KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČESKÉ REPUBLIKY

ČLENOVÉ KOMORY PODNIKŮ KOMEČNÍ BEZPEČNOSTI ČR

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

ATALIAN CZ,s.r.o.
AVIATICA, U Trezorky 921/2,
CZ 158 00 Praha 5 - Jinonice
www.abfacility.com

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

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

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

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

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

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

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

Silvermen s.r.o.
Bašty 6
602 00 Brno
www.silvermen.cz

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Synergia management czech s.r.o.
Drtinova 557/10
150 00 Praha 5
www.synergia.cz

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ing. Martin Neuschl
Šachetní 391
261 01 Příbram

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČESKÉ REPUBLIKY

ČASOPIS KOMORY PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČR
BŘEZEN - ČERVEN/2023

BEZPEČNOST S PROFESIONÁLY

OHLÉDNUTÍ ZA KONFERENCÍ OCHRANA MĚKKÝCH CÍLŮ 2023

KOGNITIVNÍ ÚTOKY PROČ A JAK SE JIM BRÁNIT?

CHYTRÁ ŘEŠENÍ PRO DIGITÁLNÍ MĚSTA

ISSN 2336-4793

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČESKÉ REPUBLIKY

BEZPEČNOST
S PROFESIONÁLY

Šéfredaktor
Mgr. Bc. Kateřina Poludová, DiS.

Jazyková spolupráce
PhDr. Alena Hasáková

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

Inzerce
kpkbcr@volny.cz

Nesignované fotografie a články
Redakce

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

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

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

Rozšiřování zdarma

Na zadních stranách obálky
členové KPKB ČR

OBSAH

ÚVODNÍ SLOVO

Vážení čtenáři,

držíte v rukou druhé letošní číslo našeho odborného časopisu Bezpečnost s profesionály.

Na jeho stránkách Vám přinášíme opět zajímavé články s atraktivními tématy, jaká byla především součástí programu naší letošní červnové konference Ochrana měkkých cílů 2023.

Konferenci jsme organizovali již tradičně ve spolupráci s Asociací kyberbezpečnosti AFCEA a Fakultou biomedicínského inženýrství ČVUT.

Konference se těší velkému zájmu odborné veřejnosti a na tu letošní se registrovalo téměř 260 účastníků. Toto nás samozřejmě velmi těší a jsme připraveni zorganizovat další ročník této akce opět v příštím roce.

Další neopomenutelnou záležitostí oblasti bezpečnosti stále zůstává návrh zákona o bezpečnostních činnostech. V nedávné době došlo na Ministerstvu vnitra ČR k reorganizačním změnám, které zasáhly i Samostatné oddělení bezpečnostních služeb, jež tento zákon už po několik let připravuje. Tímto samozřejmě není práce na zákoně ukončena a my jsme připraveni se na jeho tvorbě i nadále podílet.

Rovněž bychom se chtěli aktivně zapojit do již vzniklé aktivity Ministerstva práce a sociálních věcí ČR k problematice cen v oblasti bezpečnostních služeb. Byli bychom rádi, aby se na podzim uskutečnil workshop na toto téma na půdě Poslanecké sněmovny.

Máme před sebou letní prázdninové dny, které nám jistě přinesou příjemné chvíle odpočinku s možností nabrání nových sil a elánu do další práce.

Krásné léto Vám všem za celé prezidium KPKB ČR přeje

Ing. Václav Jahodář
prezident KPKB ČR

KONFERENCE
OCHRANA MĚKKÝCH CÍLŮ 2023

Již posedmé se konala konference Ochrana měkkých cílů – letos tedy s přídomkem 2023. Proběhla 8. června v hotelu Olšanka a stala se jednou z dalších významných událostí letošního roku v oblasti komerční bezpečnosti a ochrany.

Pořádání konference se ujaly renomované organizace jako Komora podniků komerční bezpečnosti České republiky, z. s., Česká pobočka AFCEA a ČVUT FBMI (Fakulta biomedicínského inženýrství). Spolupráce těchto tří subjektů umožnila přinést odborníkům z různých oblastí bohatý program a řadu námětů k diskusím.
Primárně se konference zaměřovala na problematiku ochrany měkkých cílů, jež sama o sobě představuje široké spektrum témat, jako je kybernetická bezpečnost, fyzická ochrana, ochrana dat, bezpečnost infrastruktury a další.
Účastníci konference měli příležitost se seznámit s nejnovějšími trendy, technologiemi a strategiemi v oblasti ochrany měkkých cílů a měli možnost vyměnit si zkušenosti s předními odborníky v oboru. Mezi hlavními řečníky konference byli totiž skutečně přední odborníci z oborů bezpečnosti, akademické sféry a veřejného sektoru a jejich příspěvky přinesly na problematiku ochrany měkkých cílů nové pohledy a cenné perspektivy.
Konference Ochrana měkkých cílů 2023 byla dobře zorganizovaná a přinesla hodnotnou platformu pro výměnu názorů, sdílení informací a navazování nových kontaktů v oblasti komerční bezpečnosti. Účastníci získali ucelený přehled o současných výzvách, možnostech a nejlepších postupech v dané oblasti. Jednání tak přispěla k posílení povědomí o důležitosti a nutnosti ochrany měkkých cílů a podpořila další rozvoj této oblasti v České republice.
Děkujeme všem, kteří nás podpořili.
Poprvé v historii jsme se dostali na počet 200 účastníků. Děkujeme a těšíme se Vás při dalších akcích, které budeme připravovat.

Organizační tým konference

WWW.YOUTUBE.COM/@KOMORAPODNIKUKOMERCNIBEZPE4710

Videa z jednotlivých přednášek naleznete na našem profilu na sociální síti Youtube. Nad rámec videí jsou zde také otázky a odpovědi jednotlivých přednášejících.









MANAGEMENT MÍST VELKÉ KONCENTRACE OSOB OPTIKOU EVROPSKÉ UNIE

Tento text si klade za cíl indikativně zmapovat, zda a nakolik se tématům „měkkých cílů", „míst velké koncentrace osob" či jinak obdobně vnímaným výzvám věnuje agenda Evropské unie. Jedná se přitom o doplnění vystoupení na konferenci Měkké cíle 2023 dne 8. června 2023.

Je přitom příznačné, že související terminologie v angličtině, ale i v jiných jazycích situaci dále komplikuje (crowd control, crowd management).

Pokud tedy chceme související dokumenty zmapovat, lze na konci května 2023 hovořit o následujícím spektru textů (z celkových 211), přičemž nezřídka se jedná o navazující modifikace některých podkladů:

- pojem „crowd security": 0 výsledků
- pojem „crowded places": 45 výsledků
- pojem „crowd management": 135 výsledků
- pojem „crowd" a „CCTV": 30 výsledků
- pojem „crowd science": 1 výsledek

První zmínky o tématu: Evropská policejní akademie

Nejstarší zjištěná zmínka o tématu (crowd management, crowd control, crowd violence) v unijních podkladech se týká zřejmě let 2003 a 2004. Jedná se o stručný přehled vzdělávacích kurzů pro experty z členských států na téma kontroly davu (které se konaly ve Francii a Nizozemsku), respektive kurzy k tématu zvládání diváckého násilí (ve Španělsku a Portugalsku). [1]

Ochrana kritické infrastruktury

Další téma souvisí s komplexním protiteroristickým úsilím, které se úrovni Evropské unie nevyhnulo. Jedním z jeho rozměrů byla ochrana kritické infrastruktury. Rada Evropské unie deklarovala v této souvislosti v roce 2005 nutnost dosažení shody o důležitosti ochrany kritické infrastruktury: „... jako součásti vyvážené strategie boje proti terorismu. Ochrana kritické infrastruktury před útokem tvoří nedílnou součást ochranných bezpečnostních opatření členských států vedle ochrany dalších teroristických cílů, jako jsou místa velké koncentrace osob a měkké cíle... Z bezpečnostních důvodů je třeba zachovat důvěrnou povahu informací o infrastruktuře."[2] Právě přehršel veřejně dostupných a potenciálně zneužitelných informací představuje výzvu dodnes (včetně například umístění podzemních staveb, rozvodů elektřiny a podobně).

Výcvik lodních posádek

Poněkud mimo priority České republiky se nachází téma zvláštních požadavků na výcvik členů posádky některých typů lodí, které v letech 2007 až 2022 představuje rozpracování obsahu Mezinárodní úmluvy o standardech výcviku, kvalifikace a strážní služby námořníků (International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, STCW). [3] V prostředí Evropské unie se pak konkrétně jedná o následující dvě pravidla:

• Pravidlo V/2: Povinné minimální požadavky na výcvik a kvalifikaci velitelů, důstojníků, členů mužstva a ostatních osob na osobních lodích typu ro-ro.[4] Velitelé, důstojníci a ostatní posádka, kteří jsou určeni k tomu, aby pomáhali cestujícím v nouzových situacích na osobních lodích typu ro-ro, musí mít ukončený výcvik v řízení velkého množství lidí /crowd management/ stanovený v oddílu A-V/2 odst. 1 předpisu STCW.

• Pravidlo V/3: Povinné minimální požadavky pro výcvik a kvalifikaci velitelů, důstojníků, členů posádky a ostatních osob na osobních lodích jiného typu než ro-ro.[4] Posádka určená k tomu, aby pomáhala cestujícím v nouzových situacích na osobních lodích, musí mít ukončený výcvik v řízení velkého množství lidí stanovený v oddílu A-V/3 odst. 1 předpisu STCW.

Bezpečnost sportovních, zejména fotbalových utkání

„Fotbalová agenda" se ve vztahu k tématu objevuje od roku 2004. Zmínky jsou mimo jiné o nutnosti policejní přítomnosti v davu diváků. Další proklamatorní dokument se věnuje sportu, zejména fotbalu, s důrazem na přesun fanoušků na stadion a ze stadionu. [5]

Opatření navržená pro maximalizaci bezpečnosti a zabezpečení v souvislosti s fotbalovými zápasy s mezinárodním rozměrem, obsahují v roce 2010 následující konstatování, týkající se evergreenu odpovědnosti za určitá nákladná bezpečnostní opatření: „...zatímco fotbalové násilí a nepořádky mohou představovat kriminalitu (a v důsledku toho primární odpovědnost určených orgánů), vládní nebo policejní orgány nemusí nutně kontrolovat nebo ovlivňovat řadu klíčových faktorů, které dopadají na míru rizika (například dynamika řízení davu na stadionech /crowd management/ a širší bezpečnostní opatření). V mnoha členských státech mohou být policejní orgány odpovědné například za dynamická bezpečnostní opatření, zatímco pořadatel utkání (klub/sdružení) je odpovědný za vzájemně související fyzická opatření." [6]

Ochrana obyvatelstva

V dokumentu označovaném jako „Mechanismus civilní ochrany Společenství při významných událostech v Evropské unii" (bod 15.e) vyzývá Rada Evropské unie roku 2010 členské státy, aby pokud to jejich systémy civilní ochrany vyžadují: „...podporovaly vypracování evakuačních plánů, které plně zohledňují dynamiku davu a techniky zvládání davu (crowd dynamics and crowd management techniques) s cílem podpořit vhodnou reakci veřejnosti a vyhnout se nekontrolovaným a nekoordinovaným reakcím." [7]

Prevence a potírání organizovaného zločinu

Spíše na okraji tématu je možno zmínit příklady dobré praxe z členských států, a to konkrétně Kypru, pro rok 2011. Kyperští policisté se vyjádřili v tom smyslu, že mezi jejich preventivní opatření protidrogové trestné činnosti spadá i posilování vztahu s veřejností spoluprací v komunitách a kontrola mládeže na místech velké koncentrace osob (crowded places).[8]

Implementace Prümské dohody

Příručka o výměně informací v oblasti prosazování práva (roky 2014 až 2016) uvádí, že každý členský stát určí národní kontaktní místo pro účely poskytování údajů týkajících se předcházení trestným činům a udržování veřejného pořádku a bezpečnosti při významných akcích, zejména při sportovních akcích nebo zasedáních Evropské rady. S cílem dále zvýšit svou praktickou hodnotu obsahuje příručka kontaktní údaje příslušných orgánů, uvedených v informačních výkazech členských států. Konkrétně se to ovšem týká pouze policejního sboru Maďarska a jeho „Úseku pro zvládání masových akcí" (division of crowd management), který je aktivní zřejmě zejména ve vztahu k fotbalovým utkáním.

