezpečně v serverovnách. Z toho vyplývá např. nižší hluk nebo méně generovaného tepla přímo v dohledovém centru.

- **Řešení pro operátory** – vytváří jednotnou pracovní plochu, kdy využívají pouze jednu klávesnici a myš a mají přístup ke všem zdrojům.
- **Bezpečnost** – systém pro distribuci je zcela oddělen od zdrojových systémů.
- **Omezení drahých AV kabelů** – zatímco 50 m CAT6 kabelu stojí v řádu stokrát, 50m optický HDMI kabel určený pro provoz 24/7 se pohybuje v řádech tisíců korun.

Důležité vlastnosti

Robustnost a servis

- určeno pro provoz 24/7
- redundance
- snadnost výměny komponent
- podpora výrobce

Zabezpečení a šifrování

- veškeré signály musí být šifrovány tak, aby je nebylo možné odposlouchávat

- s ohledem na legislativu NIS2 audit logging, Zero Trust Policy, řízení přístupů/identit, šifrování systému samotného
- softwarová podpora a aktualizace
- důvěryhodný výrobce a dodavatel (např. certifikace ISO 27001)

Rychlost systému – běžný uživatel by neměl poznat, že pracuje s KVM zdrojem.

Petr Barták

projektový manažer
dispečerská pracoviště
Nowatron Elektronik, spol. s r.o.

Nowatron Elektronik, spol. s r.o.

Je leaderem na trhu profesionálních zobrazovacích systémů a projekční a prezentační techniky. Dodává jednotlivá zařízení, ale také navrhuje kompletní řešení na klíč. Příklady těchto řešení představují např. školící střediska, konferenční sály, muzea, kongresová a informační centra, sportovní stadiony, reklamní a informační systémy, dispečerská pracoviště, digitální kina, planetária, simulátory, virtuální realita a mnoho dalších. Společnost dlouhodobě udržuje stabilní portfolio dodavatelů a sortiment produktů.

GUANLAN AI

NEJNOVĚJŠÍ TECHNOLOGIE PRO KOMPLEXNÍ OCHRANU MĚKKÝCH CÍLŮ

Společnost Hikvision, světový lídr v oblasti videomonitoringu a AIoT řešení, představila na konferenci Ochrana měkkých cílů 2025 svou nejnovější technologii – Guanlan Large-Scale AI Modely. Zároveň prezentovala ucelený přístup k ochraně měkkých cílů, který pokrývá všechny klíčové fáze bezpečnostního procesu: od odrazení pachatele, přes včasnou detekci hrozby a zpomalení jejího postupu, až po implementaci efektivních reakčních scénářů.

Prevence a odrazení pachatele

Jedním z hlavních prvků prevence je viditelná přítomnost bezpečnostních systémů. Komerční systémy umístěné na strategicky viditelných místech, doplněné o výrazná upozornění na monitorovaný prostor, působí preventivně a mohou odradit pachatele už v počátku jeho činnosti. Dále se využívají výstražné zvukové a světelné signály (jako jsou například stroboskopická světla) a možnost obousměrné komunikace díky zabudovaným mikrofonom a reproduktorům v kamerách.

Včasná detekce hrozeb

Klíčovým faktorem v technické ochraně měkkých cílů je rychlá a přesná detekce hrozeb. Kamery ColorVu 3.0 přesně detekují osoby a vozidla i za špatného osvětlení. Funkce „linkování“ umožňuje sledovat pohyb pachatele mezi kamerami v reálném čase a rychle informovat bezpečnostní složky.

Guanlan AI – nový standard v analýze dat a detekci

V oblasti detekce hrozeb a zpětného dohledávání důkazů představila společnost Hikvision svou nejnovější technologii – Guanlan AI, která posouvá možnosti kamerových systémů na zcela novou úroveň. Tyto rozsáhlé modely umělé inteligence umožňují hlubokou analýzu dat v reálném čase a poskytují nástroje pro efektivní vyhodnocení situací nejen v okamžiku incidentu, ale i zpětně při jeho vyšetřování.

Příklady konkrétního nasazení Guanlan modelů

- **DeepinViewX kamery** – zdvojnásobují rozsah videoanalýzy, snižují falešné poplachy až o 90 % a zvyšují

presnost detekce i v náročných prostředích.

- **Nahrávací zařízení AcuSeek** – vyhledává objekty ve videozáznamech pomocí přirozeného jazyka, například „muž s červenou čepicí“, což výrazně urychluje analýzu. Následně lze výsledky dále třídit podle vizuální podobnosti nebo časového výskytu, čímž se výrazně urychluje a zpřesňuje analýza velkého objemu dat.
- **Termokamery HeatPro a chytré checkpointové kamery** – budou součástí budoucího nasazení. Uživatelé mohou očekávat vysokou přesnost a agilitu při řízení přístupu, kontrole teploty či detekci pohybu v reálném čase.

Případové studie z praxe ochrany měkkých cílů – od sportovních areálů po univerzitní kampusy

Mezinárodní zkušenosti ukazují, jak technologie Hikvision mění přístup k bezpečnosti i efektivitě provozu. V rozlehlém sportovním komplexu Zayed Sports City ve Spojených arabských emirátech byl nasazen komplexní bezpečnostní systém zahrnující chytré kamery a videoanalýzu. Pro účely zpomalení a případného zadržení osob, které nemají mít přístup do prostoru stadionu, a pro detekci podezřelého chování či potenciálních hrozeb byl nasazen rozsáhlý bezpečnostní systém čítající 670 kamer a ANPR systém pro automatické rozpoznávání registračních značek vozidel. Výsledkem bylo zvýšení provozní bezpečnosti, efektivnější správa pohybu osob v celém areálu a rychlejší reakce na incidenty.

Podobně ambiciózní projekt proběhl na jedné z univerzit v Saúdské Arábii, kde byl nasazen integrovaný systém chytrého kampusu s technologiemi Hikvision. Na ploše více než 30 budov bylo instalováno přes 6 000 kamer, přístupové systémy a ANPR technologie pro automatické rozpoznávání značek. Řešení umožňuje včasnou detekci, zpomalení pohybu pachatele a rychlou reakci na incidenty. Inteligentní kamery navíc podporují provozní řízení i výuku,

čímž vznikl moderní kampus – tzv. digitální oáza, kde technologie přirozeně propojují bezpečnost a vzdělávání.

Kybernetická bezpečnost a legislativa

Produkty Hikvision jsou vyvíjeny s důrazem na kybernetickou bezpečnost po celý životní cyklus – od návrhu až po implementaci. Společnost splňuje přísné evropské a mezinárodní normy včetně ISO/IEC 27001, ISO 28000, CSA STAR a také požadavky směrnice NIS2. Společnost Hikvision spolupracuje s mezinárodními monitorovacími organizacemi, aktivně hlásí CVE zranitelnosti a zajišťuje soulad s bezpečnostními standardy i ve veřejném sektoru.

Pro více informací navštivte sekci „kybernetická bezpečnost“ na oficiálních webových stránkách Hikvision: Kybernetická bezpečnost – Podpora – Hikvision Česká republika

Web: Technologie – Hikvision Česká republika

Kontaktujte nás: Prodej – Všechny formuláře – Hikvision Česká republika

Případová studie (UAE): Hra, set a match: Jak přední sportovní komplex Spojených arabských emirátů chrání fanoušky pomocí pokročilého bezpečnostního systému od Hikvision.

Případová studie (SA): Vytváření digitální oázy: Cesta saúdské univerzity k inteligentnímu vzdělávání.

Ing. Kateřina Čihák
Key Account Manager

**CORROSION
RESISTANT+**

"Warning! Private area! No parking!"



Příklad využití obousměrné komunikace díky zabudovaným mikrofونům.

- Trigger Audio Alarm
- Trigger Strobe Light

Ukázka funkcí stroboskopického světla a audioalarmu.



Systém AcuSeek s vyhledáváním „osoby, která kouří a nese kufr“.



Systém AcuSeek s výsledky vyhledávání daného cíle.



Technologie rozpoznávání registračních značek (ANPR) integrovaná do kamer na parkovištích u stadionu. Tento systém zvyšuje bezpečnost a umožňuje efektivní správu parkování. Díky AI může bezpečnostní tým rychle a snadno vyhledávat videozáznamy při vyšetřování nehod a incidentů.

SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ (SŘBI)

Kdo, co, kdy, jak, čím a proč? To jsou (mimo jiné) tzv. kriminalistické nebo analytické otázky. Podle nich se vyučuje už desítky let a ještě dlouho bude. Pojďme se podívat, jestli můžeme tento prehistorický dotazovací set použít také ke zjištění bližších informací k novému zákonu o kybernetické bezpečnosti, tzv. implementačnímu zákonu NIS 2.

Pokud nový zákon o kybernetické bezpečnosti již dobře znáte, dál nečtěte a vrhněte se na jiný zajímavý článek, nebo si dejte kávu a nohy na stůl. Pokud ale stále nemáte jasno, jak na vás nový zákon nebo jiná populární regulace dopadne, čtěte dál. O mnoho stručněji to napsat nelze.

Pokud jsou otázky v nadpisu dobré pro kriminalisty, zpravodajství a analýzu, třeba budou dobré i pro náš účel. A pojďme si na ně odpovědět stručně, v bodech a bez zbytečné omáčky.

KDO je povinen SŘBI zavést a provozovat?

1. Povinné osoby podle zákona (později přibudou další, např. podle zákona o odolnosti subjektů kritické infrastruktury, který bude provádět evropskou směrnici CER¹).
2. Osoby, kterým to bylo uloženo akcionářem/zřizovatelem (např. kraj, město, majitel), oborovou autoritou (např. Úřad pro civilní letectví, Ministerstvo zdravotnictví, Státní úřad pro jadernou bezpečnost, Český telekomunikační úřad, Česká národní banka aj.).
3. Osoby v postavení dodavatele, u kterých to požadují klienti (např. dodavatel softwaru, který dodává povinné osobě nebo jejímu dodavateli).
4. Účastníci zadávacích řízení, pokud je to součástí zadávacích podmínek.
5. Pojištěnci, jestliže pojištění zahrnuje kybernetická rizika nebo to vyžaduje přímo pojistná smlouva.
6. Osoby, které se rozhodnou samy

pro jeho zavedení (u těch nejde o povinnost, ale mnohdy o racionální rozhodnutí zavést standard, který by na konci stejně musely pracně vytvářet).

CO je normativním východiskem SŘBI?

1. nZoKB (NIS2²) – proto se do toho většina z nás pouští.
2. SO 27001³ – norma často vyžadovaná zahraničními partnery.
3. DORA⁴ – specifická oborová regulace.
4. NIST řady 800⁵ – zejména pokud máte co do činnosti s americkými partnery.
5. Zákon o zpracování osobních údajů⁶ – protože v drtivé většině případů jsou údaje zpracovávány v informačních systémech.
6. Interní nebo adoptované standardy, normy, předpisy nebo směrnice – velmi často doplňují zákon a vyhlášky.
7. Stále častěji pojistné podmínky naší pojišťovny.