Úschovny zavazadel na železnici

Poměrně nesamozřejmý aspekt bezpečnosti se objevuje v roce 2014, kdy výstupem specifického dotazovacího procesu byly postřehy týkající se úschovních skříněk v nádražních areálech, vnímané jako určitá bezpečnostní výzva. „Ve většině členských států jsou na nádražích umístěna jak automatické, tak personálem vybavené úschovny zavazadel. Vzhledem k jejich použití a umístění by úschovna zavazadel mohla být považována za vysoce rizikovou, pokud se jedná o záležitosti boje proti terorismu. Ve většině evropských zemí jsou automatické skříňky a skříňky s obsluhou umístěny uvnitř stanic, někdy v blízkosti pokladen nebo míst velké koncentrace osob (crowded places), většina zemí pro ně neurčila zvláštní pravidla." [9]

Městská agenda

V průběhu roku 2018 se k tématu, dalo by se říci, konečně, vztahují i výstupy související s bezpečností, respektive celkovým rozvojem velkých aglomerací. Zmíněná je možnost financování souvisejících aktivit (projektů) po linii „Městské inovativní akce" (Urban Innovative Actions, UIA) [10] v rámci Evropského fondu pro regionální rozvoj. „Zajištění fyzické odolnosti budov, fyzická ochrana míst velké koncentrace osob a podpora bezpečnosti již od návrhu mohou být způsobilými akcemi pro financování. To by mohlo zahrnovat opatření ke zvýšení bezpečnosti a podpoře veřejné bezpečnosti prostřednictvím návrhu veřejného prostoru, osvětlení a kampaní na zvýšení povědomí veřejnosti v rámci opatření na obnovu měst." [11]

Cvičení s námětem špinavé bomby

Specificky se k tématu míst velké koncentrace osob a jejich ochrany vztahuje cvičení pořádané v Litvě v roce 2019: „V současné době jsou celostátní cvičení civilní ochrany organizována v souladu s Národním plánem cvičení civilní ochrany na léta 2018–2020, schváleným nařízením Ministerstva vnitra Litvy č. 1V-68 ze dne 19. ledna 2018. Podle tohoto plánu byla v roce 2018 provedena cvičení (další jsou plánována na rok 2019) na téma Akce pracovníků systému civilní ochrany po výbuchu samostatně připravené výbušniny s radioaktivními materiály na místě velké koncentrace osob..." [12]

Téma Společné zahraniční bezpečnostní politiky

Podpora místních policejních sil v oblasti označované jako crowd management patří k relativně častým tématům zahraničního angažmá Evropské unie, viz Severní Makedonie (2005), Kosovo (2010), Bosna a Hercegovina (2013), Myanmar (2014, 2016), Ukrajina (2017) nebo Středoafrická republika (2018). Konkrétně policejní reforma v Arménii (2013 a 2014) zmiňuje: „Vnímáme důležitost řešení nedostatků v oblasti policejní práce, jak je zdůrazněno ve zprávě ad hoc parlamentního výboru o událostech z března 2008, která byla předložena v září 2009... Zdůrazněna je zejména potřeba zvýšit transparentnost v policejním systému, zlepšit profesionalitu policie během veřejných demonstrací a shromáždění, mimo jiné prostřednictvím školení o zvládání davu /crowd management/ a lidských právech. Zdůrazněna je naléhavá potřeba dále posílit důvěru veřejnosti v policii (kapitola 5.1)." [13]

Shrnutí

Témata, přímo, nepřímo nebo okrajově související s agendou míst velké koncentrace osob, jsou v současnosti nárazově přítomna v celé řadě konceptů a dokumentů Evropské unie. Česká republika a její vědeckovýzkumné instituce mohou tyto dokumenty studovat jako odrazové můstky pro účely svých výstupů doslova proto, „aby nevynalézaly kolo odznovu".

Poznámka: Příspěvek vznikl za využití podpory z projektu Digitální modelování evakuačních plánů v zájmových stavbách a měkkých cílech s prvky umělé inteligence (VB01000034).

Jedná se o projekt v rámci programu bezpečnostního výzkumu České republiky pro roky 2021–2026: Vývoj, testování a evaluace nových bezpečnostních technologií (SECTECH). Řešiteli projektu jsou: Mezinárodní bezpečnostní institut, z. ú., Vysoké učení technické v Brně, Gatum Advisory s. r. o. a VDT Technology a. s. (leden 2022 až prosinec 2023). Předmětem projektu je vývoj a testování softwarové platformy k modelování mimořádných událostí za účelem zlepšení a zefektivnění evakuačních opatření v zájmových stavbách a měkkých cílech. Jádrem platformy bude software na simulaci pohybu osob, který bude obohacen softwarovou analýzou reálných videozáznamů ke kalibraci behaviorálního modelu simulací.

doc. Mgr. Oldřich Krulík, Ph.D.
Mezinárodní bezpečnostní institut, z. ú.

1) Three-Year Report on the Operation and Future of the European Police Academy. Brussels, 9. XII. 2003. No. 15722/2003. Návrh Rozhodnutí Rady o zřízení Evropské policejní akademie (EPA) jako orgánu Evropské unie. Brusel, 1. X. 2004. KOM (2004) 623 v konečném znění 2004/0215 (CNS). https://eur-lex.europa.eu/legalcontent/cs/txt/pdf/?uri=celex:52004pc0623&from=lt

2) European Union Critical Infrastructure Protection (CIP). Brussels, 28. X. 2005. No. 13882/2005.

HAYES, Ben et al. NeoConOptins. Statewatch ISBN 978-1-874481-34-8, p. 49. https://www.statewatch.org/media/documents/analyses/neoconopticon-report.pdf

3) Directive 2008/106/EC of the European Parliament and of the Council of 19 November 2008 on the Minimum Level of Training of Seafarers. Brussels, 19. XI. 2008, No. 3649/2008.

4) Organisation of the Final Stage of the European Football Championship. Brussels, 30. VIII. 2004. No. 11963/2004.

5) White Paper on Sport. Brussels, 12. VII. 2007, No. 11811/2007.

6) Draft Council Conclusions Adopting the Work Programme on Further Measures Designed to Maximise Safety and Security in Connection with Football Matches with an International Dimension. Brussels, 23. XI. 2007. No. 15615/2007. https://data.consilium.europa.eu/doc/document/ST-15615-2007-INIT/en/pdf

7) Draft Council Conclusions on the Use of the Community Civil Protection Mechanism in Major Events in the European Union – Adoption. Brussels, 21. V. 2010. No. 9837/2010.

https://data.consilium.europa.eu/doc/document/ST-9837-2010-INIT/en/pdf

8) Complementary Approaches and Actions to Prevent and Combat Organised Crime: A Collection of Good Practice Examples from European Union Member States. Brussels, 30. V. 2011. No. 10899/2011. https://data.consilium.europa.eu/doc/document/ST-10899-2011-INIT/en/pdf

9) Outcome of the Questionnaire on Passenger and Baggage Control in the Rail Sector. Brussels, 21. XI. 2014. No. 15808/2014.

10) Urban Innovative Actions. https://www.uia-initiative.eu/en

11) Urban Agenda for the EU – Pact of Amsterdam. http://ec.europa.eu/regional_policy/en/policy/themes/urban-development/portal/

12) 8th Round of Mutual Evaluations: 'The Practical Implementation and Operation of European Policies on Preventing and Combating Environmental Crime': Report on Lithuania. Brussels, 2019. No. 10080/1/2019 REV1.

Final Report of the Eighth Round of Mutual Evaluations on Environmental Crime - Information and Discussion at the Council. Brussels, 15. XI. 2019. No. 14065/2019. https://data.consilium.europa.eu/doc/document/ST-14065-2019-INIT/en/pdf

13) Annotated Agenda of the 4th Meeting of the EU-Armenia Subcommittee. Brussels, 18. IV. 2013: No. 8644/2013.

Annotated Agenda of the 5th EU-Armenia Sub-committee Meeting. Brussels, 21. III. 2014. No. 6738/2014.

European Union Relations with Armenia. European Council. https://www.consilium.europa.eu/en/policies/eastern-partnership/armenia/

KOGNITIVNÍ ÚTOKY

PROČ A JAK SE JIM BRÁNIT

Co je kognitivní útok? Jedná se jen o další nadbytečný pojem, který časem odplaví příliv jiných, podobně „nepotřebných“? Nedomnívám se.

Se vzrůstající kvalitou bezpečnostních technologií je stále obtížnější je překonávat. Systémy kybernetické bezpečnosti, komplexně řízená objektová bezpečnost, umělá inteligence, videoanalytika, akustická detekce… to vše činí útoky proti zvolenému cíli obtížnějšími.

Pro útočníka je proto stále výhodnější útočit na zranitelnost lidského výkonu. Výkon člověka, na rozdíl od výkonu technických prostředků, neprochází zásadními modernizačními vlnami, novými verzemi, pro bezpečnostní personál dokonce ani není publikováno příliš softwarových aktualizací. Jestliže tedy útočník potřebuje překonat soubor bezpečnostních opatření, složených z lidských, technických a procesních aktiv, zvolí pochopitelně tu oblast, která je nejsnáze překonatelnou bez nočního vidění a pokročilé algoritmizace. Je to logické – pokud útočník leze přes plot, také zvolí jeho nejsnáze zdolatelnou část.

Podle publikované prezentace společnosti Hikvision jsou nejčastějším typem útoků na jimi produkované technologie útoky na identitu uživatele, nikoliv útoky na technické jádro řešení. Podle společnosti Datasence je v případě kybernetických útoků na kancelářské systémy více než 90 % úspěšně dokonaných útoků vedeno nikoli na zranitelnost technologie, ale na zranitelnost člověka.

Mimo oblast přímé bezpečnostní praxe je specifikem kognitivních útoků to, že ovlivněný člověk není jejich nástrojem, chceme-li vektorem, ale jejich konečným cílem. Tím můžeme mít na mysli „velké“ kognitivní útoky zaměřené na nějakou sociální, ekonomickou nebo podobnou skupinu s cílem ovlivnit volby nebo veřejné mínění. Těmto typům útoků se autor věnuje také, spíše však na půdě workshopů organizace AFCEA.

Kdo jsou typičtí aktéři neboli pachatelé kognitivních útoků? Jedná se o široké spektrum subjektů, které začíná státy a státem sponzorovanými útočníky, zahrnuje politické subjekty i kriminální organizace a končí jednotlivci, kteří pracují na zakázku nebo se zlým úmyslem.

Kdo pak stojí na druhé straně tohoto pomyslného kolbiště? Opět se jedná o široké spektrum subjektů a skupin.

U zmíněných „velkých“ útoků je cílem široká veřejnost nebo její část. V takovém případě se zpravidla jedná o dezinformační kampaně, manipulaci veřejným míněním, o rozpoutání obav či nedůvěry, nebo naopak o vzbuzení falešné důvěry.

Další skupinou obětí mohou být politici a exekutivní orgány, kdy cílem útoku může být snaha ovlivnit jejich rozhodování, politické postoje nebo strategie. Specifickou skupinou obětí mohou být sociální a etnické skupiny s cílem například šířit mezi nimi nenávist či rozpory nebo podněcovat konflikty. Samostatnou skupinou obětí jsou novináři a média.

To, co nás ale zajímá v bezpečnostní praxi, je provozní a bezpečnostní personál, v jehož případě může vést kognitivní útok k chybovým výkonům typu false positive, false negative nebo k chybovým výkonům obecně. V případě bezpečnostního personálu jsou nejčastěji užívanými formami útoku lest, klam, zatajení nebo přehlcení.

Někdy jsou jako typické oběti kognitivních útoků uváděny pouze osoby s nějakým kognitivním znevýhodněním nebo diskvalifikací. Specifické kognitivní nedostatečnosti, jako například nedostatečnosti v oblasti vnímání, myšlení nebo poruch paměti, pochopitelně předurčují jejich nositele k tomu, aby útočníkovi podlehli. Je však prostou skutečností, že kognitivní výkonnost kteréhokoli jedince je od ideálů a bezchybných výkonů objektivně více či méně vzdálená. Takové znevýhodňující aspekty můžeme považovat za akceleranty podlehnutí kognitivnímu útoku.

Akceleranty podlehnutí kognitivnímu útoku:

- nedostatečnost zraku
- nedostatečnost sluchu
- poruchy vnímání
- poruchy myšlení kvantitativní
- poruchy myšlení kvalitativní
- poruchy/nedostatečnost krátkodobé paměti
- poruchy/nedostatečnost dlouhodobé paměti
- specifické komunikační a informační diskvalifikanty (např. konfabulace)
- specifické vlivy chronického a akutního stresu
- snížená schopnost uvědomit si výše uvedené diskvalifikanty

Kognitivní útok je manipulativní strategie nebo technika, která zneužívá lidské myšlení, vnímání nebo emoce s cílem ovlivnit jednotlivce, skupiny nebo veřejnost tak, aby přijímali nebo vykonávali určité akce, názory nebo chování ve prospěch útočníka. Kognitivní útoky se zaměřují na ovlivnění mentálního procesu a vnímání informací, ať už prostřednictvím dezinformací, manipulace, psychologických triků, nebo zneužití lidské důvěry nebo citové zranitelnosti. Cílem kognitivních útoků může být dosažení politických, sociálních, ekonomických nebo psychologických výhod.

Na rozdíl od jiných skupin útoků, jako jsou útoky fyzické, kybernetické a další, jsou užívané kanály pro kognitivní útoky pro útočníka velmi výhodné, protože jsou zpravidla sdílené, nezřetelné, zahlcené a podceňované. Kromě nejčastějšího osobního sdělení a osobního působení na oběť se jedná o sociální sítě, zdrojové weby, redakční weby, portály, televizi, rádia, herní průmysl, podcasty, vzdělávací programy a specifická prostředí (například hlučná, prašná…).

Jaké „disciplíny“, metody a postupy používají kognitivní útočníci? Bohužel jich mají k dispozici široké spektrum – v závislosti na cílové skupině a požadovaném dopadu útoku mohou volit nejen mezi populárními dezinformacemi a phishingnem, ale mohou využívat falešných zpráv, manipulací s výrokovou logikou, techniky manipulace, falešné prezentace nebo sebeprezentace a řady dalších postupů. Řídí se přitom pouze náročností a efektivitou zvolené metody a zajištěním vlastní bezpečnosti.

Jestliže tedy útočník chce dosáhnout neschopnosti bezpečnostního pracovníka na recepci zpracovat další podněty, zahltí ho prostě velkým množstvím vjemů a vygenerovaných úloh, včetně klamných incidentů. Jestliže útočník potřebuje dosáhnout změny v bezpečnostní praxi organizace, protože taková praxe neumožňuje provedení jeho útoku, může systematicky zpochybňovat využívané postupy a metody, například ve zprávách, prezentacích, videích, nebo dokonce účelově infikovaným vystoupením na odborné konferenci.