KDY je povinnost SŘBI zavést?

1. Povinné osoby podle zákona do 3. čtvrtletí 2026.
2. Osoby v postavení dodavatele a účastníci zadávacích řízení dle termínu stanoveného klientem (tedy i podstatně dříve než do 3. čtvrtletí 2026).
3. Ke stejnému zkrácení lhůt jako u dodavatelů může dojít u pojištěnců.

JAK se SŘBI zavede a provozuje?

1. Posouzení motivace a východisek, rozhodnutí, zda a jaký standard bude osoba zavádět.
2. Identifikace a hodnocení primárních (většinou businessových) aktiv.
3. Stanovení rozsahu SŘBI.
4. Identifikace a popis vztahů podpůrných a primárních aktiv.
5. Analýza rizik, návrh opatření, tvorba modelů, klasifikace...
6. Zajištění udržitelnosti.
7. Dosažení souladu a průkaznosti (např. vůči NÚKIB⁷, Policii ČR, pojišťovně, zřizovateli).

ČÍM se nejčastěji SŘBI zavádí a jak se provozuje?

1. Mikropodniky⁸ – těm vystačí pro oblast organizačních opatření kancelářský software, tužka a papír. Technická opatření také nejsou složitá a většinou stačí jedna chytrá hlava.
2. Pro malé podniky jsou většinou nutné pokročilejší nástroje a kvalifikovaný personál nebo externí konzultant.

3. Střední a velké podniky, zejména v režimu vyšších povinností, se neobejdou bez speciálního prostředí a nástrojů, metodik a embedovaných scénářů. Provozování SRBI je pro velký podnik, zejména pro povinnou osobu, pomocí kancelářského softwaru a čtverečkového papíru cestou k velkému bolení hlavy.

Společná pro všechna řešení je nutnost udržovat zavedený systém aktuální, živý a dynamický. Oprášit ho jednou ročně nebo když si vzpomenu – s tím už se podle nového zákona nevystačí.

PROČ zavést a provozovat SRBI?

1. U povinných osob je to zákonná povinnost.
 2. U dodavatelů a pojištěnců je to smluvní povinnost.
 3. U kohokoli ve 21. století je to otázka „přežití“.
- Pokusil jsem se tedy najít stručné od-

povědi na všech sedm kriminalistických otázek. Tyto stručné odpovědi však nepochybně nepostačí ke správnému a důslednému zavedení SRBI. Věřím však, že mohou čtenáři pomoci udělat si přesnější obrázek o směřování k informační a kybernetické bezpečnosti. Ta totiž opravdu není jen zákonnou povinností, ale je především projevem funkčního pudu sebezáchovy. Zeptejte se v nemocnicích, leckde vám budou vyprávět kyber-historky jak od Hitchcocka.

Pamatujte:

- SRBI se netýká pouze povinných osob podle zákona, ale všech, kdo chtějí být připraveni na kybernetické hrozby.
- Implementace musí být provedena povinnými osobami nejpozději do 3.Q 2026, ale v řadě případů je vhodné nebo nutné začít okamžitě.
- Nejčastěji používané normativní

rámce jsou nZKB, NIS2, ISO řady 27000, NIST řady 800 a DORA.

- Základem správné implementace je systematický postup, od identifikace primárních aktiv, přes analýzu rizik, až po zajištění udržitelnosti.
- Dokonce i jednoduché metody (kancelářský software) mohou být účinné, pokud je zvolen systematický a pečlivý přístup.
- Zavedení SRBI je nejen zákonnou povinností, ale nutností k zajištění přežití a odolnosti v kybernetickém prostoru.

Stejně jako řada členů KPKB před vámi nezdráhejte se nám napsat nebo zavolat. Rádi vám naznačíme směr a pomůžeme s prvními kroky.

PaedDr. Martin Uher
martin.uher@arbatas.cz

¹ Směrnice CER (Critical Entities Resilience Directive) – Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti subjektů kritické infrastruktury. Stanovuje pravidla pro zvýšení fyzické a provozní odolnosti kritických subjektů v členských státech EU. Více informací: <https://eur-lex.europa.eu>

² Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti napříč Evropskou unií (Network and Information Security Directive 2). Dostupné z: <https://eur-lex.europa.eu>

³ Mezinárodní norma ISO/IEC 27001:2022 stanovující požadavky na systém řízení bezpečnosti informací (Information Security Management System, ISMS). Více informací: <https://www.iso.org/isoiec-27001-information-security.html>

⁴ Digital Operational Resilience Act (Nařízení EU č. 2022/2554), evropská regulace digitální provozní odolnosti finančních institucí. Více informací: <https://eur-lex.europa.eu>

⁵ Sada dokumentů Special Publication NIST 800 vydávaná National Institute of Standards and Technology, USA. Obsahuje metodické postupy řízení kybernetické bezpečnosti. Více informací: <https://csrc.nist.gov/publications/sp800>

⁶ Zákon č. 110/2019 Sb., česká právní úprava zpracování osobních údajů v návaznosti na evropské nařízení GDPR. Dostupné z: <https://www.zakonyprolid.cz/cs/2019-110>

⁷ Národní úřad pro kybernetickou a informační bezpečnost, ústřední správní úřad České republiky odpovědný za kybernetickou bezpečnost. Více informací: <https://www.nukib.cz>

⁸ Doporučení Komise 2003/361/ES – Doporučení Evropské komise ze dne 6. května 2003 o definici mikropodniků, malých a středních podniků (SME). Stanovuje jasná kritéria pro odlišení podniků podle velikosti (počet zaměstnanců, roční obrát a bilanční suma). Více informací: <https://eur-lex.europa.eu>

DOPORUČENÍ ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ 01/2025

ANEB 20 LET POD DOHLEDEM KAMER

Necelý rok poté, co Úřad pro ochranu osobních údajů (dále již jen Úřad) vydal v únoru minulého roku aktualizovanou podobu tzv. Metodiky k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů (dále již jen Metodika 2024), došlo k rozšíření sbírky dokumentů souvisejících s kamerovými systémy o další materiál.



Jedná se o tzv. Doporučení ÚOOÚ č. 01/2025 ke kamerovým systémům umístěným ve školách a školských zařízeních (dále již pouze Doporučení 01/2025), které bylo přijato dne 15. ledna 2025. Nejen obsahem dvou výše jmenovaných dokumentů, ale i historickým vývojem v této oblasti se budeme zabývat v následujících odstavcích.

Že jsou kamerové systémy nejčastěji nasazovaným „bezpečnostním“ prostředkem ve školách, bez ohledu na druh či stupeň vzdělávacího zařízení, je skutečnost, se kterou jsme se setkali už před vstupem České republiky do Evropské unie. Je ovšem potřeba si popravdě říci, že na způsobu rozhodování o jejich instalaci a následném využívání se toho za více než 20 let moc nezměnilo. A to nejen při pohledu do projektové dokumentace, ale i z hlediska přístupu k pravidlům souvisejícím s ochranou osobních údajů (dále již pouze OOÚ).

Poté, co bez širšího zájmu veřejnosti vyšla pod názvem *Provozování kamerových systémů*¹ v roce 2012 první obšírnější metodika (za kterou si i po dlouhých třinácti letech tým pod editačním vedením Mgr. Bc. Davida Buriana zaslouží poklonu), potkal stejný osud i *Metodiku 2024*.

Ne že by co do obsahu nebyla využitelná, ale ke své i naší smůle jí nepřála atmosféra – zajímavějším tématem než možnost (ne)vhodného nasazení kamer z pohledu OOÚ bylo nejprve používání turniketů, přístupových systémů, součinnost složek PČR a problematika registru střelných zbraní. Nyní, v době vydání *Doporučení 01/2025*², se spíše než vyhodnocení praktických poznatků z nasazování bezpečnostních technologií řeší střety zájmů konzultantů a způsoby čerpání dotací spřízněnými odborníky.

Doporučení 01/2025

Když se na téma kamer v souvislosti s OOÚ podíváme reálným pohledem,

měli bychom si v první řadě přiznat, že pokud by nešlo o školy (obzvláště s přihlédnutím k událostem posledních měsíců), nikdo si *Doporučení 01/2025*, až na právníky a odbornáře, ani nevšimne. Nepřináší totiž nic zásadně nového, spíše jen popisuje stará témata novými slovy.

Berme tedy *Doporučení 01/2025* spíše jako možnost připomenout si *Metodiku 2024* anebo šanci alespoň částečně si zrekapitulovat dvě dekády tohoto tématu. A to nejen s využitím doposud vydaných materiálů *Úřadu*, ale také s příklady z reálné praxe.

Pro ty, kteří téma ochrany osobních údajů sledují z hlediska vztahu ke kamerám jakožto hlavním představitelům tzv. *invazivní techniky* od samotného počátku, nebude obsah dokumentu až tak překvapivý.

První obecná zmínka o kamerových systémech v souvislosti s pořizováním a zpracováváním osobních údajů je

datována do roku 2002. V souvislosti se školstvím o rok později. Abychom začali náš komentář *Doporučení 01/2025* trochu pozitivně, zaměříme se v něm na ty body z jeho obsahu, na nichž se snad všichni, kterých se tato problematika týká, dokážou shodnout.

Záznam

Asi jediným odstavcem textu, u kterého lze potvrdit pravidelný pozitivní posun, je oblast záznamu – myšleno ukládání osobních údajů. A to ať už vlastní délky záznamu nebo místa záznamu.

V *Doporučení 01/2025* je uvedeno, že nezbytná doba uložení kamerových záznamů musí být správcem stanovena, zdůvodněna a zdokumentována jako nezbytně nutná pro zajištění účelu. To žádné novum pochopitelně není, ale skutečnost, že je zde popsáno možné stanovení délky záznamu v závislosti na způsobu provozu, to už novum je. Uvedený příklad s odlišnou dobou pro běžný provoz (týdenní záznam) a s jinou pro specifické účely školního roku (až 3 týdny v době letních prázdnin) lze použít jako vzor i mimo školní prostředí.

P ř e d příchodem GDPR (a tedy v době bez kovaných právníků s alibistickým přístupem) jsme z pozic konzultantů v rámci odpovědi Úřadu podobně úspěšně obhajovali obdobné termíny u přepravních firem – od naložení vozidla do jeho vyložení přepravcem v cílovém místě. Tři dny u krátké trasy, deset dní u komplikovanější. Dnes, kdy už má de facto každý nějaké to ISO, v rámci něhož jsou podobné procesy popsány, si případně může vypomoci provázáním potřeb delšího záznamu a povinností ochrany dané interní směrníci.

Poznámka: v souvislosti s délkou záznamu připouští *Metodika 2024* ve znění odstavce 3. 1. 5 (Nezbytně nutná doba uložení záznamů) jako přijatelnou dobu záznamu 72 hodin.

S dobou záznamu přímo souvisí i lhůty vyplývající z pravidel pro předávání zpracovávaných údajů oprávněným subjektům (pro následující popis si oprávněné subjekty zůžeme na orgány činné v trestním řízení – tedy kompetentní zástupce PČR).

Obdrží-li správce žádost o poskytnutí záznamu z kamerového systému, pak

se dle *Metodiky 2024* považuje jako přiměřená doba pro poskytnutí záznamu lhůta 1 měsíce od obdržení žádosti. O tuto dobu si tedy správce může legálně prodloužit délku záznamu. Ovšem ačkoli se takovéto navýšení může zdát dostatečné, ne vždy bývá související proces ve lhůtě naplněn. Je tedy potřeba brát v potaz i dobu, kterou mají k dispozici orgány činné v trestním řízení. Tedy další možné legální prodloužení.

Za zmínku také stojí specifická možnost, kterou *Metodika 2024* připouští (viz odstavec 3.3.2.2 písmeno b). Ta v případě, že v obsahu dohledaného záznamu žádosti zjistí závažné skutky, správci umožňuje, aby poskytl kompetentním orgánům záznamy z vlastního rozhodnutí.

Pokud jde naopak o možnosti správce, jak se bránit opakovaným neopodstatněným žádostem, je zde právo na přiměřený poplatek. Toho lze využít při nepřiměřených nebo na první pohled neodůvodněných žádostech. Jen je možná škoda, že u původní formulace z roku 2021 „Za poskytnutí kamerových záznamů subjektu údajů má správce právo žádat přiměřenou úhradu nákladů spojených s poskytnutím kamerového záznamu“ došlo k posunu využití této možnosti až na žádost o poskytnutí druhé a další kopie.

Co se týká místa záznamu, doufejme, že zvítězí zdravý rozum a z diskutovaných variant (lokálně na paměťových zařízeních správce/školy, lokálně na paměťových zařízeních zpracovatele – například bezpečnostní služby, vzdáleně s využitím cloudových služeb) pad-

mého počátku. *Doplňující formulář pro oznámení zpracování osobních údajů kamerovými systémy* obsahoval v rámci popisu opatření k zajištění požadované ochrany osobních údajů i konkrétní výčet přijatelných možností. Z technických uvedme například zámky, mříže, elektronické zabezpečení, ale také nastavení přístupových práv či využívání antivirové ochrany. Z organizačních se jednalo o směrnice a dokumentaci. Stačilo jen zaškrtnout a závazek pochopitelně i splnit.

Využití bezpečnostní služby, ať už soukromého komerčního subjektu anebo městem provozované obecní policie, je sice na první pohled jednodušší. Ušetříme za zámek a zamřížovaná místnost nebude nikoho děsit. Ale jde o zapojení dalšího subjektu, což může být (například kvůli častým změnám na vedoucích postech) větší komplikací, než se na první pohled zdá. Nicméně případné dohody mezi obecní policií a státní školou či jejím zřizovatelem by nic bránit nemělo. Většina z nich už je stejně napojena na bezplatné obecní dohledové pulty, a jestliže už „měšťáci“³ zvládají sledovat desítky kamer z panelových a bytových domů, proč ne taky ze škol.

A proberme ještě třetí možnost – využití cloudových služeb. To, že se kybernetické útoky pomocí tzv. „zadních vrátek“ kamerových systémů neřeší mediálně, neznamená, že se to neděje. Chtělo by se říci, že škola není nemocnice a (doposud) ani objektem kritické infrastruktury. Anebo že jde o uzavřené systémy.

Když ale připustíme, že každá techno-



ne volba na první či druhou z nich. Lokální záznam sice přináší i technické a organizační zabezpečení místa, nejčastěji místnosti, ale to tu bylo od sa-

logie s připojením na internet je otevřená a že do škol se nejčastěji instalují ty nejlevnější kamery, pak v kombinaci se stavem digitalizace škol (viz libo-

volná tematická nebo výroční zpráva České školní inspekce) je toto řešení časovanou bombou.

Základní ochranné funkce kamer (nejen ve školách)

V obsahu *Doporučení 01/2025* je v souvislosti s popisem základních ochranných funkcí kamer uvedeno, že správci osobních údajů si od instalace kamerového systému slibují tři základní ochranné funkce – preventivní, reaktivní a důkazní.

Když vynecháme čtvrtou (o níž se nejen nepíše, nemluví, ale jen šeptá), kterou je aktivní využití analytických funkcí, pak popravdě řečeno, co taky jiného od kamerových systémů očekávat? Vždyť kamery a kamerové systémy (v podobě, jak je posledních 25–30 let známe) jsme si do této pozice povýšili sami. Z původně cenově nedostupné technologie používané pouze v podporné roli ve specifických situacích (banky, armáda, doprava) se kamery postupně staly běžnou součástí našeho každodenního života.

Pro další komentáře se nám v těchto souvislostech hodí srovnání s prvním tuzemským celostátním projektem „kamerové invaze“, kterým byl ve zlatých devadesátkách dotační projekt MVČR na zřízení MKDS (městských kamerových a dohlížečích systémů). Jeho výsledkem byl odliv policistů z ulic, a ačkoli na pokles kriminality měly výraznější vliv jiné okolnosti, je tento projekt i přes změnu donora aktuálně ve fázi (opět plošné) digitalizace a automatizace.

I zde probíhala v prvních letech polemika o výše zmíněných třech základních funkcích kamer (viz stanoviska ÚOOÚ z prvních let platnosti zákona č. 101/2000 Sb.). A ačkoli dnes kamery určené pro dohled na veřejných prostranstvích v rámci *digitalizace*⁴ mají v obsahu výběrových řízení jako jednu z nosných podmínek i tu čtvrtou (výše zmíněnou) základní ochrannou funkci, už se nad tím nikdo nepozastavuje.

Na to, zda kamery vybavené zmíněnými funkcemi umožní výrazně rychlejší reakci na různé kritické situace (v současnosti jsou kromě mediálně nejprobíranější detekce palných zbraní v souvislosti s oblastí školství nejvíce aktuální například detekce rvaček, vandalismu, křiku, chladných zbraní nebo nestandardního chování), nám odpoví vývoj několika příštích měsíců. Tvzení, že kamery (ne) plní preventivní funkci a díky nim (ne) dochází k reálnému odrazení pachatele od nežádoucího jednání, je a bude i nadále diskutabilní.

Nejedná se zatím o žádný všudypřítomný „pre-crime“ („předzločin“ – myšlenka, že výskyt trestného činu lze předvídat dříve, než k němu dojde), ale o využití dostupného. Nemusí se nám to líbit, ale nějak to už je ve 21. století normální – prostě to přišlo s dobou. A ten, kdo sleduje problematiku K-12⁵ na západ od Evropy, by někdy mohl i napovídat.

A ano, mimořádné situace tím se vši pravděpodobností nezabráníme. Ale v době, kdy nestojí na každém rohu strážný, prostě nic reaktivnějšího k dispozici není.

Škola jako součást kritické infrastruktury?

Tolik první stručný komentář k letošnímu lednovému doporučení Úřadu k oblasti OOÚ. Ne, že by se jím někdo v reálném světě řídil. Ve školách je stále prioritou pololetní vysvědčení, pak jarní prázdniny, přijímací zkoušky, jejich vyhodnocování atd. – a najednou ukončení školního roku a konečně prázdniny, během kterých se snad alespoň na některých školních objektech podaří rekonstrukce elektroinstalace, střechy nebo oken. To jsou priority. Školám by snad jen pomohlo, kdyby byly součástí kritické infrastruktury. Ostatně co jí dnes, v době, kdy vše souvisí se vším, vlastně není.

Zatím si však toto spojení dala do názvu jen jedna z nových asociací – **Asociace škol kritické infrastruktury**, z.s. (založená roku 2022). Ovšem zda svou činností povýšila svou skromnou Asociaci bezpečná škola z.s. (založenou roku 2016), ukáže nejspíš až čas. Slevové programy pro své členy však mají obdobné. Ale i tak je na místě oběma držet palce, protože když už nic jiného, pak se o bezpečnostních tématech alespoň více mluví.

Na ostatní body rozepsané v *Doporučení 01/2025*, ať již jde o evergreen pod názvem „míra omezení zásahu do soukromí“ či novinku loňského roku, tzv. balanční test (schválně, už jste si ho někdo na své škole zkusil?), se bude vhodnější podívat přímo do zdrojového materiálu – tedy do polozapomenuté *Metodiky 2024*.

Poznámka závěrem

Nejspíše však dojdeme k závěru, že splnit požadavky dané zákonem či vyhláškou se bude vždy někomu zdát nedostatečné. Jako čerstvý příklad můžeme použít informaci o řešení konkrétního kamerového systému v konkrétní škole, o kterém informuje ÚOOÚ ve své poslední Výroční zprávě (ZV-2024, zveřejněné 25. 3. 2025)⁶. Na straně 27 tohoto

dokumentu je v odstavci **Kamerový systém se záznamem na základní škole uvedeno:**

„ÚOOÚ se zabýval dotazem ohledně kamerového systému se záznamem užívaným ve školním zařízení. Konkrétně se jednalo o umístění kamer v odborných učebnách, přičemž žáci a zaměstnanci podepsali souhlas se zpracováním obrazového i zvukového záznamu v rámci školy. Ve své odpovědi Úřad zdůraznil okolnost, že v praxi zpravidla považuje kamery umístěné v učebnách školy za nepřiměřené oproti zájmům a základním právům a svobodám dotčených subjektů údajů. Dále Úřad upozornil, že provádět předmětné zpracování na základě souhlasu také obvykle nepovažuje za vhodné. Pro faktickou nerovnováhu mezi školou a subjekty údajů lze totiž pochybovat o dobrovolnosti udělení, rovněž odvolatelnost souhlasu v kontextu účelu předmětného zpracování je snadná.“

Michal Randa

redaktor oborů Bezpečnost
a Elektrotechnika / portál TZB-info

Poznámky, zdroje a literatura

¹ Provozování kamerových systémů – metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů (ISBN 978-80-210-6017-3); zdroj www.uoou.cz.

² Doporučení ÚOOÚ č. 01/2025 ke kamerovým systémům umístěným ve školách a školských zařízeních; zdroj www.uoou.cz.

³ „měštáci“; hovorový výraz pro pracovníky městských a obecních policí.