Aktivní kognitivní útočníci:

- státní aktéři a státem sponzorovaní útočníci
- kriminální organizace
- politické subjekty
- agresivní marketing
- jednotlivec

Příklady dalších často používaných triků a postupů (také tipy pro zadání do vyhledávače):

- efekt přeživšího
- efekt vynikajícího
- falešné informace o produktu
- falešné zprávy
- framing
- gaslighting
- hrátky s výrokovou logikou
- implicitní předsudky
- konfirmační zkreslení
- manipulace veřejného mínění
- ovlivnění prostředím
- phishing
- pretexting
- skupinová polarizace
- sociální inženýrství sociálních médií
- socio-inženýrský útok
- sugerování
- techniky manipulace
- vishing
- využití mediálních prostředků
- whaling

Vzhledem k tomu, že tento článek je vytvořen podle prezentace na konferenci Ochrana měkkých cílů 2023, je vhodné na tomto místě uvést alespoň dva příklady praktické aplikace kognitivních útoků proti měkkému cíli. Půjde o příklady „malých“ útoků, vedených proti jednotlivci nebo skupině osob.

Příklad první – překonání fyzického perimetru. Jestliže útočník překonává fyzický perimetr přes recepci, může snadno užít lsti, klamu a zahlcení. Jestliže útočník s pracovníkem recepce předem telefonicky či mailem komunikuje, může se mu podařit vyvolat na straně recepce dojem nějaké chyby nebo nepochopení, jejichž řešení je spojené s následnou omluvou, pochopením a třeba i humorem a útočník pak už přichází do objektu většinou za situace, kdy je k němu recepce vstřícná a předem kooperativně naladěná. Pokud zároveň spolupracovník útočníka zajistí (například špatným parkováním, hlukem, obtěžujícími telefonáty, rozlitím nápoje, nebo nejlépe kombinací více faktorů) vyčerpání momentální kognitivní kapacity pracovníka recepce a pokud svůj příběh doplní paralelně generovanou konfirmací svého tvrzení například emailem, je jeho šance na překonání perimetru velmi silná. V extrémních případech může útočník překonání perimetru spojit s vyvoláním bezpečnostního nebo požárního poplachu nebo s odepřením služby telekomunikačního systému.

Příklad druhý – posílení dopadu útoku proti návštěvníkům. Typickým postupem zvoleným pro útok proti návštěvníkům může být opakované vyvolání bezpečnostní nebo požární signalizace s cílem jejího následného podcenění při skutečné bezpečnostní události. Ve fyzicky složitém prostředí může být útok daleko prostší – stačí odstranit, případně zakrýt jednu nebo dvě evakuační šipky. Evakuující se dav je možné ovlivnit také osvětlením nebo naopak absencí osvětlení. Zakouřením evakuační trasy dýmovnicí lze osoby snadno odklonit z bezpečné trasy do místa, kde je skutečná hrozba. Byly zaznamenány případy zapálení nebo exploze vozidla s cílem vyvolání dojmu, že evakuace je nebezpečná, nebo útočníci vydávající se za policii, lákající ukryté osoby z bezpečné místnosti.

Proč je úspěšné provedení kognitivního útoku tak často spojené s umělým vytvořením výše naznačených situací, generujících silný, akutní stres, lhostejno zda emotivní nebo kognitivní? Je to vyzkoušený a efektivní postup. Mezi obvyklé reakce na akutní stres patří, kromě dalších, tunelové vidění, inhibice sluchu, strach, napětí, úzkost, agrese, ztráta flexibility, překotná rozhodnutí, nevhodný výběr priorit, poruchy paměti, poruchy logického myšlení, poruchy koncentrace či zmrazení. Lze si představit vhodnější prerekvizity úspěšného kognitivního útoku? Jen stěží.

Ukažme si na něj prstem

Vždy, když na nás někdo útočí, potřebujeme vědět, kdo to je. Jinak je naše obrana poloslepá a polohluchá. Problémem atribuce (také přičitatelnosti – té části analýzy útoku, kdy se snažíme identifikovat, kdo stojí za útokem, kdo ho provedl a jaké jsou jeho cíle) kognitivních útoků je, že selhávají běžné metody, užívané pro fyzické nebo kybernetické útoky.

Obvykle se však potýkáme s nedostatkem dat, komplexitou útoku, pozdní detekcí, nepochopením záměru útočníka, pestrostí typologie útočníků, různými vektory útoku, včetně jejich řetězení a paralelizace, s neznámou vzdáleností ke zdroji, malým odstupem „signálu od šumu“, neexistencí exaktních stop, snahou rychle „na někoho ukázat“ a dlouhou řadou dalších problémů. Často jsme odkázáni na různé formy příznakové nebo dopadové atribuce s velkým rizikem fatální chyby.

Známé atribuční modely, jako jsou ATRIUM, Diamond Model, Mitre ATT&CK, Q-model (technicko-operačně-strategická komunikační úroveň), selhávají. Relativně dobře je použitelná téměř již prehistorická Analýza konkurenčních hypotéz, pro laiky jsou ale nejlépe použitelné jednoduché modely jako algoritmus známý z útoku Equifax attack 2017.

Dříve publikované atribuční schéma, použité při útoku Equitax attack 2017:

- Identifikace a popis útoku za účelem zahájení procesu atribuce.
- Shromáždění dostupných informací, které se týkají útočníka, cílů útoku a používaných metod, s cílem získat komplexní povědomí o útoku.
- Analýza získaných informací a tvorba profilu útočníka, který poskytne hlubší porozumění jeho motivacím a způsobům útoku.
- Identifikace potenciálních důvodů a motivací, které mohou stát za provedením útoku, s cílem poskytnout vysvětlení pro jeho původ.
- Porovnání současného útoku s předchozími incidenty a jejich atribucemi za účelem odhalení případných vzorců a souvislostí.
- Zhodnocení důvěryhodnosti a spolehlivosti použitých zdrojů informací s cílem zajištění přesnosti a spolehlivosti dat.
- Posouzení konzistence a koherence získaných informací z různých zdrojů s cílem zajistit věrohodnost a přesnost analýzy.
- Zhodnocení důležitosti a relevance jednotlivých faktorů a informací.
- Identifikace nejasností nebo nezodpovězených otázek, které vyžadují další prozkoumání a objasnění.
- Vyvození závěrů o původu a pachatelích útoku.

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČESKÉ REPUBLIKY

Ještě složitější než atribuce, s cílem relativně bezpečného veřejného označení viníka, je obstarávání důkazů, které obstojí před soudem. Kognitivní útoky jsou často založeny na využití psychologických triků a manipulace, jež bývá v rámci soudních procesů zpravidla obtížné prokázat. To má vliv má charakter atribuce a právní odpovědnost útočníků.

Jak se bránit?

Základem je prevence. Základem prevence jsou pak analýzy rizik, vzdělávání, informační kampaně, procvičování, drilování. Dobré je trivializovat a algoritmizovat bezpečnostní procedury. Příkladem dobré trivializace a algoritmizace je klasický a legendární návod pro použití ručního hasicího přístroje (odjistit-namířit-hasit), spojený s nezaměnitelnou grafikou.

Pracovník na bezpečnostně relevantní pozici musí být veden k tomu, aby rozpoznal své hranice. Jedním ze základních prvků bezpečnostní výbavy postupů kontaktních pracovníků jsou funkční fráze, které v takových situacích použijí. Správné použití věty typu „Teď ne prosím", „Kolega je již na cestě sem", nebo „Požární poplach, opusťte prostor dveřmi vpravo" pronesené se správnou dikcí ve správné chvíli, kdy pracovník nezvládá nápor souběžných požadavků, může být pro ochranu objektu efektivnější než křik a vystříkaný pepřový sprej.

Pokud bezpečnostní pracovník nezvládne řídit svou okamžitou zátěž a odpírat další požadavky, může snadno vyčerpat celou svou kognitivní kapacitu a stát se tak zranitelným, jak jen útočník potřebuje. To vše lze školit, cvičit, drilovat a připravovat do pracovních postupů.

Trivializace ergonomie bezpečnostních sdělení a pokynů

- analyzovat, analyzovat, analyzovat
- minimalizovat, minimalizovat, minimalizovat
- neustále ověřovat soulad s účelem a cíli projektu
- měřit, sbírat zpětnou vazbu, monitorovat
- zapojit testery z cílové skupiny, včetně osob s kognitivním omezením
- neustále zlepšovat, vyvarovat se však změn základních výrazových prostředků

Je třeba poskytnout personálu i návštěvníkům dostatek informací, které si nebudou odporovat. Systém kognitivní ochrany musí být složený nejen ze školení a cvičení, ale také z úpravy prostředí, hlášení, brožurek, videí, článků, řádů, směrnic, tabulek, bezpečnostních postupů a algoritmů. Vše, co může být trivializováno, musí být stejně jednoduché jako výše zmíněný návod k použití hasicího přístroje. Ergonomie bezpečnostních manuálů, karet a tabulek, ale třeba i směrovek musí být podřízena tomu, že je budou používat osoby pod vlivem akutního stresu, a konzumace složitého textu vyčerpá podstatnou část jejich kognitivních kapacit – ty pak mohou chybět při krizové komunikaci nebo rozpoznání zlomyslně předložené nepravdy, klamu či zavádějící informace.

Elementárním a nepominutelným východiskem pro posilování odolnosti lidského faktoru, procesů i vhodnosti prostředí je správně, logicky a efektivně zavedený systém trvalého zlepšování. Může být postaven na některém z konceptů kvality managementu, prosté implementaci PDCA cyklu, logice norem ISO řady 9000 nebo standardů NIST. Je v zásadě jedno, jaké metodické východisko organizace zvolí. Stačí, že příslušný koncept podporuje sériové a cyklické vazby mezi poznáním, analýzou, plánováním, návrhem, testováním, implementací, detekcí, dokumentací, syntézou a dalšími notoricky známými elementy procesů trvalého zlepšování kvality. Bez trvalé péče systém kognitivní obrany selhává.

Pro úroveň ochrany měkkého cíle jsou také podstatné přesahy nebo dopady „velkých" kognitivních kampaní na celospolečenské úrovni do naladění a výkonnosti bezpečnostně relevantních pracovníků. To bylo znatelné například v době covidu, kdy velké kampaně měly často dopad na individuální motivaci a výkonnost jednotlivých bezpečnostních pracovníků (do jisté míry to také souviselo s kumulativním efektem souběžně působícího chronického a akutního tresu). Tyto vnější vlivy je třeba včas detekovat a analyzovat jejich dopad na odolnost bezpečnostně relevantních rolí.

Vynikajícím zdrojem informací, publikací a úvah o kognitivním útočení jsou webové stránky a publikace NATO Allied Command Transformation. Na nich stačí vyhledat výskyt řetězce „Cognitive Warfare" a rázem máte zábavu na celý víkend a poučení na celý rok.

Pokud Vás zajímají témata odolnosti lidského faktoru nebo ergonomie bezpečnostně relevantních komuniké, neváhejte mě kontaktovat. Roboti a umělá inteligence to (zatím) sami nezvládnou.

PaedDr. Martin Uher, MBA
ARBATAX s.r.o. a Securo.Pro

Poznámka redakce: Autor se okolnostem lidského faktoru v bezpečnosti věnuje v oblastech tvorby procesů, vzdělávání, penetračního testování a synergií technologických a personálních řešení.

MGR. PAVLEM BĚLOHRADSKÝM Z IBIPC

ROZHOVOR

INSTITUTE OF BLAST & IMPACT PROOF CONCRETE

Počátkem června 2023 jste vystoupil na konferenci Ochrana měkkých cílů. Ve svém příspěvku jste se zaměřil na problematiku terorismu, sabotáží a hybridního konfliktu. Proč právě tato témata?

Důvod je jasný. Současná bezpečnostní situace v Evropě se v průběhu jediného roku radikálně změnila a adekvátní proměnou prochází také naše myšlení, byť míra dynamiky je poněkud nižší. Člověk si podvědomě jen nerad připouští negativní skutečnost, že kyvadlo dějin Starého kontinentu, zatíženého dvěma světovými konflikty, se opět přibližuje ohnisku válečné vřavy.

Víte, změna každého stavu může nastat pouze dvěma způsoby. Buď postupnou evolucí, nebo radikální revolucí; a dle teorie Charlese Darwina ji přežijí pouze jedinci druhu, kteří jsou schopni se prostředí nejlépe přizpůsobit. Jak se my přizpůsobíme očekávané změně? Záměrem mého vystoupení bylo upozornit na hrozby důsledků ukrajinského konfliktu v souvislostech evropského regionu a nabídnout preventivní řešení proti některým z nich.

Domnívám se, že většině našich obyvatel je stále vzdálené ztotožnit se reálně s takovou situací. Žijí v představě, že se jich válka netýká, že je daleko. Pokud však připustíme Vaše závěry, jak jsme na případný konflikt připraveni?

Jsem toho názoru, že do této etapy dějinného období vystupujeme jako jedinci absolutně nepřipraveni, a krátce vysvětlím proč. Pro věc je určující absence vlastního poznání, které je nepřenositelné a které v čase mizí v propadlišti dějin. Sám jsem narozen 15 let po druhé světové válce; jako děti jsme si hráli na partyzány, v místním Kovošrotu usedali za rajčáky tanků či kniply letadel a bojovali po vzoru našich dědů s nepřítelem.