⁴ Digitalizace; jeden ze základních pilířů rekonstrukce kamerových systémů k naplňování tzv. Specifického cíle E.4 „Efektivně rozvíjet využívání městských kamerových a dohlížečích systémů (MKDS) za účelem zvyšování bezpečnosti a prevence kriminality“ dle Implementačního plánu Strategie prevence kriminality v České republice na léta 2022 až 2027. V letech 2016–2021 došlo v rámci cca 300 rekonstrukcí prvků MKDS k modernizaci přibližně ve 100 obcích a městech, přičemž témata typu „Pokročilá / inteligentní analýza“ byla součástí osmi žádostí o dotaci a „Modernizace / digitalizace / zkvalitnění záznamu“ součástí přibližně devadesáti žádostí o dotaci. Zdroj: Strategie prevence kriminality na webech MVČR.

⁵ K-12; anglický jazykový výraz, který označuje rozsah let veřejně podporovaného základního a sekundárního vzdělávání ve Spojených státech a Kanadě. Zdroj: wikipedia.org.

⁶ Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2024; zdroj www.uoou.cz.

HISTORIE A SOUČASNOST KONSTRUKCE A POUŽÍVÁNÍ PASIVNÍCH A POLOPASIVNÍCH SYSTÉMŮ

PROSTOROVÉHO ODPOSLECHU (2. ČÁST)

První zařízení tohoto projektu – EC1 nebylo spuštěno do sériové výroby, protože zadavatel požadoval větší dosah a odstranění standardní amplitudové modulace. NRP proto vyvinula v roce 1962 variantu EC Mark 5. Ta svou cylindrickou konstrukcí umožňovala velmi dobře zakamuflovat EC Mk5 do nábytku, do součástí stavebních konstrukcí i výzdoby interiéru. Použitá modulace byla již FM a pro maskování zvukového signálu byl použit systém se subnosnými prvky.

Pro potlačení tohoto paradoxu bylo navrženo použití vlastního zdroje napájení, tedy baterie. Navíc byl použit FET tranzistor na koncovém stupni retroreflexního vysílače. Tím vznikla skupina ZTP označená v 1. části článku (v minulém čísle BsP) jako PPASE (skupina zařízení polopasivních neboli také poloaktivních, jež mají na rozdíl od PASE i napájecí zdroj – baterii).

International Ltd.). V čele společnosti stál Lee Tracy, který v roce 1978 odešel z MI6 a neváhal využít svých zkušeností k vytvoření komerčních produktů.

PPASE SABRE:

Frekvence budicího vysílače:
885,500 MHz

Výkon budicího vysílače:
10 až 100 mW

Frekvence odraženého signálu:
885,625 MHz

Rozměry jednotky přijímače s vysílačem:
158 x 85 x 290 mm

Váha jednotky přijímače s vysílačem:
4 kg

Rozměry ARRS jednotky:
30 x 9 x 133 mm

Váha ARRS jednotky s bateriemi:
34 g

Provozní doba jednotky ARRS, bez výměny baterií: 15 měsíců

Přijímací anténa: YAGI

Vysílací anténa: YAGI

V souvislosti s tím bych se rád zmínil o systému PPASE vyvíjeném od počátku 70. let 20. století v ČSSR na pracovišti bývalé 6. správy SNB, následně Technické správy bývalého Federálního ministerstva vnitra. Již se značným odstupem času a na základě porovnání mohu konstatovat, že toto pracoviště v bývalé ČSSR patřilo díky výzkumu, vývoji a výrobě techniky pro potřeby tehdejší rozvědky a kontrarozvědky mezi světovou třídu. Když nepočítám sovětskou KGB, pak ČSSR systém PPASE jako jediná služba z tehdejších států Varšavské smlouvy samostatně vyvíjela a vyvinula. Práce na dalším zdokonalování skončily



Obr. 7 ZTP Easy Chair EC Mk5. ⁹



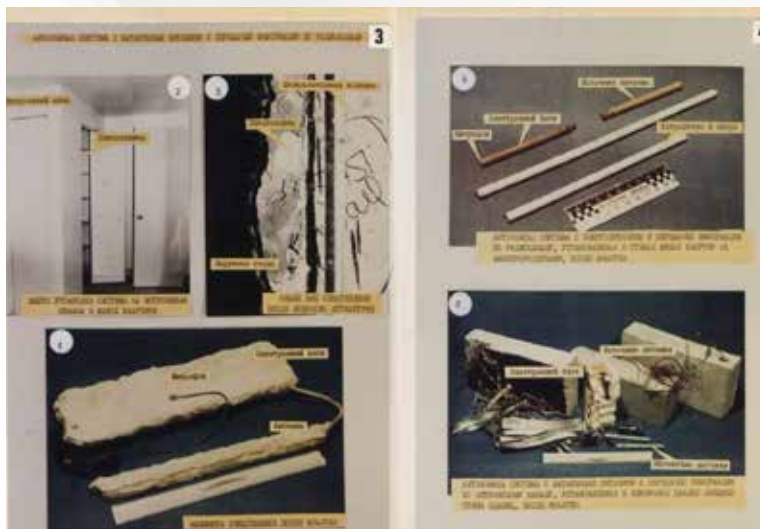
Obr. 8 Sestava systému SABRE (vlevo centrální jednotka a vlastní ZTP, vpravo opěrný bod). ¹⁰

Použití elektronických obvodů v PASE ale nevyhnutelně vedlo ke zvýšení „odebírané“ části energie budicího signálu, a tudíž k nutnosti zvýšení úrovně signálu vysílače. To paradoxně vedlo ke zvýraznění první demaskující vlastnosti.

Jedním z příkladů, který odpovídá úrovni například britského speciálního vybavení na přelomu 70. a 80. let 20. století může být systém SABRE. Vyráběla jej společnost Security Research (Audiotel

po převratu – v roce 1990. V roce 2024, kdy tento článek píšu, slaví hlavní vývojový pracovník tohoto ARRS 90 let.

internetu. Podívejme se nyní na modernější systémy používané americkou NSA. Díky



Obr. 9 Ukázka částí dokumentu „Zařízení pro tajné shromažďování informací identifikované v budovách sovětských misí ve Washingtonu, D.C.“¹¹

V odborných zpravodajsko-technických kruzích Varšavské smlouvy bylo známo, že mezi lety 1969 až 1978 provedla zpravodajská služba KGB SSSR operaci Ikarus, během níž byla identifikována, analyzována a katalogizována odposlechová technika Ústřední zpravodajské služby CIA a kontrarozvědných jednotek Federálního úřadu pro vyšetřování (FBI), která byla zjištěna v sovětských institucích ve Spojených státech. Spis s názvem „Zařízení pro tajné shromažďování informací identifikované v budovách sovětských misí ve Washingtonu, D.C.“ byl zaslán i bezpečnostním službám zemí bývalé Varšavské smlouvy a já jsem měl možnost se s ním v 80. letech minulého století seznámit.

odhalení Edwarda Snowdena (v prosinci 2013) dostala veřejnost k dispozici objemný, veřejně přístupný katalog velmi zajímavých elektronických odposlouchávacích nástrojů, které NSA používá. Stal se mimo jiné i inspirací pro radioamatérskou výrobu a přispěl k další komercializaci této oblasti.

Rozšířená je skupina ARRS sady „Angryneighbor“. Její centrální jednotkou je jednotka označená jako CTX4000, což je přenosná radarová jednotka s kontinuálním signálem (CW). Používá se jako přijímací a vysílací zařízení pro prostředky ARRS a pracuje v pásmu 1...2 GHz. Spolupracuje s celou škálou prostředků pro odposlech hovorů, klávesnic, PC,

šířenou šířkou pásma do 450 MHz. Stojí přibližně 40 000 USD. Photoanglo byl společný projekt NSA a britské GCHQ¹³ na vývoji radarového systému nové generace. Používá antény různých typů – rohové, spirálové, parabolické, logperioidické. Část signálu vysílače se používá jako heterodyn (oscilátor v přijímači, jehož frekvence se směšuje s frekvencí přijímaného signálu). K videovstupu se doporučuje připojit standardní zařízení. To je součástí programu s názvem COTS (Commercial Off-The-Shelf), což je komerční hotové vybavení, tedy zařízení, které je připraveno k použití. Účelem je to, aby se maximálně využilo komerčně dostupných komponentů. Začlenění širokého spektra komerčně užívaných komponentů do speciální techniky umožňuje dosahovat prakticky neomezených možností modernizace, rozvoje a rozšíření, tak aby splňovaly budoucí požadavky. V první řadě se to týká aplikace různých typů modulační přenosných signálů.

Jedním ze ZTP pro prostorový odposlech patřících do sady „Angryneighbor“ je prostředek s kódovým označením Loudauto. Je to typický představitel ZTP skupiny PPASE. Byl vyvinut v roce 2007 v péči americké NSA.

Citlivý mikrofon EK/EY (komerčně dostupný a levný mikrofon firmy Knowles pro naslouchadla) umožňuje poslouchat hovorovou konverzaci v místnosti na vzdálenost cca až 6 metrů. Tento ZTP je napájen baterií o napětí 3 V a spotřebovává tak málo energie, že samovybíjecí proudy akumulátoru mohou být větší než provozní proud odebíraný zařízením. Délka je asi 1,5 cm bez napájecího modulu. ZTP je aktivováno budičím signálem o frekvenci 1 až 2 GHz. Analogový zvuk z mikrofonu je převeden na digitální signál pomocí pulzní polohové modulační (PPM). Tato modulace je značně rozšířena v komerčních výrobcích, např. v komunikaci bezkontaktní čipové karty dle ISO/IEC 15693 a také pro implementaci RF protokolu elektronického kódu výrobku třídy 1 pro štítky RFID. Komponenty pro toto zařízení je možno zakoupit v řádu stovek Kč. V mnoha ohledech lze systém Loudauto považovat za další vývoj již zmíněného programu CIA – Easy Chair. Velmi zjednodušeně lze principiální schéma prostředku Loudauto nakreslit následovně (viz obr. 12).

Zvuk přichází na standardní miniaturní mikrofon, je zesílen a filtrován. Analogový signál z mikrofonu se přivádí na vstup polohového modulatoru (PPM). Celý proces může být softwarově snadno implementován v malém standardním průmyslovém mikrokontroleru.

Obecně Loudauto připomíná poněkud primitivní variantu poloaktivních (polopasivních), dnes hojně používaných RFID identifikátorů (karet, přívěsků, štítků) v různých průmyslových odvětvích.

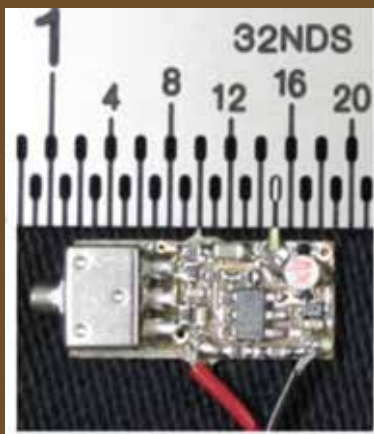


Obr. 10 Centrální jednotka CTX 4000.¹²

Tento dokument podrobně popisoval řadu různých druhů ZTP CIA a FBI nalezených v sovětských diplomatických budovách a zařízeních ve Washingtonu, D.C., v New Yorku a San Francisku, rekreačním komplexu ve vlastnictví Sovětského svazu, v bytech a automobilech sovětského diplomatického personálu. Tento materiál je dnes možno najít na

obrazu, datového provozu atd. Vysílací výkon budičím signálu je 2 W, s externím zesilovačem až 1 kW. Šířka pásma až 45 MHz.

Od roku 2009 je jednotka CTX4000 postupně nahrazována modernější verzí Photoanglo. Ta se vejde do malého kufříku. Frekvenční rozsah je rozšířen do 4 GHz, výkon již jen 2 W, ale s roz-



Obr. 11 ZTP Loudauto.¹⁴

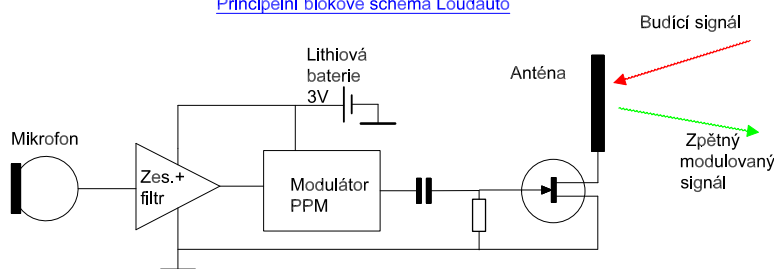
Pro připomenutí, RFID (Radio Frequency IDentification) je metoda automatické identifikace objektů, při níž se pomocí rádiových signálů čtou nebo zapisují data uložená v tzv. RFID transpondérech, respektive ovladačích. Pro provoz na vzdálenost větší než 10 metrů jsou tyto výrobky obvykle naladěny v pásmu 900 MHz, ale přesná pracovní frekvence závisí na ladění přijímací antény RFID. V daném případě není přílišným problémem dostat se s vyladěním do kmitočtového rozsahu jednotky CTX4000B nebo Photoanglo.

zlatá medaile na Sensors Expo & Conference 2014 v Kalifornii).

Zvyšování frekvenčního rozsahu na 4 GHz u Photoanglo umožňuje NSA využívat velké množství snímačů RFID pracujících v pásmu 2,4 GHz, které jsou k dispozici na komerčním trhu. Podle mého názoru nejen americká zpravodajská služba prostě nemůže nevyužít této možnosti k rozšíření svého arzenálu, zejména proto, že vzhledem k množství různých zdrojů rádiového vyzařování v tomto rádiovém pásmu, je poměrně snadné se v tomto rádiovém pásmu ukrýt. Tento proces zároveň odkrývá možnosti v již zmíněné komercializaci využívání této techniky v rámci nelegálního konkurenčního, a nejen konkurenčního zpravodajství.

Ing. Karel Hříbal, CSc.

Principiální blokové schéma Loudauto



Obr. 12 Principiální blokové schéma ZTP Loudauto.¹⁵

Navíc možnosti komerčních RFID identifikátorů stále rostou. Již nejsou jen pasivními, ale i poloaktivními senzory, dokonce i plnohodnotně aktivními, které díky vlastnímu napájení mají i některé „chytré“ schopnosti. Novější varianta standardu RFID předpokládá existenci několika tříd transpondérů, které se liší rozsahem rádiových frekvencí a komunikačními schopnostmi.

Počínaje třídou 3 a vyšší jde o poměrně složitá zařízení, která jsou však poměrně snadno realizovatelná pomocí hotových IOPF, jako je nebo spíše byl čip SL900A od společnosti AMS. Jedná se o integrovaný obvod, který splňuje požadavky dokumentu EPC Gen2 (EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID) Class 3. Je navržen tak, aby vytvářel pasivní nebo polopasivní RFID transpondéry třídy 3 UHF (860...960 MHz). Přičemž pro různé aplikace vyžaduje připojení minimálně externích součástek. Například pokud nahradíte externí teplotní čidlo mikrofonom, získáte docela slušný odposlechový prostředek s mnohem většími možnostmi než Loudauto. A to je třeba poznamenat, že SL900A není v žádném případě poslední výkřik rozvoje (2014 –

Zdroje a poznámky k článku:

⁹ Výchozí obrázek: <https://www.cryptomuseum.com/covert/bugs/ec/ec5/index.htm>; překlad popisů a vlastní nákres.

¹⁰ Archiv autora článku.

¹¹ <https://thebrushpass.projectbrazen.com/coldwarbuggingsovietunion/>.

¹² <https://www.slideshare.net/slideshow/ant-catalog/253873898>; https://www.eff.org/files/2014/01/06/20131230-appelbaum-nsa_ant_catalog.pdf.

¹³ GCHQ (Government Communications Headquarters) – vládní komunikační centrum Spojeného království je zpravodajská služba odpovědná za provádění radioelektronické rozvědky a poskytování ochrany informací vládě a armádě; je součástí Společného výboru pro zpravodajské služby, a to společně s MI5 („vnitřní rozvědka“) a MI6 („vnější rozvědka“).

¹⁴ <https://www.slideshare.net/slideshow/ant-catalog/253873898>; https://www.eff.org/files/2014/01/06/20131230-appelbaum-nsa_ant_catalog.pdf.

¹⁵ Nákres autora článku.

NOVÉ MOTOCYKLY

U POHOTOVOSTNÍ MOTORIZOVANÉ JEDNOTKY

V červnu letošního roku převzala Pohotovostní motorizovaná jednotka (PMJ) Krajského ředitelství Policie ČR do své výbavy motocykly BMW F 900 GS Adventure.



Proč PMJ pořídila právě tyto motocykly a jakou mají výbavu?

Pro odpovědi na tyto a další otázky jsem se vypravil na základnu PMJ v Praze v Ďáblicích. Jako motorkáře a uživatele motocyklu stejné značky mě zajímalo, z jakého důvodu si jednotka vybrala právě tyto stroje. Také jsem byl zvědavý, jak se povedlo sloučit motorkářské a policejní vybavení, aby byla zajištěna bezpečnost policisty při jízdě na motocyklu, a zároveň nebyla ovlivněna schopnost provést potřebný zásah.

Po příjezdu do areálu PMJ se mě ujal zástupce vedoucího odboru PMJ mjr. Mgr. Josef Jeřábek, se kterým jsem se bavil o vybavení a výcviku policistů, kteří jezdí na nových motocyklech této jednotce přidělených. Představil mi osobně

dva policisty (Dominik a Richard), kteří na těchto strojích jezdí. Ti mi prozradili, že jsou motorkáři i v civilu. Jak jsem se později dověděl, zkušenosti s řízením motocyklu v civilu jsou také podmínkou pro přidělení služebního motocyklu policistovi sloužícímu u PMJ.

Co je PMJ?

Pohotovostní motorizovaná jednotka (PMJ) je specializovaný policejní útvar, který se zaměřuje na rychlou reakci na tísňová volání a situace vyžadující okamžitý zásah. Hlavním cílem jejich činnosti je ochrana životů a zdraví osob, majetku, odhalování trestné činnosti, pátrání po hledaných osobách, vozidlech a odcizených věcech.

PMJ vznikla 1. července 1956 pod tehdejšími názvy **Speciální pohotovostní jednotka (SPJ)**. Postupem času jednotka změnila název – od roku 1965 byla označována jako Pohotovostní jednotka (PJ) a v roce 1978 dostala název **Pohotovostní motorizovaná jednotka (PMJ)**, který používá dodnes.

Současnou základnu pražské PMJ je areál ve starých Ďáblicích, v osmém pražském obvodu. Denně odsud do ulic metropole vyjíždí hned několik dvoučlenných či trojčlenných hlídek. Na každou městskou část hlavního města dohlíží většinou dvě až čtyři hlídky PMJ, a to nepřetržitě. Služební vůz PMJ poznáte podle malého žlutého reflexního trojúhelníčku, který je umístěný na zadním a předním skle vozidla, vždy v levém horním rohu.

Motocykly u PMJ

Vzhledem k často velmi složité dopravní situaci v centru města, kdy není jednoduché dostat se rychle k místu události vozidlem, nabízí se využití motocyklů. Tato myšlenka není nijak nová, motocykly byly ve výbavě PMJ již krátce po jejím vzniku, v šedesátých letech. Tehdy se jednalo o československé stroje Jawa 500 OHC a sovětské M72.

Aby motocykly vyhovovaly všem dnešním potřebám PMJ – zvládly přejet například vyšší obrubníky, uměly se pohybovat v lehkém terénu a zároveň byly dostatečně výkonné a agilní v městském provozu – zvolila policie speciálně navržený model BMW F900 GS Adventure. V současné době jsou policisté vybaveni v rámci zkušebního provozu třemi těmito motocykly. Pokud se projekt osvědčí, mají v plánu jejich počet navýšit na 10–12 kusů.

Proč právě značka BMW? Tento výrobce má již bohaté zkušenosti s výrobou modelů motocyklů přímo pro policejní účely. Například ergonomii ovládacích prvků má zvládnutou daleko lépe než jiní výrobci. Model F900 GS Adventure byl zvolen pro ideální poměr výkonu a hmotnosti pro provoz ve městě či v lehkém terénu, jako jsou parky nebo zalesněné plochy na území hlavního města Prahy.

Systém motocyklové hlídky je obdobný jako u hlídky automobilové – tzn. zásah provádějí nejméně dva policisté, aby si mohli při zákroku poskytnout vzájemné krytí. Každý policista přitom jezdí na své motorce. Z podstaty činnosti PMJ, kdy má jít o rychlý zákrok na místě události, jezdí vždy společně dvě motorky, což je rozdílem oproti službě dopravní policie, kdy můžete na motorce potkat i policistu samotného.

Výbava policisty na motorce

Z hlediska motocyklové výbavy používají policisté překlápňovací přilbu LS2 (LS2 Advant X) se dvěma interkomy. Jeden interkom je napojený na mobilní telefon a prostřednictvím technologie Mesh slouží i ke vzájemné komunikaci mezi jezdci. Druhý interkom slouží pro komunikaci s operačním střediskem. Oproti dopravní policii nemají policisté vysíláčky na motorce, ale na sobě, protože motocykl je pro ně jen prostředek k přesunu na místo zásahu a spojení musí mít zajištěno i mimo motocykl. Policista na motorce je oblečený do černých kevlarových kalhot Street Racer. Na horní polovinu těla nosí policisté chrániče (Zandona Action X7) s ochrannou páteří s protektory D3O i na ramenou a loktech, které při případném nárazu ztuhnou, zpevní se a poskytnou vysokou míru ochrany. Na chrániči těla mají policisté dres v policejních barvách se standardním označením policistů a nosič balistických plátů s dalším potřebným vybavením, jako je teleskopický obušek, nůž, Taser X26, IFAK, osobní kamera a zásobníky do krátké zbraně. Krátkou zbraň Glock 17 se svítlnou Streamlight nosí policisté ve stehenním pouzdře.