Doma jsme poslouchali příběhy hrdinů odboje, vyprávění rodičů, jak se pod nimi zdvíhala země při bombardování, o hrůzách Lidic a Ležáků, o denně vydávaných seznamech popravených vlastenců v období heydrichiády. Držel jsem v rukou dědův Československý válečný kříž 1939 a československou medaili Za chrabrost, listoval v sešitu přídělových lístků na základní potraviny, na půdě jsme měli od války schované ostré náboje a pistoli, jako klukovi mi to přišlo úplně normální. Ve škole branná výchova s přípravou na jaderný konflikt, pochodová cvičení s prostředky individuální protichemické obrany, hodem granátem na cíl a střílením. Všichni muži prošli dvouletým drilem vojenské služby, ovládáním techniky, ostrými střelbami.

V takovém prostředí vyrůstala celá naše generace; prožívali jsme období studené války a byli, většinou proti vlastní vůli, metodicky připravováni včetně vnitřního mentálního nastavení na budoucí globální konflikt. Tyto zkušenosti a poznatky u mladé generace zcela absentují, dosud není vytvořen funkční systém ochrany k výchově odborníků či obyvatel. Chybí jednoznačná strategie, systematika, metodika, vzdělávání a publicita. Jejich zavedení potřebuje politickou podporu, čas a peníze; není ani jedno z toho. Pokud by byl vyhlášen krizový stav ohrožení státu nebo válečný stav, nezbude čas na jakoukoli prevenci a bude to řešit každý sám za sebe.

Promiňte, ale s tím se nemohu zcela ztotožnit, máme přece vytvořenou Koncepci ochrany obyvatelstva, složky civilní ochrany i obrany, nejsou snad v takovém mimořádném případě veřejnosti k dispozici alespoň kryty, včetně jaderných bunkrů?

Jsou, ale já sám nevím, kde je konkrétně najdu, ve městech chybí jakákoli vizuální navigace, postrádám základní koncepční informovanost a edukaci ze strany státu. A technický stav krytů? Co můžeme čekat po třiceti letech? To je „otázka za sto bodů"! V jakém stavu asi budou filtro-ventilační systémy, jak funkční jsou filtry proti bojovým plynům, biologickým zbraním či proti jadernému spadu? Jsou v dostatečném množství připraveny zásoby dehydrovaných potravin a pitné vody, přikrývek, hygienických potřeb, generátorů a zásob paliva do nich? Jsou tam v provozuschopném stavu, a jsou tam vůbec? Je pro 10 mil obyvatel naší vlasti postačující celková kapacita 250 bunkrů proti jadernému útoku a dalších 6 tisíc krytů civilní obrany? Jak jsou doopravdy vybaveny, zabezpečeny, zpřístupněny k bezodkladnému použití? Jsou zpracovány závazné režimové dokumenty pro pobyt v nich? Kdo z nás zná odpovědi?

To je jen část otázek k dané problematice, kterými se jako členové specializované Security Bunkers Aliance zabýváme a se kterými bychom chtěli pomoci řešit situaci vládě, ministerstvu vnitra i obrany a IZS. Jsme schopni nabídnout ve spojení s dalšími partnery revize, rekonstrukce, opravy i zodolnění stávajících dispozičních řešení, anebo výstavbu nových, vysoce odolných krytů civilní obrany s nejmodernějším vybavením, certifikovaných na balistickou, výbuchovou a střepinovou odolnost Vojenským výzkumným ústavem.

Domnívám se, že na úrovni státu je nutné bezodkladně přijmout potřebná opatření pro zajištění krytů vojenské a civilní obrany s předstihem. Zejména v rámci Dílčího plánu obrany ČR v oblasti obrany za stavu ohrožení státu nebo válečného stavu a Národního systému reakce na krize je potřebné obzvlášť posílit schopnost reagovat na rizika související s vnějším napadením ČR nebo jejích spojenců, kdy není zajištěna, respektive dochází k ohrožení bezpečnostní situace obyvatel našeho státu. Je zřejmé, že na případ napadení agresorem není dobře připravena žádná země EU, vlády většiny z nich to však již pochopily.

Náčelník generálního štábu AČR uvádí, že v případě konfliktu Ruska a NATO bychom byli jeho účastníkem od první minuty. Vládní představitelé prohlašují, že jsme ve válce, mění se Bezpečnostní koncepce ČR. Jsem přesvědčen, že kromě zbrojení musí vláda ČR myslet na obyvatele a zajistit jim do této proklamované změny zázemí a místo pro bezpečný pobyt.

Děkuji za rozhovor.

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

Společnost byla založena v roce 2016 jako INSTITUT OCHRANNÝCH BETONOVÝCH KONSTRUKCÍ (později Institute of Blast & Impact Proof Concrete) s cílem vyvinout společně s Fakultou stavební ČVUT Praha ultra-vysokopevnostní beton s rozptýlenou výztuží z mikrovláken vysokopevnostní oceli (který je pevný, odolný a přitom pohlcuje energii při zachování tvarové stálosti) a ve spolupráci s Katedrou ženijních konstrukcí Univerzity obrany v Brně vytvořit z betonu bezpečnostní prvky.

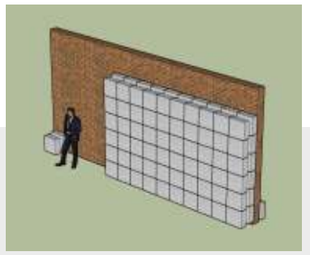
První produkce byla vystavována na veletrzích IDET Brno a ARMY Moskva, pokračoval výzkum a vývoj, změnil se název a logo, byla podepsána licenční smlouva s ČVUT, zajištěny testy a certifikace u Vojenského výzkumného ústavu na balistickou, výbuchovou a střepinovou odolnost dle NATO STANAG 2280:2016, Ed. 2 nejvyšších hodnot: A5, C4, D6. Vlastnosti deklarované patenty jsou ověřeny certifikátem ve Státní zkušebně ČVUT Praha. Duševní a průmyslová práva produktů jsou chráněna Evropským patentem a průmyslovými vzory. Firma uzavřela strategické partnerství s klíčovými partnery CS BETON, WITKOWITZ a VVÚ, jakož i řadou dalších specializovaných firem.

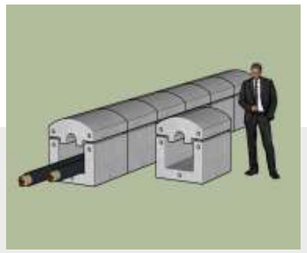
Bezpečnostní prvky IBIPC poskytují vysokou míru ochrany cílů prvního napadení, objektů důležitých pro obranu státu a vojenské i civilní infrastruktury, chrání proti hrozbám sabotáže a teroristického útoku, hybridnímu útoku a útoku profesionální armády. Nově vyvinutá ucelená řada světově jedinečných HI TEC bezpečnostních prvků přináší schopnost rychle reagovat na definované hrozby v případě mimořádné situace, stavu ohrožení státu a válečného stavu. Od bezpečnostních laviček přes balistické stěny, checkpointy a bunkry s filtroventilačním systémem po zodolněné kryty stíhacích letounů.

IBIPC je spolu s americkou Singleton Group International zakladatelem mezinárodního Joint Venture Trusted Alliance a členem Security Bunker Alliance. Je spolehlivým partnerem pro MO, armádu, policii, bezpečnostní složky a civilní obranu zejména států EU a NATO.

IBIPC
INSTITUTE OF BLAST & IMPACT PROOF CONCRETE
MADE TO SAVE YOU

PŘEDNÍ DODAVATEL BEZPEČNOSTNÍCH ŘEŠENÍ PRO OBRANNÝ PRŮMYSL, KRITICKOU INFRASTRUKTURU I CIVILNÍ OBRANU, KTERÉ CHRÁNÍ LIDI, OBCHOD A SPOLEČNOST





PRODUKTOVÁ ŘADA 2023 – VYUŽITÍ OCHRANNÝCH PRVKŮ IBIPC

Všechny prvky IBIPC mají požadované certifikáty dle NATO STANAG 2280:2016 Edice 2, splňují podmínky vysoké ochrany před ručními těžkými zbraněmi, střepinovým účinkem a výbuchy následující úrovně:

- A5 – střela 14,5 x 114 API M32
- C4 – raketa 107 mm / minometný granát 120 mm
- D6 – odolnost do 50 kg TNT

Průzory prvků Bunkr, Kryt a Checkpoint jsou osazeny neprůstřelným balistickým sklem dle normy NATO STANAG 4569 úrovně IV a splňují adekvátní podmínky ochrany cestujících v obrněných vozidlech před údery kinetickou energií, dělostřelectvem a výbuchy improvizovaných výbušných zařízení. Povrch všech prvků je ošetřen základním krycím nátěrem UNIVERSUM CAMOUFLAGE PATTERN, v opci osmi dalších kamuflážních barev dle standardu NATO M.E.R.D.E.C.

BALISTICKÉ STĚNY

a) Ochrana vojenské infrastruktury

Letecké úly, stanoviště řízení letů, velitelská stanoviště a stanoviště radarových systémů, skladů leteckého paliva, stanovišť protivzdušné obrany státu a ostatních vybraných objektů letištní infrastruktury – muničních skladů, skladů pohonných hmot, parků bojové techniky, stanovišť protivzdušné obrany, objektů velení a ostatních důležitých objektů pozemní infrastruktury.

b) Ochrana civilní infrastruktury

To je elektráren, trafostanic, důležitých skladů pro zásobování obyvatelstva, zásobáren pitné vody, nemocnic a jejich náhradních generátorů a ostatních důležitých objektů civilní infrastruktury.

MOBILNÍ BUNKRY

Prvosledová stanoviště ke zpomalení či zastavení útoku protivníka. Variabilně osazená univerzálními segmenty se střílnami, průzory, pancéřovými dveřmi, nouzovými východy a filtroventilačními systémy. Umístění mobilního bunkru v terénu dle taktické situace, konfigurace vyrobená na klíč dle zadání klienta.

KRYTY CIVILNÍ OBRANY

Použití jako prostředek úkrytu civilních osob v případě leteckého napadení nebo ostřelování raketovým vojskem a dělostřelectvem. Umístění – instituce, školky a školy, nemocnice, kritická infrastruktura atd. Ochranu lze zvýšit zakrytím pytli s pískem či uložením do země.

CHECKPOINTY

Pro posílení obrany na státní hranici, zesílení vnějších perimetrů vojenských a civilních letišť, zesílení obrany na mostech a důležitých tranzitních tepnách, zesílení obrany kritické a civilní infrastruktury.

BALISTICKÉ BETONOVÉ LAVIČKY A KVĚTINOVÉ BOXY

Pro zesílení obrany vnitřních perimetrů vojenských a civilních letišť, ochrany cizích ambasád, budov veřejné samosprávy, přístupových komunikací do městských center, obrany kritické infrastruktury – jak vojenské, tak civilní.

BALISTICKÉ DESKY

Pro zesílení stěn důležitých staveb infrastruktury, vojenských objektů a objektů ochrany obyvatelstva.

BETONOVÉ PYRAMIDY

Pro vytvoření zátarasů na státní hranici, zátarasů na hlavních transportních tepnách, na přístupových cestách k městským aglomeracím, na důležitých mostech a vodních tocích a na přístupových komunikacích k objektům kritické vojenské a civilní infrastruktury.

TUNELY K OCHRANĚ KABELŮ VYSOKÉ PRIORITY

Systém sloužící k ochraně elektrického vedení, optických kabelů, IT pracovišť a systémů IOT technologií kritické vojenské a civilní infrastruktury.

ZESÍLENÉ ÚKRYTY LETADEL

Nepostradatelná součást letištní infrastruktury. Prostorově tuhý a odolný polotubus k bezpečnému ukrytí stíhacích letounů na vojenských základnách, zejména v hraničních oblastech. Schopnost eliminace propustnosti rádiového, infračerveného a jaderného záření.

MOBILNÍ T - STĚNA

Pro rychlé vytvoření vysoké úrovně bezpečnostního opatření vojenských a civilních objektů. Pro zesílení obrany vnitřních perimetrů, přístupových komunikací do městských center, na kontrolní propouštěcí místa, před vstupy a vjezdy do objektů, ke kontrole vozidel.

WWW.IBIPC.COM

CHYTRÁ ŘEŠENÍ PRO DIGITÁLNÍ MĚSTA

Ivo Popardowski působí v branži ochrany majetku a osob již přes dvacet let. Je zakladatelem a generálním ředitelem ABAS IPS Management. Z lokální firmy vybudoval středoevropskou společnost, která zavádí moderní technologie. Přitom nezapomíná na svou vášeň pro výtvarné umění, jehož hodnoty vnímá i jako člověk sběratel. Je zakladatelem občanského sdružení pro podporu obecně prospěšných činností.

Fyzická bezpečnost v sobě zahrnuje i bezpečnost firem a osob. Jak se vyvíjejí moderní technologie v tomto segmentu?

Bezpečnost je v dnešní době souborem komplexních služeb, z nichž každá má svůj specifický vývoj. Pokud bych ale měl jmenovat klíčové trendy, které prolínají všemi jejími segmenty společně, pak je to z pohledu vlastních bezpečnostních technologií posun od využívání umělé inteligence k tzv. akční inteligenci. Z hlediska související legislativy se jedná o návrhy k zavádění nových standardů. A důležité je zmínit také aspekt bezpečného prostředí jako faktoru kvality životní úrovně, který vzniká vzájemným provazováním ryze bezpečnostních a komunikačních technologií, a to na všech úrovních každodenního života (internet věcí – IoT, SMART City).