Výběr vhodné obuvi byl velkým oříškem. Vybrat boty, které poskytují kvalitní ochranu pro jízdu na motorce a zároveň umožňují policistům běhat či používat donucovací prostředky, nebylo jednoduché. Nakonec byla vybrána obuv značky Forma Adventure Low WP.

Vybavení v kufrech obou motocyklů není totožné, jak by člověk mohl před-

pokládat. Díky tomu, že jezdí vždy dva motocykly společně jako tým, navzájem se výbavou doplňují. Výbava obsahuje ledvinku s prostředky první pomoci (zejména na zástavu tepenného krvácení), házečí pytlík na vodu pro záchranu tonoucího, transportní plachtu na přenos zraněného, automatizovaný externí defibrilátor (AED), alkohol tester, drogové testy DrugWipe, prostředky k označování překážek v provozu (sprej), pásku Policie a věci osobní potřeby.

Motoroky jsou dále vybaveny modročervenou signalizací v přední části a modrým teleskopickým majákem v zadní části. Světelný nápis POLICIE / STOP má motocykl vpředu i vzadu.

Aktuálně se řeší také uložení dlouhých zbraní na motocyklu. Z dlouhých zbraní používá PMJ samopal Heckler & Koch MP5 a útočnou pušku Heckler & Koch G36. Na motocykly se počítá se zbraní typu PDW, konkrétně Heckler & Koch MP7 – což je zajímavý kompromis mezi samopalem a útočnou puškou.

Jak jsem zmínil v úvodu – podmínkou pro přidělení služebního motocyklu policistovi PMJ jsou jeho předchozí zkušenosti s řízením motocyklu v civilu. Jezdit na motorce v náročném městském provozu není rozhodně nic jednoduchého, navíc pokud je nutné se dostat na místo zásahu co nejrychleji. Naštěstí jsou řidiči motocyklů u PMJ zároveň vášnivými motorkáři a věřím, že to mají v hlavě dobře srovnané – jinak by ani nemohli být příslušníky tohoto prestižního útvaru. Samozřejmě si svoje motocyklové dovednosti zvyšují i v rámci služební přípravy. Motorkáři u PMJ využívají endurovou školu nedaleko Benešova u Prahy pod vedením zkušených trenérů Kuklíků.

Vyplatí se motocykly u PMJ?

Podle slov zástupce velitele PMJ je nej-

větší devizou motocyklů rychlý dojezd na místo zásahu na území hlavního města Prahy. Vzhledem ke komplikované dopravní situaci v Praze se rychlost dojezdu na motocyklu nedá s automobilem vůbec srovnávat, a to ani v případě, kdy automobil jede na majáky – policista na motocyklu bude na místě zásahu vždy dříve než jeho kolega v autě. Nehledě na možnost motocyklu překonávat obrubníky, schody či se pohybovat v úzkých uličkách, průjezdech nebo mimo silnici, kam se běžné služební vozidlo typu Škoda Kodiaq nedostane. Právě čas může být při některých typech zásahů (např. aktivní střelec, masivní krvácení, srdeční zástava) klíčovým faktorem, který může rozhodnout o jeho úspěšnosti.

Bc. Petr Žák

Jednou stopou Českem, z.s.



SPOLEČENSKÁ ODPOVĚDNOST A ETICKÉ KONCEPCE UPLATNITELNÉ V PROSTŘEDÍ MALÝCH A STŘEDNÍCH FIREM V KONTEXTU VLIVŮ A DOPADŮ PANDEMIE COVID-19 (2. ČÁST)

Pro budoucí růst dané firmy a potenciál jejího růstu jsou rozhodné klíčové faktory manažerského řízení a rozhodování v organizaci.

Jednotlivé faktory, které jsou relevantní, se týkají jak osob vlastníků a manažerů, tak samotné podnikatelské činnosti, konkrétně jde o:

- Finanční zdroje a jejich vytváření a redistribuci v dané firmě.
- Personální zdroje firmy a jejich efektivní využití pro jednotlivé úrovně řízení i pracovní pozice.
- Systémové zdroje firmy, pokud jde o stupeň propracovanosti jak informačních, tak plánovacích a kontrolních systémů.
- Obchodní zdroje firmy, včetně vztahů se zákazníky, podílu na trhu, vztahů s dodavateli, výrobních a distribučních procesů, technologií a pověstí, které firmě zajišťují postavení v segmentu komerční bezpečnosti.

Čtyři faktory, které se vztahují k vlastníkově daného podniku, případně managementu jednotlivých oddělení v organizaci podniku, jsou definovány následovně:

- Strategické cíle vlastníka dané firmy, jeho osobnostní předpoklady i formulace korporátní strategie malé a střední firmy obecně.
- Operativní schopnosti vlastníka firmy, jeho tvrdé dovednosti při výkonu důležitých činností a procesů ve zvolené firmě.
- Manažerské schopnosti a dovednosti, ochota vlastníka delegovat činnosti a pravomoci na management, a to včetně odpovědnosti a řízení činností ostatních zaměstnanců v organizaci konkrétní firmy.
- Strategické schopnosti a dovednosti vlastníka soukromé bezpečnostní firmy, které umožňují dívat se za hranice současnosti a sladit silné a slabé stránky se stanovenými strategickými cíli vzhledem ke korporátní strategii.

Jak malá a střední firma postupně přechází z jedné fáze do druhé, mění se význam jednotlivých faktorů. Na fakto-

ry je možno nahlížet tak, že se střídají tři úrovně důležitosti: **za prvé klíčové proměnné, které jsou pro úspěch naprosto nezbytné a musí mít vysokou prioritu; za druhé faktory, které jsou pro úspěch dané firmy jednoznačně důležité a musí jim být věnována určitá pozornost; za třetí faktory, které se vrcholového vedení bezprostředně netýkají.** Pokud každý z osmi dříve uvedených faktorů rozdělíme do kategorií podle jeho důležitosti v jednotlivých fázích vývoje firmy, získáme jasný obraz o měnících se požadavcích managementu i vlastníka daného organizačního uskupení firmy.

Mění se povaha manažerských výzev je zřejmé. V počátečních fázích dávají malé i střední firmě životaschopnost vlastníka vykonávat práci. Malé firmy jsou postaveny na talentu majitele a jeho schopnosti prodávat, vyrábět, vynalézat nebo cokoli jiného. Tento faktor má tedy nejvyšší význam. Schopnost majitele delegovat je však na spodním konci žebříčku, protože zaměstnanců, které by mohl delegovat, je málo, pokud vůbec nějaký jsou.

S růstem firmy přicházejí do prodej, výroby nebo poskytování služeb i firemní know-how další lidé, kteří nejprve podporují a posléze i nahrazují schopnosti majitele, čímž se význam tohoto faktoru snižuje. Současně musí majitel trávit méně času prací a více času řízením podřízených zaměstnanců. Musí zvýšit objem práce vykonávané prostřednictvím jiných lidí, což znamená delegování.

Do hry vstupuje neschopnost mnoha zakladatelů opustit děláni a začít řídit a delegovat činnosti i procesy z hlediska daného podniku. Majitel, který uvažuje o strategii růstu malé a střední firmy, musí pochopit změnu osobních činností, kterou takové rozhodnutí přináší, a prozkoumat aktuální manažerské potřeby. Podobně by měl jednat i podnikatel, který uvažuje o založení firmy – že je třeba od začátku provádět veškerý prodej, výrobu nebo další činnosti, včetně řízení finančních aktiv malé a střední firmy a plánování smě-

rování firmy v souladu s korporátní strategií.

Význam hotovosti se mění s tím, jak se mění podnikání dané firmy a fáze její existence. Na začátku podnikatelské činnosti je důležitým zdrojem rozjezdu podnikání, ve fázi úspěchu malé a střední firmy se stává snadno zvládnutelným, a pokud organizace firmy začne následně růst, je opět hlavním problémem. Oblasti řízení lidských zdrojů, plánování a systémů strategického řízení postupně nabývají na důležitosti, jak daná firma postupuje od pomalého počátečního růstu k následnému dynamickému růstu.

Tyto zdroje je třeba získat s určitým předstihem před fází růstu, aby byly k dispozici, až budou potřeba. Sladění podnikatelských a osobních cílů je ve fázi existence dané firmy klíčové, protože vlastník firmy se musí smířit s velkými finančními a časovými nároky vývoje a růstu dané firmy. Mění se role faktorů jasně ilustruje potřebu flexibility vlastníka. Převažující zájem o hotovost je v některých fázích poměrně důležitý a v jiných méně důležitý.

V segmentu malých a středních firem v rámci komerční bezpečnosti je možné identifikovat bariéry růstu dané firmy v souvislosti s osobnostními předpoklady vlastníka této firmy, ale též managementu. Mimo bariéry, které souvisejí s osobou vlastníka či managementu, je možné uvést i externí a interní vlivy související s fungováním i potencionálním růstem daného podniku. Identifikace bariér růstu firmy je důležitá pro jejich pochopení i pro následné možnosti odstranění a řešení těchto bariér v kontextu růstu konkrétní firmy. K nejvýznamnějším bariérám, ale i specifickým příležitostem patří především tři následující:

- Absence manažerských a strategických dovedností v osobě vlastníka či managementu** – s přibývajícím informacemi mnozí vlastníci podniků brzy zjistí, že se toho musí hodně naučit jak z hlediska měkkých, tak tvrdých

dovedností. Ať už jde o získání aktuálních informací o nových právních předpisech a povinnostech, seznámení se se sociálními médií nebo aplikací vyjednávacích technik s různými zainteresovanými stranami; pro vlastníka podniku i management je nutné rozvíjet a udržovat dovednosti aktuální, a to i ve vztahu k českému stavebnímu trhu.