Umělá inteligence v oblasti fyzické bezpečnosti – co si pod tím můžeme představit?

Technologický posun je v oblasti fyzické bezpečnosti nejmarkantnější především u videodohledových systémů. Použiji tedy příklady z tohoto odvětví. Původní analogové kamerové systémy používaly již od konce 90. let k zaznamenávání podezřelých aktivit, jako jsou například opuštěná zavazadla, videodetekci. A ačkoli z dnešního úhlu pohledu šlo spíš jen o hrubé rozpoznávání změn jasu v obraze, v oboru fyzické bezpečnosti se jednalo o přelom ve způsobu vzdáleného dohledu. Detekce však byla jen doplňkovou službou a její využití z pohledu obchodu marginální.

Z pohledu uživatele šlo navíc v podstatě o pasivní přístup, vyhodnocování děje probíhalo se zpožděním a ve výsledku se jednalo o nespolehlivé procesy s množstvím provozních chyb a falešných poplachů. Dnešní kamerové systémy využívají jak umělou inteligenci, tak i strojové učení. Bezpečnostní trh nepovažuje analytiku jako doplněk, ale jako pevný základ.

Poskytovatelé bezpečnostních služeb se díky tomu mohou soustředit na takřka libovolné analýzy, které jim s vysokou přesností pomáhají klasifikovat naprosto rozdílné objekty a operativně vyhodnocovat dopad jejich (ne)přítomnosti. To vše s aktivním využitím dat v on-line prostředí a v různých scénářích. Už nejsme ve stadiu, kdy nás inteligentní funkce jen upozorňují, že něco není v pořádku, ale rovnou nám pomohou zvolit vhodnou reakci. Mezi odborníky se říká, že jsme se posunuli „od analytiky k akci", a toto si už začínají uvědomovat i potenciální uživatelé. Poptávka po proaktivním využití kamer jako vzdálených senzorů to potvrzuje. Pokud bych měl z množství používaných analytik poukázat na ta nejčastější, poukázal bych na takřka neomezené vyhodnocování chování lidí ve sledovaném prostoru a čtení registračních značek vozidel (ANPR), včetně doprovodných informací o rychlosti, typu a barvě identifikovaného vozidla.

Využití takových dat už není jen doménou bezpečnosti. Vyhodnocovací algoritmy si zde najdou také specialisté z oblastí marketingu, retailu, logistiky, ale také stavitelé chytrých měst. Z globálnějšího pohledu je na místě upozornit, že kamera je jen jedním ze senzorů v rámci celku zvaného internet věcí. Je tedy naprosto zřejmé, že umělá inteligence mění nejen bezpečnostní sektor.

Zmínil jste chytrá města. S nimi úzce souvisí tzv. smart řešení, tedy trend hledající řešení snižující náklady nejen firem, ale i obcí, měst a krajů. Co zajímavého nabízíte samosprávám?

Na úrovni samosprávy je toho k využití nepoměrně více. Nebavíme se již o dílčích částech, ale o komplexním řešení. Z pohledu kvality života ve smyslu smart se zde nejvíce mluví o uplatnění v dopravě, životním prostředí, úrovni bydlení, o lidech, co tu žijí, a o správě města.

Každé město, které se vydalo směrem k chytrým řešením, můžeme nazývat také městem digitálním. Jedná se o koncept, kdy jsou za účelem efektivnějšího využití infrastruktury a snížení spotřeby energií plošně využívány digitální, informační a komunikační technologie. Kromě klasických komerčních subjektů se zde také objevují i prvky kritické infrastruktury státu. I zde tak hraje podstatnou roli bezpečnost.

Když se oprostíme od kamer, je dle mého názoru nejpodstatnější dostatečná kapacita dat. Následně jejich zabezpečení a kvalifikovaná obsluha. Bezpečnostní sektor byl vždy zvyklý na provozní režim 24/7 a aplikace chytrého města jsou v provozu také 24 hodin denně a 7 dní v týdnu, což je skutečnost, na kterou nebyla samospráva zvyklá. Budou pro ni tedy zajímavé služby komerčních firem, které provozují praxi prověřená a nezávislým orgánem certifikovaná dohledová a poplachová přijímací centra.

Tak jako byl při přechodu na IP technologie rozšířen vzdálený monitoring poplachů o audio/video dohled s obousměrnou komunikací, tak nyní dochází k zapojení umělé inteligence a internetu věcí. V rámci profesionálních dohledových center vznikají datová úložiště a jsou provozována cloudová řešení. A mezi tolik používané pojmy jako bezpečnost a smart tak lze pomalu dát rovnítko.

Každé z nastíněných témat by si určitě zasloužilo detailnější rozbor, ale kdybyste měl závěrem říci jednu myšlenku, která by to byla?

Pokročilé senzory mají už nyní obrovský vliv na to, aby prostředí, ve kterém žijeme, bylo chytřejší, bezpečnější a efektivnější. Když se nad tím zamyslím, dovolil bych si tvrdit, že přítomností umělé inteligence v bezpečnostních systémech v kombinaci s internetem věcí a provozem cloudu se posouváme k dalším fázím využití technologie nejen pro bezpečnost, ale také pro provozní a obchodní účely.

Děkuji za rozhovor.

Redakce BsP

MINIMALIZACE NÁSILNÉHO JEDNÁNÍ VŮČI ZAMĚSTNANCŮM NA PRACOVIŠTÍCH

S DŮRAZEM NA ZKUŠENOSTI ÚŘADU PRÁCE ČESKÉ REPUBLIKY

Cílem tohoto článku, který bude mít pokračování v dalších číslech BsP, je zmapovat prostředky ochrany zaměstnanců proti násilnému jednání na pracovištích, se zohledněním zkušeností Úřadu práce České republiky. V první části textu je pozornost zaměřena na úřední osoby a násilí vůči nim na pracovištích, kde tyto osoby pracují – s využitím zkušeností z poměrně specifického prostředí Úřadu práce České republiky (respektive jeho poboček a pracovišť).

Právě s ohledem na tyto zkušenosti se článek více zaměřuje na ochranu úředních osob proti násilným incidentům, které se sice odehrály na pracovišti, ale ponejvíce ze strany klientů vůči nim, ne v rámci pracovněprávních vztahů.

Právní úprava ve vztahu k tématu násilí vůči úředním osobám

Ochrana při výkonu pravomoci z hlediska přestupkového práva

Ochranu při výkonu pravomoci úřední osoby lze najít i v oblasti práva přestupkového. V zákoně č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, v platném znění, se v § 5 definuje přestupek jako společensky škodlivý protiprávní čin, který je v zákoně za přestupek výslovně označen a který vykazuje znaky stanovené zákonem, nejedná-li se o trestný čin.

Zákon č. 251/2016 Sb., o některých přestupcích, v platném znění, pak definuje v § 5 specifické přestupky proti veřejnému pořádku. Přestupek je spáchán, pokud pachatel podle § 5, odst. 1, písm. b) zneváží postavení úřední osoby při výkonu její pravomoci.

Za tento přestupek lze dle odst. 3 uložit pokutu do výše 10 000 Kč, jde-li o přestupek za znevážení postavení úřední osoby při výkonu její pravomoci; v případě opakování téhož přestupku po nabytí účinnosti rozhodnutí o přestupku stejného charakteru pak pokutu až do výše 15 000 Kč.

Postavení úředních osob z hlediska trestního práva

Ve vztahu k násilí vůči zaměstnancům veřejných institucí při výkonu služby (tedy násilí „zvnějšku" vůči úředním osobám) je relevantní úprava obsažená v zákoně č. 40/2009 Sb., trestním zákoníku, v platném znění, který v § 127, odst. 1 vyjmenovává jako úřední osoby následující pozice:

- a) soudce,
- b) státní zástupce,
- c) prezident České republiky, poslanec nebo senátor Parlamentu České republiky, člen vlády České republiky nebo jiná osoba zastávající funkci v jiném orgánu veřejné moci,
- d) člen zastupitelstva nebo odpovědný úředník územní samosprávy, orgánu státní správy nebo jiného orgánu veřejné moci,
- e) příslušník ozbrojených sil nebo bezpečnostního sboru nebo strážník obecní policie,
- f) soudní exekutor při výkonu exekuční činnosti a při činnostech vykonávaných z pověření soudu nebo státního zástupce,
- g) notář při provádění úkonů v řízení o dědictví jako soudní komisař,
- h) finanční arbitr a jeho zástupce,
- i) fyzická osoba, která byla ustanovena lesní stráží, stráží přírody, mysliveckou stráží nebo rybářskou stráží, pokud plní úkoly státu nebo společnosti a používá při tom svěřené pravomoci pro plnění těchto úkolů.

Navazující odstavec 2 stejného paragrafu trestního zákoníku dodává, že /.../ k trestní odpovědnosti a ochraně úřední osoby se podle jednotlivých ustanovení trestního zákona vyžaduje, aby byl trestný čin spáchán v souvislosti s její pravomocí a odpovědností.

Násilí spáchané na těchto úředních osobách při výkonu jejich pravomoci je dle § 325 trestního zákoníku považováno za specifický trestný čin násilí proti úřední osobě, který je podle intenzity provinění hodnocen trestní sazbou odnětí svobody až na 4 roky, v závažnějších případech, které jsou upraveny zvláštními skutkovými podstatami, jsou stanoveny vyšší trestní sazby. V případě nejzávažnějším z kvalifikovaných skutkových podstat dle odst. 4 citovaného ustanovení (způsobí-li pachatel svým činem smrt) se jedná o trest odnětí svobody na 8 až 16 let.

Trestným činem je podle § 326 trestního zákoníku i vyhrožování s cílem působit na úřední osobu, za které může být pachateli uložen trest odnětí svobody až na 3 roky, resp. na 5 let v případě, spáchá-li uvedený čin se zbraní. Skutková podstata tohoto trestného činu postihuje jednání spočívající ve vyhrožování jinému usmrcením, ublížením na zdraví nebo způsobením značné škody v úmyslu působit na výkon pravomoci úřední osoby nebo pro výkon pravomoci úřední osoby. Výčet výhrůžek je přitom taxativní a podle této skutkové podstaty tedy nelze stíhat jednání spočívající například ve vyhrožování omezením osobní svobody či pomluvou či menší škodou, než je škoda značná (což je dle § 138 trestního zákoníku škoda minimálně 1 000 000 Kč). Z hlediska působení na jednání úředních osob se přitom i v těchto případech může jednat o vyhrožování, které je vnímáno obdobně úkorně jako vyhrožování ublížením na zdraví. V tomto smyslu je tedy diskutabilní, zda je ochrana úředních osob v trestně právní rovině dostatečná.

Z výše uvedeného lze dovodit, že z pohledu trestního zákoníku požívají úřední osoby při výkonu své pravomoci určité míry vyšší zákonné ochrany. Záleží pak na intenzitě jednání, zda toto naplní znaky trestného činu.

Trestným činem je dle § 13 trestního zákoníku protiprávní čin, který trestní zákoník označuje za trestný a který vykazuje znaky uvedené v takovém zákoně. Zákon dále předpokládá, že k trestní odpovědnosti za trestný čin je třeba úmyslného zavinění, nestanoví-li trestní zákoník výslovně, že postačí zavinění z nedbalosti.

Dílčí shrnutí k právní úpravě problematiky ochrany zaměstnanců proti násilnému jednání

Právní rámec České republiky se dotýká oblasti násilí na pracovištích (včetně pracovišť veřejné správy) spíše v obecné rovině. Pokud konkrétní organizace chce cíleně tuto oblast a konkrétní postupy uvnitř organizace k ochraně svých zaměstnanců nastavit, musí tak při vědomí legislativní úpravy a s přihlédnutím k tzv. „nejlepší praxi" provést úpravu postupů za využití relevantní interní směrnice.

Analýza situace v rámci Úřadu práce České republiky

Úřad práce České republiky využívá pro evidenci násilného jednání na pracovištích webovou aplikaci, do které mají přístup všichni zaměstnanci, kontrolní vstupy pak mají vedoucí představitelé Úřadu. Tato webová aplikace slouží primárně k evidenci jednotlivých incidentů a následné práci s nimi (zajištění podpory a ochrany zaměstnanců, preventivní opatření do budoucna apod.). Aplikace se stále vyvíjí, nicméně se díky ní již podařilo nashromáždit relevantní data, která jsou popsána níže.

V krátkém sledu byly v rámci Úřadu práce ČR vydány v minulých letech vnitřní předpisy, které se týkají bezpečnostní agendy:

- Rozhodnutí generální ředitelky č. 6/2016: „Zřízení odborné pracovní skupiny generálního ředitelství Úřadu práce České republiky pro zajištění bezpečnosti pracovišť Úřadu práce České republiky".
- Rozhodnutí ředitele odboru správy majetku, provozu a investic č. 12/2016: „Postup při uplatňování opatření pro zajištění bezpečnosti pracovišť Úřadu práce České republiky v rámci realizace investičních akcí".
- Směrnice generální ředitelky č. 10/2017: „Rámcový standard pro řešení bezpečnosti na jednotlivých pracovištích Úřadu práce České republiky".
- Směrnice generálního ředitele č. 6/2022: „Rámcový standard pro řešení bezpečnosti na jednotlivých pracovištích Úřadu práce České republiky a složení odborné pracovní skupiny pro bezpečnost", který výše uvedené předpisy ruší a nahrazuje.

Tyto vnitřní předpisy řeší ovšem spíše technickou stránku zabezpečení pracovišť v reakci na ohrožení zaměstnanců Úřadu ze strany klientů a dalších návštěvníků Úřadu. Rovněž se předpokládá provedení analýzy rizik jednotlivých pracovišť (metoda a způsob provedení této analýzy nejsou v interních předpisech uvedeny, i když jednotlivé prostory jsou rozděleny podle míry rizikovosti).