- b. Nedostatek zpětné vazby a negativní přístup k podnikání a ostatním zaměstnancům** – vlastníci či management se mohou naučit nové dovednosti a znalosti i měkké a tvrdé dovednosti. Nicméně nedostatečná zpětná vazba i negativní přístup k podnikání podniku mohou představovat bariéru v růstu malé i střední firmy. Opětovně se jedná o bariéru, která se váže k osobě vlastníka firmy či managementu a nelze ji v některých případech odstranit. Souvisí s tím i skutečnost soustředění se na podnikatelskou činnost malé a střední firmy a na řešení jednotlivých činností a procesů postupně. V segmentu komerční bezpečnosti jsou důležité také kvalitní služby a produkty pro jednotlivé segmenty zákazníků. Důležitá je i dostatečná nabídka těchto firem a soukromých bezpečnostních služeb pro zákazníky a rovněž využití technických a technologických inovací v podnikatelské činnosti konkrétních jednotlivých firem.
- c. Nedostatek kreativity a přepřacování vlastníka či managementu** – zahrnuje zejména v počátečních fázích vývoje podniku a jeho následného růstu nadměrnou fyzickou či psychickou pracovní i řídicí zátěž vlastníka či managementu dané firmy. Podnikatelská činnost každé firmy musí být dostatečně kreativní a nové podněty i podnikatelské koncepce v organizaci dané firmy mohou podpořit růst podnikatelské činnosti, ale též ziskovost či konkurenceschopnost v prostředí malé a střední firmy.

S ohledem na výše uvedené bariéry, které jsou personalizované, lze uvést i externí a interní bariéry, které ovlivňují růst konkrétní firmy v segmentu komerční bezpečnosti.

Obecně je možno uvést, že celkově mohou všechny malé a střední firmy ve svém růstu narazit na další individualizované překážky s ohledem na jejich podnikatelskou činnost. Rozhodná je jejich včasná a dostatečná identifikace, jejich řešení a překonání v podnikatelské činnosti firmy. Na základě dostatečných informací je pak možné stanovit opatření a řešení těchto bariér a navázat na růstové možnosti firmy a její podnikatelské činnosti.

Mezi nejčastější překážky, s nimiž se firmy ve své podnikatelské činnosti se-

stávají, patří zejména:

- Nedostatek finančních zdrojů a nejasnosti týkající se finančního řízení konkrétní organizace firmy. To se týká zvláště začínajících malých a středních firem.
- Nedostatečné podnikatelské plánování a strategické řízení. Spočívá často v přílišném soustředění na nevýznamné strategické úkoly, s tím souvisí absence korporátní strategie nově vznikajících firem a absence řešení krátkodobých až dlouhodobých strategických cílů.
- Problémy v daném tržním segmentu se zákazníky. Jednotlivé firmy se ve svém segmentu a růstu setkávají s nedostatečným zájmem zákazníků o své služby, i v případě soukromých bezpečnostních služeb, a také s tím, že nemohou identifikovat vhodné relevantní zákazníky. Je to typický problém malých soukromých bezpečnostních firem,
- Cenotvorba a ziskovost produktů a služeb. Bývá problémem nastavení cen pro zákaznické segmenty, aby nabídka produktů a služeb byla dostatečná a umožňovala ziskovost i konkurenceschopnost firmy, i v segmentu komerční bezpečnosti.
- Absence osvojení podnikatelského myšlení a strategického řízení. Malé a střední firmy se často snaží dělat vše samy, aniž by využívaly dodavatele a externí podporu, což souvisí i s osobnostními předpoklady, dovednostmi a znalostmi vlastníků a managementu těchto firem, i v segmentu komerční bezpečnosti.

Zásadním problémem je pro mnoho malých a středních firem omezení financování a finančních zdrojů. Bez kapitálu je řízení a provoz v podstatě všech konkurenčních firem nemožný a strategické plány na jejich rozšíření mohou být ohroženy. Mnoho malých a středních firem například neví o daňových úlevách na výzkum a vývoj, které mají k dispozici, a to je oblast, kde růst může být skutečně přínosem, a především konkurenční příležitostí.

Problémem však není vždy jen získávání finančních prostředků. Malé a střední firmy mohou narazit také na potíže a specifické problémy, pokud jde o přidělování finančních prostředků. Bez větších předchozích zkušeností s řízením konkrétní firmy se může zdát, že pochopení toho, kam a kdy směřovat disponibilní finanční zdroje, je prakticky problematické pro vlastníky i management, a to nejenom v segmentu komerční bezpečnosti.

Když se zpomaluje růst prodeje služeb a produktů konkrétní malé a střední firmy, je to často důsledkem toho, že se firma zaměřuje na špatný trh, nebo že produkty a služby pro zákaznické segmenty nejsou nastaveny vhodným způsobem. Podstatné je také oslove-

ní cílové skupiny prostřednictvím nových médií, jako jsou sociální média a internet, nebo upoutání pozornosti relevantních zainteresovaných stran prostřednictvím personalizovaných komunikačních i informačních kanálů.

Jak daná firma roste a rozvíjí se, je pravděpodobné, že bude potřebovat vstoupit na nové trhy, aby došlo k rozšíření podnikatelských aktivit. Správné stanovení cen produktů i služeb s ohledem na ziskovost vyžaduje strategické řízení i myšlení, množství postupů a zkušeností. Zohlednění marží, prodejního a marketingového úsilí, řízení zásob a všeho ostatního, co bylo vynaloženo na vytvoření, vývoj, výrobu a distribuci produktů a služeb, může být v praxi velmi složité. Obecně tak hovoříme o prostředí malých a středních firem, specificky pak v segmentu komerční bezpečnosti.

Zejména u menších i středních firem je často skutečným zdrojem úspěchu myšlení a osobní cíle vlastníka konkrétního podnikatelského subjektu. Rozhodující je správné a efektivní uplatnění strategického řízení organizace dané firmy. V segmentu komerční bezpečnosti je nutné získávat důvěryhodné dodavatele a zaměstnance, kteří se postarají o každodenní pracovní povinnosti, aby bylo možné z hlediska soukromých bezpečnostních služeb dále růst a aby byly produkty i služby ziskové a konkurenceschopné.

Nejvíce problematické jsou lidské zdroje a jejich řízení na konkrétních pracovních pozicích v rámci soukromých bezpečnostních služeb. S ohledem na výše uvedené problémy bude jednotlivě každá firma v průběhu svého rozvoje čelit různým výzvám v závislosti na segmentu komerční bezpečnosti, odvětví a dostupnosti disponibilních zdrojů. Existují však některá společná témata, která většina malých a středních firem v určitém okamžiku svého růstu identifikuje. Tyto překážky mohou pocházet z interních i externích zdrojů a je důležité je identifikovat k jejich účinnému i úspěšnému překonání.

Mezi nejvýznamnější interní překážky patří především:

- Hledání vhodných zaměstnanců a jejich pracovní uplatnění na daných pracovních pozicích v malé a střední firmě i v kontextu prodeje produktů a služeb.
- Přístup ke zdrojům a materiálům, což je pro malé a střední firmy v segmentu komerční bezpečnosti poměrně klíčové.
- Ignorování ukazatelů výkonnosti malých a středních firem a jejich nezhlednění v korporátní strategii firem a ve strategickém řízení pro funkční úroveň řízení v malých a středních firmách; typicky jde o strategické řízení lidských zdrojů či strategické řízení finančních zdrojů a další.
- Nutnost monitorovat vývoj kon-

kurence v odvětví a nastavení vhodných konkurenčních opatření pro produkty i služby v prostředí malých a středních firem.

- Neefektivní procesy a interní infrastruktura organizace jednotlivých firemních organizací.
- Problémy s řízením malých a středních firem, s aplikací principů strategického řízení a realizací korporátní strategie i provozních strategií.
- Nedostatečně koncipovaná marketingová a obchodní strategie konkrétní malé i střední firmy v segmentu komerční bezpečnosti.
- Nastavení neudržitelných obchodních modelů a konceptů v souvislosti s podnikatelskou činností malých i středních firem.
- Nedostatečný důraz na kreativitu produktů a služeb, ale také na technické a technologické inovace produktů a služeb v organizačních schématech malých a středních firem.

V podnikatelské praxi v evropských zemích existuje i v současné době přesvědčení, že firmy všech velikostí a významů fungují výhradně pro zisk svých vlastníků a případně i vlastních zakladatelů. Jen málo firem si v minulých letech uvědomovalo potřebu spojit svou podnikatelskou činnost s etikou a filozofickým rámcem konceptu společenské odpovědnosti (CSR – Corporate Social Responsibility), a zejména se závazky vůči české či jiné evropské podnikatelské entitě nebo životnímu prostředí v kontextu hlavních pilířů, na kterých je koncept CSR postavený.

To je také důvod, proč se o podstatě společenské odpovědnosti a konfliktu mezi skutečným a simulovaným altruismem nadále diskutuje i v důsledku existujících externích vlivů a dopadů pandemie COVID-19.

Různé odborné přístupy jsou uvedeny i v odborné literatuře. Například je odkazováno na názory Friedmana na společenskou odpovědnost firmy a její význam. Postupem času se však názory na roli firem v sociálně-ekonomické realitě, odvozené z klasické ekonomie, stávají pro současnou sociálně-ekonomickou realitu stále méně relevantní. Je tomu tak s ohledem na dopady a vlivy pandemie COVID-19 i na pokračující externí vlivy a ekonomický vývoj v evropských zemích.

Kromě toho došlo k četným změnám ve sféře fungování moderních firem různých velikostí a významů. Globalizace doprovázená rychlými technologickými změnami dala vzniknout zcela novému podnikatelskému prostředí s důrazem na technické a technologické inovace. V těchto nových podmínkách je rozvoj moderní firmy podmíněn nejen efektivním využíváním zdrojů a uplatňováním vhodných strategií, ale také zohledněním konceptu společenské odpovědnosti firem a etiky podni-

kání v procesech strategického řízení a formulace strategických cílů.

(Pokračování – 3. část – v příštím čísle BsP.)

PhDr. Mgr. Dávid Dömény, MBA, DBA

Seznam odborných zdrojů

ARMSTRONG, M. 2020. Coronavirus crisis sparks race for inventive solutions. Euro-news, Dostupné online: www.euronews.com/2020/03/21/coronavirus-crisis-sparks-race-for-inventive-solutions.

com/2020/03/21/coronavirus-crisis-sparks-race-for-inventive-solutions.

BŘEČKOVÁ, P.; HAVLÍČEK, K. 2017. Inovace a jejich financování v malé a střední firmě. Vyd. Vysoká škola finanční a správní, a.s., Praha, 120 s., ISBN 978-80-7408-137-8.

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

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

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

OECD. 2022. Science, Technology and Innovation Outlook 2020-2022 [online]. OECD. Dostupné z: <https://www.oecd.org/sti/science-technology-innovation-outlook/>.

OECD. 2022. Global State of Small Business: Uplatnění firem v mezinárodním tržním prostředí [online]. OECD. Dostupné z: <https://dataforgood.fb.com/global-state-of-smb/>.





PODPOŘTE SPOLEK

SRDCE DĚKOVA, Z.S.



6916985329/0800



DĚKUJEME ZA PŘÍSPĚVEK A VAŠI PODPORU

Hezký den všem, již čtvrtý rok trávím část svého života v obci Děkov nedaleko Rakovníka. Obec se nachází v oblasti bývalých Sudet, se všemi souvislosti s tím spojenými. Hodně mě štval neutěšený stav chátrajícího kostela sv. Jana Křtitele, který se nachází uprostřed obce. Především tedy to, že se s ním nic neděje. O kostelu jsme mluvili často doma s přítelem a na konci roku i s kamarády a sousedy. A tak se najednou začaly dít věci. Zjistilo se, že kostel není lhostejný více lidem a během pár měsíců vznikl spolek Srdce Děkova, z.s., který si položil za cíl kostel zachránit.

Začali jsme jednat s panem farářem z místní diecéze, jenž byl moc rád, že jsme ochotni kostelu pomoci, i s okolními spolky, které již mají s opravami kostelů a kostelíků zkušenosti. Najednou se před námi otevřela nová výzva – společně s podobně nadšenými lidmi něco pro zlepšení stavu historické duchovní památky udělat. Máme před podpisem smlouvy o výpůjčce kostela s Arcibiskupstvím pražským. V první řadě chceme kostel uklidit, nechat zasklít rozbitá okna, vyčistit okapy, nasvítit ho a zajistit, aby zvon zase zvonil. Máme už i transparentní účet 6916985329/0800.

Kostel bychom rádi využili pro koncerty, výstavy, svatby, ale třeba i filmaře. Budeme moc vděční za vaše rady, zkušenosti, zapojení, a třeba i příspěvek. Máme krásnou zemi, tak pojďme udělat něco ušlechtilého, ať se nám i našim dětem líbí zase o něco víc.

Mgr. Kateřina Poludová
šéfredaktorka

SMUTNÁ ZPRÁVA

Dovolujeme si vás informovat, že 28. 7. 2025 nás nečekaně opustil náš kamarád, kolega a bezpečnostní expert pan **Mgr. David Rožek, CPP®**.

David působil v oblasti komerční bezpečnosti 19 let. V současnosti byl činný jako externí bezpečnostní poradce a školitel pro několik klientů ze soukromé i státní správy, byl odpovědný za tvorbu bezpečnostní politiky i bezpečnost-

ních opatření. Věnoval se výzkumu radikalismu a efektivní spolupráci mezi státním a soukromým bezpečnostním sektorem. Rovněž působil jako prezident České komory detektivních služeb, byl spoluautorem několika publikací o ochraně měkkých cílů a hodnotitelem bezpečnostních projektů pro MVČR. Je to pro nás velká ztráta.

Soucítíme s jeho rodinou.



II. MEZINÁRODNÍ KONFERENCE OBEČNÍCH POLICIÍ V ČESKÉM TĚŠÍNĚ



Vážení přátelé,

s potěšením vás zveme na II. Mezinárodní konferenci městských policíí v Českém Těšíně, kde se sejdou odborníci z různých oborů, aby se podělili o své poznatky a osvědčené postupy při zajišťování bezpečnosti a ochrany našich měst. Konference je určená nejen pro zástupce z oblastí městských a obecních policíí, státní správy, samosprávy, integrovaného záchranného systému, bezpečnostních sborů a dalších subjektů, ale i pro odborné firmy z různých oborů.

**Konference se bude konat ve dnech 10. – 12. 9. 2025
v prostorách Kulturního a společenského
střediska KaSS „Střelnice“ v Českém Těšíně**

- Konference se zaměří na aktuální témata, kterými jsou:
- Kybernetická bezpečnost, umělá inteligence
- Digitální Česko – podpora digitálních dovedností
- Bezpečná škola – měkké cíle
- Bezpečné město - bezpečí kritické infrastruktury, vyhledávání osob v ohrožení
- Sociální problematika, přeshraniční spolupráce
- Praktické využívání kamerových systémů, monitoring v objektech pod správou města a obcí, problémy ve veřejném prostranství
- Využívání moderních technologií a jejich rizika
- Mezinárodní bezpečnostní situace, zvládání krizových situací

Tato prestižní akce bude mít i v letošním roce podporu ministerstev a významných profesních sdružení zastupujících obecní a městské policie v Česku, na Slovensku a v Polsku, která nás těší. Rádi bychom rovněž poděkovali všem našim partnerům, jejichž podpora nám umožňuje připravit jak bohatý a rozmanitý odborný program plný zajímavých přednášek, tak i fasci-
nující doprovodný program, který věříme, že uspokojí potřeby všech účastníků.

Připojte se k nám na tuto jedinečnou konferenci a přijďte se inspirovat, sdí-

let své zkušenosti, postřehy a navázat cenné kontakty mezi českými, polskými a slovenskými strážníky, policisty a složkami integrovaného záchranného systému a to vše v neformálním prostředí.

Konference je určená pro odbornou veřejnost. S nadšením však letos otevíráme dveře i širšímu publiku, včetně žáků základních škol a široké veřejnosti, kteří budou mít dne 11. 9. 2025 možnost v rámci doprovodného programu ve venkovních prostorách nahlídnout pod pokličku práce složek integrovaného záchranného systému a jiných odborných subjektů z Čech a Polska v čele s Odborem prevence kriminality MV ČR.

Nenechte si ujít tuto příležitost být součástí této akce, která bude utvářet budoucnost nejen obecní a městské policie.

Přijměte naše pozvání a zažijte s námi nezapomenutelné chvíle!

Podrobné informace o konferenci naleznete na webových stránkách města, které budou průběžně aktualizovány.

Podrobné informace o konferenci naleznete na webových stránkách města, které budou průběžně aktualizovány.

Tým MP Český Těšín



Karel Kula
starosta města Český Těšín



Ing. et Bc. Martin Látko, MBA
ředitel Městské policie Český Těšín





NABÍDKY ZVÝHODNĚNÝCH PRODUKTŮ

Pro zaměstnance Ministerstva obrany ČR a Ministerstva vnitra ČR

SLEVA 40 % na majetkové pojištění MŮJ MAJETEK

Nabízíme trvalou 40% slevu na pojištění stavby, domácnosti a odpovědnosti za škodu. Dále nabízíme 20% slevu na pojištění Mazlíček.

SLEVA 30 % na havarijní pojištění a povinné ručení

Nabízíme **základní slevu ve výši 30 %** na všechny produkty v rámci pojištění osobních motorových vozidel: havarijního pojištění i povinného ručení.

SLEVA až 40 % na životní pojištění MŮJ ŽIVOT

Nabízíme unikátní životní pojištění určené pro všechny členy rodiny se **slevou za propojištěnost až 40 %**.

SLEVA 50 % na pojištění odpovědnosti při výkonu povolání

Příklad: Při uzavření standardní smlouvy **Můj majetek** na dům a domácnost s pojistným 7 500 Kč **získáte slevu 3 000 Kč**, kterou můžete využít na pojištění dalšího majetku, nebo pojištění členů rodiny v rámci životního pojištění. Případně můžete ušetřené prostředky využít na investování do podílových fondů, nebo jako splátku hypotečního úvěru. Všechny tyto možnosti můžete konzultovat s našimi poradci.

Chcete další informace nebo si sjednat pojištění? Kontaktujte nás.

Petr Krul, Poradce
M 777 206 633
petr.krul@generaliceska.cz
www.petrkrul.cz



ČLENOVÉ KOMORY PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČR

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

SAFE Technology SAFETE, s.r.o.

Na Výsluní 519/17
100 00 Praha 10 – Strašnice
www.systemkiss.cz



HIGH SECURITY PRODUCTS, a. s.

Pod stárkou 378/3
140 00 Praha 4
www.h-s-p.cz



Agentura Pancēr, s. r. o.

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



European Security Solutions s.r.o.

Tyršova 3214/8
695 01 Hodonín
www.eseso.cz



ATON Security s.r.o.

Na Stráži 1576/35
190 00 Praha 9
www.cleanline.cz



TRIVIS – Centrum vzdělávání, s.r.o.

Na terase 355/8
182 00 Praha 8
www.trivis.cz



ECES Institut, s.r.o.

Kutuzovova 547/13
703 00 Ostrava
www.eces.cz



WAKENHAT s.r.o.

Sazečská 560/8
108 00 Praha 10 Malešice
www.wakenhat.cz



SYBENAM - Systém bezpečnosti na míru

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



ELSERVIS - Ivo Kolář

Dědinská 898/15
161 00 Praha 6



SIMACEK FACILITY CZ spol. s r. o.

Trnkova 34
628 00 Brno
www.simacek.cz



ANIM plus – RS, s.r.o.

Areál TJ MEZ, 755 01 Vsetín – Ohrada
www.anim.cz



Mezinárodní bezpečnostní institut, z. ú.

Na Ořešence 580/4, Praha 6, 162 00
+420 224 232 611



ANIM plus – RS, s. r. o.

Areál TJ MEZ, 775 01
Vsetín – Ohrada
www.anim.cz



General Provider s.r.o.

Sídlo: Kodaňská 432/15
101 00 Praha 10
www.generalprovider.cz



SECURITY MONIT s.r.o.

Hoblíkova 548/6
613 00 Brno
www.security-monit.cz



APEurope s. r. o.

Kaprová 42/14
110 00 Praha 1
www.aperurope.cz



Security MCO s.r.o.

Struha 865
517 54 Vamberk
www.mco-security.cz



Trade Corporations s.r.o.

Mostecká 273/21
118 00 Praha 1
info@tcorp.cz



Solidita s.r.o.

Jefábová 419
250 73 Radonice
www.solidita.cz



SEKURO & Group s.r.o.

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



CENTURION loss prevention a. s.

Kundratka 17/1944
180 82 Praha 8
www.centurionlp.cz



ABAS IPS Management s. r. o.

Jankovcova 1569/2c
170 00 Praha 7
www.abasco.cz



Preventa Service s.r.o.

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



OKO 69 s.r.o.

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



Česká pošta Security, s.r.o.

Sídlo: Politických vězňů 909/4
Nové Město, 110 00 Praha 1
pistek.roman@cpst.cz



ARES GROUP s.r.o.

Libušská 189/12
142 00 Praha 4
www.ares-group.cz



Stratia s.r.o.

Podolská 613/28
147 00 Praha 4
www.stratia.cz



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

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

Pro Bank Security, a. s.

Václavské nám. 21
110 00 Praha 1
www.probank.cz



ČVUT - Fakulta biomedicínského inženýrství

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



GADO s.r.o.

Heršpická 11b
639 00 Brno
www.gado.cz



Ing. Martin Neuschl

Šachetní 391
261 01 Příbram

INPOS SECURITY

Křížkový Újezdec 42
251 68 Kamenice
www.inpos.cz



PRIMM bezpečnostní služba s. r. o.

Kutnohorská 309
109 00 Praha 10
www.primm.cz



INCRISCO s.r.o.

Sádecká 400
252 30 Řevnice
info@incrisco.cz



Gatum Group, s.r.o.

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