Jak již bylo uvedeno, Úřad práce České republiky zavedl reportování incidentů prostřednictvím webové aplikace. Data získaná díky evidování jednotlivých incidentů vůči zaměstnancům ukazují, že násilné incidenty, které se na pracovištích Úřadu odehrávají, v drtivé většině nesouvisí se vztahy mezi zaměstnanci. Bohužel však dochází k opakovaným násilným incidentům vedeným proti zaměstnancům poboček Úřadu v souvislosti s jejich zaměstnáním či výkonem státní správy, a to bohužel i s fatálními následky.

Jak bude demonstrováno v tabulkách s daty získanými prostřednictvím aplikace (v příštím čísle BsP), lze vysledovat různou míru agrese vůči zaměstnancům, v závislosti na tom, jakou agendu zpracovávají. Nezanedbatelným faktorem je také místo výkonu práce, kdy regiony s dlouhodobě vysokým podílem sociálně vyloučených lokalit a s vysokou mírou nezaměstnanosti vykazují značně vyšší počty incidentů.

Násilí mezi zaměstnanci navzájem

Ze záznamů Úřadu vyplývá, že incidenty mezi zaměstnanci navzájem jsou spíše raritní. Jinými slovy řečeno, drtivá většina incidentů se odehrála mezi osobami „zvenčí" (ať už se jedná přímo o klienty Úřadu či jejich doprovod) a zaměstnanci Úřadu. Ve sledovaném období (2017 až 9. červen 2023) bylo zaznamenáno pouze 9 incidentů mezi zaměstnanci navzájem.

Analýzou jednotlivých záznamů bylo navíc zjištěno, že v jednom případě byla agresivita způsobena duševním onemocněním zaměstnankyně, v ostatních případech pak byla podnětem násilného jednání vzájemná animozita zaměstnanců, respektive neochota uznávat nadřízené postavení vedoucích zaměstnanců.

Z provedené analýzy lze vyvodit několik obecnějších závěrů:

- Celkový počet incidentů vůči zaměstnancům Úřadu práce České republiky „zvenčí" byl řadu let v zásadě setrvalý (s mírným snížením v letech 2018 a 2020). Rok 2022 a ještě více 2023 je však ve znamení nárůstu počtu incidentů – kdy jen za prvních 160 dní roku 2023 bylo zaznamenáno bezmála tolik incidentů, jako v průběhu celého roku 2020.
- Počet žadatelů o různé druhy sociálních dávek a zprostředkování podpory v oblasti zaměstnanosti postupem času výrazně narůstá, a tudíž lze důvodně očekávat i zvýšený počet incidentů. Tomu odpovídá též výše zmíněný trend postupného nárůstu incidentů v posledních dvou letech.
- Počet incidentů se výrazně liší dle krajů, což je dáno sociální strukturou žadatelů a počtem žadatelů ze sociálně vyloučeného prostředí, kteří jsou často v prosazování svých požadavků agresivnější.
- Ani jednotlivé kraje nelze vnímat jako celek. V rámci jednotlivých krajů existují specifická území, která vykazují ve srovnání s ostatními výrazně vyšší míru agresivity klientů.
- Téměř 100 % incidentů se odehrálo na pracovištích, i když některé výhrůžky směřovaly i mimo pracoviště (ve smyslu výhrůžek typu „vím, kde bydlíš, ... po práci si na Tebe počkám" apod.).
- Dva zaznamenané incidenty se odehrály v místě bydliště klienta, kde probíhalo sociální šetření.
- Nejvyšší míra násilného jednání ve vztahu k zaměstnancům Úřadu se odehrává ve formě vulgárních slovních útoků. Bezmála stejně velké procento představují výhrůžky.
- U obou dvou výše uvedených slovních projevů (vulgarity, výhrůžky) nelze zaručit, že nepřerostou do fyzického napadení.
- Agresivita formou fyzického napadení je zatím relativně nízká – nepřesahuje 10 %. Od roku 2020 však bohužel tento podíl postupně roste.
- V roce 2021 došlo k usmrcení zaměstnankyně Úřadu; tato skutečnost bývá následně nezřídka zmiňována v rámci incidentů ze strany agresorů při vyhrožování a zastrašování: „když to šlo v Praze, půjde to i tady".

- Postupně roste i poškozování majetku Úřadu.
- Jako závažné narušení integrity úřední osobnosti je nutno vnímat také sexuální obtěžování.
- Agresivní jednání žadatelů a klientů je orientováno často agendově – koncentruje se zejména do agend, které rozhodují o dávkách osob, zejména ze sociálně vyloučených skupin, nebo nutí žadatele do pracovní aktivity (hmotná nouze, zprostředkování zaměstnání a podpora v nezaměstnanosti, státní sociální podpora). Dávky státní sociální podpory jsou však provázané. Pokud jsou konkrétní osoby vyloučeny z evidence uchazečů o zaměstnání, mohou přijít o status osoby v hmotné nouzi.
- U příspěvku na péči a u dávek pro osoby se zdravotním postižením je četnost agresivních jevů nejnižší, což je částečně dáno i specifičností této klientely. I zde však mohou incidenty nastat, spíše však ze strany pečujících nebo doprovázejících osob.
- V souvislosti s tématem a v návaznosti na personální posílení oblasti bezpečnosti se v průběhu ledna 2023 vytvořil v rámci Generálního ředitelství Úřadu práce České republiky interní tým, který se začal jednotlivými incidenty zabývat intenzivněji.
- Zaměstnancům Úřadu je naprosto nezbytné poskytovat vedle psychologické podpory a zlepšení bezpečnostních prvků také pomoc v oblasti právní.
- Úroveň ochrany úředníků proti výhrůžkám z hlediska trestního práva je diskutabilní. Výhrůžky jsou často velmi vyhrocené, zároveň však většinou ještě nenaplňují skutkovou podstatu trestného činu, která je v tomto smyslu stanovena vůči provinilcům poměrně mírně. Fakticky se tak snižuje vnímání společenské nebezpečnosti některých verbálních projevů vůči úředníkům. Podcenění (resp. nedostatečné postihování) závažných výhrůžek přitom může v konkrétních případech vést k eskalaci konfliktů, končících v nejzávažnějších případech fyzickým násilím.
- V rámci zajištění ochrany a bezpečnosti zaměstnanců Úřadu je nezbytné eliminovat či zredukovat možná rizika, a to ve smyslu vybavenosti kontaktních pracovišť. V této souvislosti bude pracovní skupina pro bezpečnost Generálního ředitelství Úřadu práce České republiky do budoucna činit postupné kroky, a to například zajišťováním kvalitní ostrah /ochranky v objektech Úřadu, modernizací přepážkových systémů nebo užší spoluprací s Policií České republiky.

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČESKÉ REPUBLIKY

Syntéza monitoringu tisku k tématu útoku z roku 2021

Soud poslal na doživotí do vězení Jiřího Dvořáka (roku 2022 byl ve věku 67 let), který v červnu 2021 zastřelil zaměstnankyni na úřadu práce, polil kyselinou svou bývalou kolegyni a nastražil střelné zařízení na pronajímatelku svého bytu... Způsob provedení trestných činů vykazoval neobvyklou brutalitu, bezcitnost a pohrdání lidským životem.

Dvořák podle obžaloby zastřelil zaměstnankyni úřadu... v její kanceláři na pražských Vinohradech. Žena mu v roce 2016 nepřiznala podporu v nezaměstnanosti a následně ho vyřadila ze seznamu zájemců o zaměstnání... Do budovy se dostal lstí – vrátnému řekl, že je ženin známý a že ji přišel překvapit. Úřednici, která byla matkou dvou dětí, nedal žádnou šanci k obraně. Zasáhl ji do břicha a odešel. Těžce zraněná úřednice zemřela v nemocnici. Kriminalisté zjistili, že zadržený muž ženě předtím písemně vyhrožoval, a to už v roce 2016. V minulosti totiž neúspěšně žádal o podporu v nezaměstnanosti. Policie tehdy výhrůžku vyhodnotila jako přestupek proti občanskému soužití a oznámila věc správnímu orgánu úřadu městské části Praha 2. „Do současné doby, tedy téměř celých pět let, nemáme informaci o tom, že by se poškozená v této souvislosti opětovně obrátila na policii s tím, že by ji podezřelý znovu kontaktoval nebo jakkoliv atakoval," uvedla policie.

Muž dříve na internetu uvedl, že mu úřad práce dluží peníze. 'Úřednice na úřadu práce provokuje a snaží se vyvolat střet, kde já budu dohnán k nekorektnímu jednání a budu obviněn z ublížení na zdraví,' napsal koncem května 2021.

Střelnou zbraň držel muž nelegálně.

Součástí rozsudku je i Dvořákova povinnost uhradit pozůstalým po zavražděné ženě, dalším obětem a zdravotním pojišťovnám celkem přes čtyři miliony korun jako náhradu škody.

Při hlavním líčení nechal soudce Dvořáka za jeho nadávky, hlasité výkřiky a další projevy třikrát eskortovat z jednací síně.

Další pobyt obžalovaného na svobodě je podle znalců pro společnost nebezpečný.

Z výslechu vyplynulo, že Dvořák chtěl pokračovat v páchání zvlášť závažných zločinů, které by byly namířeny proti osobám, se kterými měl v posledních letech spory. Jednalo se jak o rodinné příslušníky, úředníky různých institucí, bývalé kolegy ze zaměstnání, zaměstnavatele, tak o pracovníky orgánů činných v trestním řízení.

V podstatě se dá říci, že měl spory s každým, s kým přišel do styku, a tento okruh osob byl veliký.

Podle znalců Dvořák netrpí duševní poruchou, avšak pro jeho patologickou osobnost je typické paranoidní vnímání. Je přesvědčen o vlastní výjimečnosti a o svém dobrém charakteru. Je velmi podezíravý. Své jednání považuje za oprávněné. Znalecké posudky označil za vykonstruované, nepravdivé a účelové.

Znalci se mužovou psychikou zabývali v roce 2016 se závěrem, že muž trpí poruchou osobnosti, ale není duševně nemocný a jeho agresivita je pouze verbální.

Ministerstvo práce a sociálních věcí chce zvýšit bezpečnost zaměstnanců... O větším zabezpečení pracovníků státu a veřejné sféry chtějí s ministerstvem vnitra jednat odboráři.

Útoky nespokojených lidí na úředníky nejsou výjimečné. V minulých letech napadl jeden z uchazečů o zaměstnání pracovnici kutnohorského úřadu práce. Způsobil jí zranění, která si vyžádala desetidenní pracovní neschopnost. Policie se zabývala také případem, kdy jeden z klientů ohrožoval na radnici v Neratovicích úřednici injekční stříkačkou a tvrdil, že ji nakazí žloutenkou. Napadení čelila i pracovnice správy sociálního zabezpečení v Rakovníku nebo pracovnice registru vozidel v budově říčanské radnice.

Zdroje:

- Policie obvinila střelce z Prahy z několika činů včetně vraždy, žádá vazbu. ČTK, 1. VII. 2021.
- Dvořáka, který střílel na úřadu práce, poslal soud na doživotí do vězení. ČTK, 5. IX. 2022.
- Státní zástupkyně žádá doživotí pro střelce z pražského úřadu práce. ČTK, 5. IX. 2022.
- Soudce vyloučil Dvořáka viněného z vraždy úřednice dvakrát ze soudní síně. ČTK, 5. IX. 2022.
- Střelec z úřadu práce chtěl pokračovat v páchání zločinů. ČTK, 30. VI. 2021.
- Střelba v Praze – Aktualita. Policie České republiky – Krajské ředitelství policie hlavního města Prahy, 30. VI. 2021. https://www.policie.cz/clanek/strelba-v-praze.aspx
- Muž v Praze zastřelil pracovnici úřadu práce, policie podezřelého zadržela. ČTK, 29. VI. 2021.z

Mgr. et Bc. Petr ŠLECHTA, Ph.D.
akademický pracovník,
Vysoká škola AMBIS
bezpečnostní ředitel, pověřenec pro ochranu osobních údajů; Úřad práce České republiky, Generální ředitelství;
e-mail: petr.slechta@uradprace.cz

Mgr. Eva MANOVÁ
advokátní koncipientka; Mazel a partneři, advokátní kancelář, s. r. o.;
e-mail: eva.manova@akmazel.cz

Mgr. et Mgr. Michal MAZEL
advokát a jednatel; Mazel a partneři, advokátní kancelář, s. r. o.;
e-mail: michal.mazel@akmazel.cz

doc. Mgr. Oldřich KRULÍK, Ph.D.
akademický a vědeckovýzkumný pracovník, Vysoká škola AMBIS; analytický pracovník odboru centrální analytiky Úřadu služby kriminální policie a vyšetřování Policie České republiky;
e-mail: ambis-krulik@email.cz

Středočeský kraj

ODBOR BEZPEČNOSTI A KRIZOVÉHO ŘÍZENÍ
ODDĚLENÍ PREVENCE KRIMINALITY

KONFERENCE „BEZPEČNÉ MĚSTO“

TERMÍN: 26. A 27. 10. 2023, MÍSTO: ŠKODA MUZEUM MLADÁ BOLESLAV

Bezpečnost a smart technologie ve 21 století...

Tyto dva pojmy mají jednoho společného jmenovatele, a tím je koncept "smart city". Nelze však v této souvislosti opomíjet významný sociální fenomén, a tou je bezpečnost, která je dynamická a v podstatě živým organismem, jež vyžaduje pružnou reakci za účelem jejího zachování.

Bezpečnost a smart řešení se stávají v této dekádě společnosti mnohem více relevantními pojmy. Jak přistoupit k vytvoření "smart city" a přitom plnohodnotně zohlednit a aplikovat systémový přístup bezpečnosti ve městech? Tento postoj, směr a mnoho dalšího bude možné načerpat na dvoudenní odborné konferenci „Bezpečné město“, která se uskuteční dne 26. a 27. 10. 2023 v Mladé Boleslavi.

Tři pilíře odborné eventu:

1. Bezpečnost ve městech;

2. inovativní řešení a smart technologie aplikované v tzv. „SMART city“;

3. sdílení dobré praxe v kontextu smart řešení, bezpečnosti, jejich kombinace.

Obsah:

- představení standardizace v kontextu prevence kriminality (technické normy EU a jejich působnost, dopady a aplikace v ČR);
- pokročilé technologii a jejich využití v tzv. SMART city;
- nekonvenční přístup k ochrany míst s vysokou koncentrací osoby, např. náměstí, nemocnice,
- dopravní uzly, kulturní objekt (označované jako tzv. měkké cíle, kterých je ve městech velký počet);
- plánovaní městské zástavby a urbanistického designu za účelem snižování kriminality ve
- městech a obcích = centrální ražení přístupu tzv. „security by design“;
- a mnoho dalšího spojené s bezpečností a snižování kriminality ve městech...

Kontaktní osoba
Mgr. Filip Gundza, MBA
vedoucí odd. prevence kriminality
Krajský úřad Středočeského kraje
Tel.: +420 257 280 490
Mobil: +420 607 050 664
e-mail: gundza@kr-s.cz

Více informací najdete na TOMTO ODKAZU

ŠKODA
ASOCIACE BEZPEČNÁ ŠKOLA
PREVENCE SE MUSÍ VYPLATIT
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY
Statutární město Mladá Boleslav
MBI MEZINÁRODNÍ BEZPEČNOSTNÍ INSTITUT
ČAS ČESKÁ AGENTURA PRO STANDARDIZACI
Středočeský kraj
VISK.CZ

DETEKCE ZVUKOVÝCH UDÁLOSTÍ

Jaké jsou novinky v oblasti ochrany měkkých cílů, majetku a kritické infrastruktury? Přinášíme rozhovor s Lukášem Svobodou, spoluzakladatelem JALUD Embedded.

Můžete nám krátce představit JALUD Embedded?

Jsme plzeňský startup zaměřený na vývoj inovativních zvukových detektorů, zařízení pro ochranu lidských životů i kritické infrastruktury. Náš produkt, Sound Event Detector (SED), dokáže identifikovat zvukové události jako výstřely, agresivní i panický křik, výbuchy a tříštění skla, vyhodnotit je jako nebezpečné, oznámit operátorovi a zkrátit tak reakční dobu z průměrných 7 minut na 5 vteřin. Kromě vlastního dedikovaného zařízení je možné integrovat SED i do kamery. Inteligentním očím (kamerám) přidáváme i inteligentní uši. Přidáváme tak operátorovi další smysl, pomáháme mu k efektivnějšímu vyhodnocování situace a snižujeme náklady na ostrahu.

Jak jste přišli na myšlenku vyvíjet právě tuto technologii a jaké byly Vaše začátky?

První impulz k vývoji zvukového detektoru přišel, když jsme spolupracovali s firmou Jablotron na vylepšení jejich senzoru tříštění skla. To nás přivedlo k myšlence vytvořit vlastní zvukový detektor. Naštěstí jsme narazili na vizionářský přístup pana Luďka Šantory, ředitele Správy informačních technologií města Plzně. Díky němu jsme mohli nainstalovat první detektory v Plzni a uskutečnit pilotní projekt. Brzy jsme si v praxi ověřili účinnost systému při detekci střelby na jedné z plzeňských ulic. V současné době je v ulicích Plzně 53 detektorů, dalších 10 je v areálu FN Plzeň. Detektory máme instalovány také v Dubí, České Lípě, Ostravě, ve FN v Olomouci a chystáme instalace v Brně, Písku, Třebíči a Chebu. V zahraničí je SED využíván v Amsterdamu, Sao Paulu nebo třeba ve Velké Británii.

Jaké jsou Vaše další plány do budoucna?

Chtěli bychom zvýšit povědomí o možnostech audio detekce na našich detektorech a ukázat dalším městům jejich výhody. V tom nám nyní pomáhá nejen vlastní HW platforma, ale i fakt, že SED lze snadno integrovat i přímo do kamery formou tzv. ACAP SW aplikace, navíc plánujeme integrace do kamer od dalších výrobců. Rádi bychom také rozšířili spolupráci s dalšími významnými partnery v oboru, abychom dále zdokonalovali a rozšiřovali náš produkt. Zároveň aktuálně rozbíháme několik zajímavých projektů, u kterých očekáváme velmi pozitivní výstup.

Můžete prozradit, o jaké projekty jde?

O jednom z nich jste již mohli slyšet ve večerních zprávách. Nově bude SED pomáhat v Krkonošském národním parku odhalovat nepovolený vjezd řidičů a upozorňovat na něj strážce parku. Dosud se nedařilo odhalit vjezd vůbec nebo ne dostatečně rychle, a tak docházelo k narušování vegetace. Motorové vozidlo jsme schopni detekovat na několik desítek či nižších stovek metrů daleko a to dává dostatečný prostor pro probuzení kamery, která pachatele zachytí. Aby detektor nepůsobil v přírodě rušivě, máme připraveno zařízení v zelené barvě.

Naší další novinkou je detekce zvuku spreje. K rozpoznávání zvuku dochází v rámci několika vteřin, proto je možné neoprávněné sprejování ve veřejných prostorách ihned identifikovat a přispět tak k ochraně majetku a snížení nákladů na odstranění škod. Dle informací Českých drah jsou průměrné náklady na čištění jednoho vlaku od graffiti přibližně 150 000 Kč a jen v prvních 6 měsících tohoto roku vynaložily dráhy na čištění už 10 milionů korun. Využití detekce sprejů ale nekončí u Českých drah, využitelná je i k ochraně památek, ve městech nebo v komerčním sektoru.

Máte nějaké zajímavé projekty i v zahraničí?

Rozhodně. Nově umíme detekovat i zvuk uhlové brusky. To bude využitelné v Belgii, kde se potýkají s velkým nárůstem krádeží kol. Ke krádežím dochází za bílého dne, často na rušné ulici, kdy pachatel přeřízne zámek a na kole odjede. Lidé okolo na událost vůbec nereagují a ignorují ji. Detekce uhlové brusky bude využitelná i na srbských hranicích, kde dochází k narušování pohraničního plotu. Na uhlídání dlouhých úseků hranic nejsou dostatečné personální kapacity, a tak díky technologii SED bude hlídání hranic efektivnější. Dále pracujeme na novém projektu, který bude sloužit v první řadě ve věznicích v zahraničí, ale podrobnosti o projektu sdělím někdy příště, protože aktuálně je ve fázi předpříprav.

Je něco, na co jste v JALUD Embedded obzvláště hrdí?

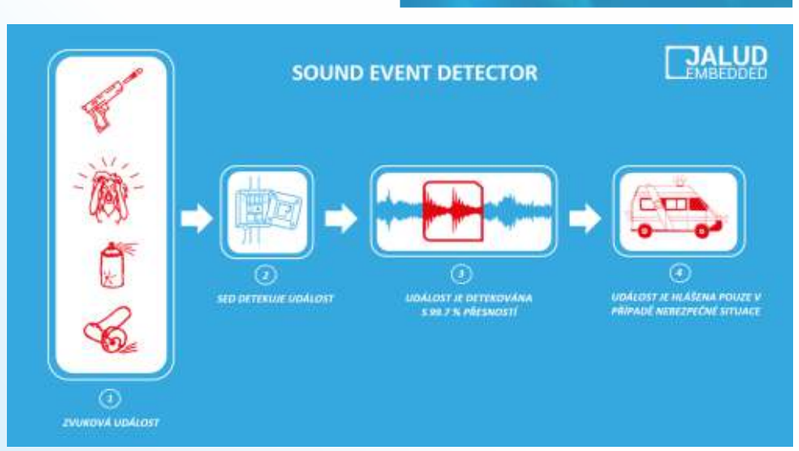
Za největší úspěch rozhodně považujeme první prokazatelně zachráněný život. V obci Dubí byli strážníci naším detektorem upozorněni na potyčku dvou mužů. Na místo byla vyslána hlídka, která tu okamžitě resuscitovala jednoho z mužů, který zkolaboval. Záchranáři strážníky informovali, že muže bylo možno zachránit jen díky jejich včasnému zásahu. Radost však máme z každého příkladu dobré praxe, kterých není málo.

Těší nás i úspěch v mezinárodní startupové soutěži We Make Future, kde jsme získali speciální cenu poroty o oblasti AI. Ceníme si i toho, že jsme postoupili na veletrh do Rimini, kde jsme byli jedním ze zástupců pro Českou republiku.

Dlouhodobě jsme velmi spokojení s širokou škálou využitelnosti i minimální chybovostí, díky níž je naše zařízení užitečným pomocníkem v každodenním provozu.

Děkujeme za rozhovor.

Redakce BsP



KONFERENCE

„EFEKTIVNÍ ŘEŠENÍ PRO BEZPEČNOST, DOPRAVU A PREVENCI KRIMINALITY VE MĚSTĚ“

Město Plzeň bylo pořadatelem odborné konference, která představila moderní trendy, inovativní řešení a dobrou praxi v oblasti bezpečnosti. Konferenci uspořádal ve spolupráci s městem Plzeň start-up JALUD Embedded, který stojí za chytrými zvukovými detektory střelby, křiku nebo tříštění skla.

Akce, která se konala v technologickém parku TechTower dne 23. května 2023, přilákala stovku odborníků z celé republiky. Zúčastnili se jí především velitelé městských a obecních policií, zástupci měst a samospráv, pracovníci odborů prevence kriminality, státní policie a hasičského záchranného sboru.

Cílem konference bylo představit moderní technologická řešení v oblasti bezpečnosti a inspirovat účastníky k další práci na vytváření bezpečnějšího prostředí ve městech. Přednášející se zaměřili na různá témata, jako je využití audio a videoanalýzy, rozvoj detektorů zvukových událostí nebo nositelného svícení jako doplňku výstroje IZS, bezpečnost škol v kontextu městských kamerových systémů nebo spolupráce s Drony SIT. Nechyběla ani prohlídka Smart City Polygonu, kde byly předvedeny praktické ukázky chytrých technologií.

Účastníci měli také možnost seznámit se s dotačními programy na inovativní řešení v prevenci kriminality, které představilo Ministerstvo vnitra ČR.

Organizaci konference podpořila Správa informačních technologií (SIT) města Plzně, která se věnuje vytváření příznivého prostředí pro technologické start-upy. Město Plzeň poskytuje těmto firmám odbornou pomoc, mentoring a prostředí pro testování jejich chytrých řešení. Luděk Šantora, ředitel SIT města Plzně, zdůraznil, že město si zakládá na inovacích a rozvoji nových generací IT prostřednictvím Plzeňského inovačního ekosystému.

Plzeňský start-up JALUD Embedded vysvětlil důležitost rozšíření kamerového systému o audioanalýzu a představil své detektory zvukových událostí, které dokážou identifikovat nejen střelbu, křik a tříštění skla. Tyto detektory již prokazatelně přispěly k záchraně lidského života, jak informoval velitel Městské policie Dubí Tomáš Pykal. Spolupráce mezi městem Plzeň a start-upem JALUD Embedded ukázala účinnost a důležitost moderních technologií v bezpečnostních opatřeních a prevenci kriminality.

Závěr konference byl věnován návštěvě Smart City Polygonu společnosti OMEXON GA Energo, kde byly představeny chytré technologie v praxi. V tomto komplexu se nacházejí systémy zvyšující bezpečnost obyvatel, zlepšující ochranu majetku, koordinující průjezd lokalitou a zajišťující bezpečnost chodců.

Konference „Efektivní řešení pro bezpečnost, dopravu a prevenci kriminality ve městě“ byla pořádána pod záštitou primátora města Plzně Romana Zarzyckého, hejtmana Plzeňského kraje Rudolfa Špotáka a Odboru prevence kriminality Ministerstva vnitra ČR.

Celá událost potvrzuje, že město Plzeň se v dané oblasti řadí mezi přední inovátory a aktivně se angažuje v implementaci moderních technologií pro zajištění bezpečnosti občanů. Spolupráce mezi veřejností, start-upy a institucemi přináší nejen konkrétní výsledky, ale také inspiraci pro další rozvoj oblasti bezpečnosti ve městech.

Zdroj: plzen.eu, tisková zpráva z 25.6.2023

ZABEZPEČOVACÍ SYSTÉMY HIKVISION

Majitelé domů a firem si pořizují zabezpečovací systémy kvůli potřebě jistoty, že jejich majetek a živobytí jsou vždy v bezpečí, a to především v době dovolených nebo pobytu mimo svůj objekt.

Tradiční zabezpečovací systémy mohou majitele domů, firem a dalších objektů upozornit, že se v jejich prostoru vyskytlo potencionální riziko nezvaného narušitele, ale nedokážou identifikovat, co přesně se děje. Poskytnutí tohoto druhu ujištění je však technicky náročnější a vyžaduje vícerozměrné zabezpečení se vzdáleným ověřováním.

K překonání tohoto nedostatku vytvořila společnost Hikvision zabezpečovací systém AX PRO. Ten zahrnuje všechna zařízení a funkce potřebné pro celkové bezpečnostní pokrytí, včetně možnosti ověřovat incidenty narušení na dálku pomocí snímků nebo videozáznamů v reálném čase.

Hlavními výhodami, které zabezpečovací systém AX PRO nabízí jsou:

1) Viditelný poplach

Zatímco tradiční bezpečnostní poplašné zařízení může upozornit, že nastal problém (například možné vloupání), podrobnosti jsou někdy nejasné a často vedou k falešným poplachům. Zabezpečovací systém AX PRO to řeší pomocí „viditelných alarmů", což znamená, že majitelé domů nebo firem mohou vzdáleně sledovat videa nebo GIF obrázky svého objektu prostřednictvím aplikace Hik-Partner Pro na svém mobilním zařízení. Detektor AX PRO PIR-CAM navíc odešle až 20 snímků v případě vloupání, čímž poskytuje okamžitý pohled na incident a podporuje rychlé a efektivní reakce.

Pomocí platformy Hik-Partner Pro lze také posílat snímky a videozáznamy incidentů do pultů centrální ochrany (PCO) v reálném čase, což bezpečnostním týmům poskytuje přehled o situaci a pomáhá jim rychle a vhodně reagovat.

2) Vícerozměrné zabezpečení

Široká škála dostupných periferií AX PRO zajišťuje maximální bezpečnostní ochranu pro domácnosti a obchodní prostory. S vysoce spolehlivými magnetickými detektory, detektory rozbití skla a detektory záclon je každé vloupání okamžitě detekováno a nahlášeno. A co víc, detektory prostředí dávají majitelům domů a firem včasné varování před úniky vody, kouřem a prudkými skoky teplot, což jim dává čas reagovat dříve, než dojde k poškození.

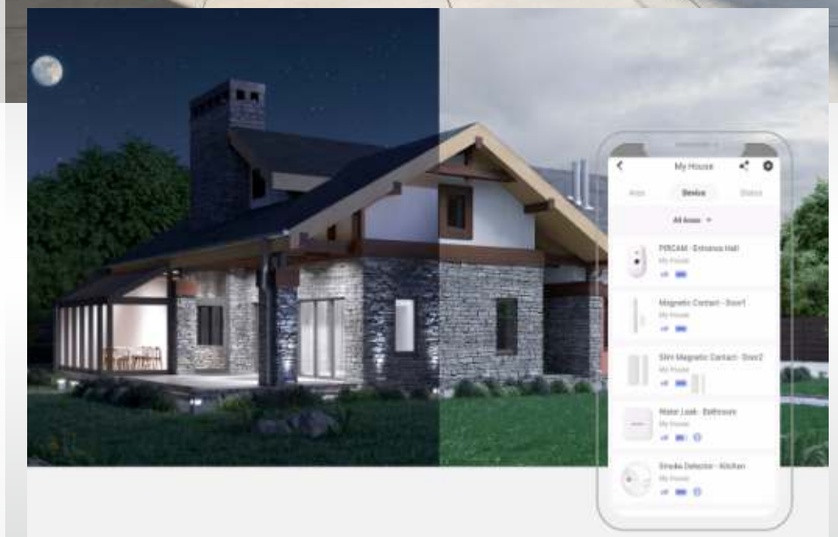
3) Méně falešných poplachů

Z běžné praxe víme, že často dochází k planým poplachům, které je téměř nemožné ověřit. Uživatelé se tak dostávají do stresu a řeší, zda na místo poslat pracovníky bezpečnostní agentury nebo se jet přesvědčit na vlastní pěst. My jsme tuto situaci vyřešili tak, že jsme do čidla zaintegrovali kamery a uživatel se tak sám vzdáleně může přesvědčit o pravosti poplachu. Do zabezpečovacího systému AX PRO je navíc možné připojit kamery s integrovanými algoritmy umělé inteligence Deep Learning, které dokážou rozlišit mezi domácími mazlíčky a jinými nevinně se pohybujícími předměty a mezi skutečnými bezpečnostními hrozbami, jako je vloupání osoby do nemovitosti.

To znamená, že majitelé domů a firem tráví méně času a energie vyšetřováním falešných poplachů. Další výhodou je schopnost soustředit čas a zdroje pouze na skutečné bezpečnostní hrozby a snížit náklady na práci s PCO na základě menšího počtu falešných bezpečnostních poplachů.

Společnost Hikvision však skutečnou a nepřekonatelnou výhodu přináší na trh s bezpečnostními technologiemi svým kombinovaným uceleným řešením pro veškeré bezpečnostní zařízení v domácnostech, podnicích a dalších objektech. Toto kombinované řešení zahrnuje široké produktové portfolio kamer, přístupových systémů, video interkomů, poplachových systémů atd. Oproti tradičním zabezpečovacím systémům, naše systémy nabízejí cloudovou správu, která zajišťuje ovládání všech našich systémů pomocí jediné platformy. Pro instalační společnosti to znamená, že nemusí jezdit k zákazníkovi kvůli každé ohlašené chybě, ale mohou to diagnostikovat vzdáleně. Pro běžného uživatele z toho naopak plyne že všechna svá zařízení vidí v jedné aplikaci.

Zabezpečovací systémy však už nyní nemají pouze bezpečnostní funkce, ale také jsou obohaceny o funkce, které z běžné domácnosti dělají chytrou domácnost, např. automatizované řízení vytápění při poklesu teploty, spínání zavlažování zahrady, ovládání přístupové brány atd.



DĚTI VS. DIGITÁLNÍ SVĚT

6 z 10 dětí si myslí, že by se jejich život nezlepšil, kdyby trávily na mobilu méně času.

Kde máte nyní svůj telefon? Leží v klidu na dně kapsy, nebo ho máte položený před sebou, aby vám nic neuniklo? A co děti? Nový výzkum Nadace O2 ukazu - je, že pětina českých dětí si svůj mobil zkontroluje alespoň jednou za hodinu. Při představě víkendu bez něj by děti ale nebyly naštvané – jen znuděné. Šest z deseti dětí si bere svůj telefon do postele, ukazují například výsledky nové - ho výzkumu.

Že jsou moderní technologie již běžnou součástí životů dětí i dospělých, není třeba připomínat. Vždyť první dotykový telefon se na trh dostal již téměř před třiceti lety a od té doby hraje čím dál důležitější roli. Zařízení jsou sofistikovanější a zároveň už běžně dostupná. Vždyť není výjimkou, že děti v předškolním věku používají telefon nebo tablet. A mnohdy obratněji než dospělí.

Jste si jistí, co, kdy a jak dlouho děti v online světě dělají? Nový výzkum od Nadace O2 totiž ukazuje, že rodiče mají trochu zkreslené představy. Myslí si, že děti tráví na mobilu průměrně o půl hodiny méně (2h 57min), než uvádějí ony samotné. U starších dětí je odhad rodičů ještě hor - ší – puberťáci ve věku 14 až 15 let tráví na mobilu dokonce o hodinu déle, než předpokládají dospělí.

„Průměrné české dítě tráví na telefonu necelé tři a půl hodiny denně, ve věku 14-15 let se tento čas dokonce navyšuje na necelých pět hodin,“ popisuje výsledky výzkumu manažerka Nadace O2 Dominika Herdová a dodává: „I pro dospělé, natož pro děti, je velmi snadné zapadnout v digitálním světě a ztratit přehled o čase, který tak potřebujeme pro skutečné zážitky a lidské interakce.“

Prostřednictvím telefonů se dětem otevírají dveře do širokého online světa, kde na ně můžou čekat inspirativní a vzdělávací aktivity, ale zároveň i řada potenciálních rizik. *„Rodiče si možné hrozby uvědomují, přes osmdesát procent z dotázaných dospělých svým dětem nastavuje, nebo v minulosti stanovovalo limit na mobilech. S rostoucím věkem ale kontrola klesá,“* vysvětluje Dominika Herdová.

Jen každé páté dítě ve věku 14-15 let má stále od rodičů stanovený denní limit, kolik času můžou strávit na telefonu. Přitom právě tato věková skupina je z hlediska online hrozeb velmi riziková. *„Právě dospívající jsou často terčem kyberšikany, sextingu, stalkingu, predátorů ale třeba i phishingových útoků,“* dodává Dominika Herdová. Kromě těchto potencionálních hrozeb s sebou nese přílišné trávení volného času na internetu i riziko závislosti na technologiích. Je proto na nás, abychom pomohli dětem porozumět rovnováze mezi digitálním a reálným světem.

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČESKÉ REPUBLIKY

OBECNÉ PŘÍZNAKY ZÁVISLOSTI

- Předmětu závislosti se věnuje nadměrné množství času
- Abstinenční příznaky, nervozita, vztek, agresivita při vysazení „digitální drogy”
- Změna nálad, zanedbávání hygieny, zhoršení prospěchu
- Nezájem o známé a kamarády, dřívější koníčky a činnosti
- Snaha dostat se k předmětu závislosti (mobil, hra apod.) za každou cenu
- Zapírání a skrývání toho, že se předmětu ZÁVISLOSTI VĚNUJE
- Změny biorytmů, zdravotní potíže, poruchy spánku

Balanc v době onlinové: bez telefonu je nuda

Zajímavý rozdíl mezi generacemi vyplouvá na povrh, když se Nadace O2 prostřednictvím výzkumu zeptala, jestli by se dětem zlepšil život, pokud by trávily méně času na mobilu. *„Třičtvrtě dotázaných rodičů si myslí, že by se život jejich dětí zlepšil. S tím děti přirozeně nesouhlasí – přeci jen současná mladá generace už vyrostla v digitální době a ‚oldschoolové‘ trávení volného času prakticky neznají. Kromě organizovaných kroužků si děti nejdou samy od sebe skákat přes švihadlo nebo zahrát vybíjenou,“* myslí si Dominika Herdová. Přibližně 6 z 10 dětí si myslí, že by se jejich život nezlepšil, kdyby trávily na mobilu méně času.

A co by děti cítily, kdyby se na víkend odpojily od online světa a strávily dva dny bez mobilu? Odpověď je jednoduchá – nudu. *„Znepokojuje mě představa, že by se děti bez digitálního zařízení nudily. A to i jen na pár dnů. Pro mě z výzkumu vyplývá to, že mladá generace se sama nedokáže zabavit a potřebuje rychle se měnící podněty. To jen dokazuje, že digitální well-being by se v dnešní době neměl brát na lehkou váhu,“* doplňuje Dominika Herdová.

Děti navíc nechtějí odložit svůj telefon ani v noci. Přestože většina rodičů zakazuje svým potomkům mobily v době, kdy by měly spát, děti si je stejně berou. Dvě děti z deseti tento zákaz nerespektují, ukázal výzkum. Přitom právě kvalitní a nerušený spánek má vliv na vývoj i psychiku dítěte.

Je proto klíčové si udržovat balanc mezi online světem schovaným v telefonech a realitou. To vystihuje takzvaný well-being, který v sobě zahrnuje celkové pohodlí, zdraví a kvalitu života ve světě digitálních technologií. Ačkoli tyto technologie přinášejí nepřeberné možnosti a přínosy, nemůžeme opomenout jejich vliv na člověka. Zdravý vztah s virtuálním prostředím má velký dopad na dětské fyzické, emocionální a sociální zdraví.

Jak ale najít zdravou rovnováhu a udržet si digitální well-being? Připravili jsme několik užitečných tipů:

1. STANOVTE SI HRANICE

Stanovte dětem pravidla a časová okna, kdy se budou moct věnovat online aktivitám. Například jim můžete vyhradit hodinu ráno a hodinu odpoledne pro kontrolu sociálních sítí a surfování po internetu. K tomu mohou pomoci aplikace rodičovské kontroly, kde dospělí můžou nastavit časový rámec, kdy dítě může telefon používat. Lze tak zabránit třeba nočnímu ponocování u obrazovky.

2. BUĎTE VZOREM

Časová okna by však neměla platit jen pro děti. Jako rodiče a učitelé máte klíčovou roli při vytváření zdravých digitálních návyků. Buďte vzorem pro své děti a studenty. Pokud sami respektujete limity a ukazujete, jak se vyvarovat přehnaného používání internetu a sociálních sítí, bude to mít pozitivní vliv na jejich vlastní chování.

3. VYTVOŘTE TECHNOLOGICKÝ PROSTOR

Vyberte si místo ve vašem domově nebo učebně, kde budete používat technologie. To vám pomůže oddělit digitální svět od zbytku života a vytvořit jasnou hranici mezi online a offline činnostmi. Například zavedením rodinného pravidla technologické zóny v obývacím pokoji zabráníte používání telefonů při jídle v kuchyni.

Zároveň nezapomínejte, že i když dítě sedí například hned vedle vás, s telefonem v ruce se nachází zároveň i ve virtuálním prostředí – sledujte, jaké pocity a emoce dítě při používání mobilu má. Není smutné? Nemračí se? Je zamlklé? Protože i když na své dítě dohlížíte, může zrovna čelit kyberšikaně nebo phishinovému útoku.

4. DIGITÁLNÍ DETOX

Není od věci si jednou za čas udělat pauzu od technologií a digitální detox. Vypněte své telefony a počítače na určitou dobu a věnujte se plně svému okolí. Tímto způsobem si můžete odpočinout od informačního přetížení a znovu se připojit ke svému vnitřnímu klidu.

Je důležité si uvědomit, že digitální svět by měl sloužit jako nástroj, který nám usnadňuje život a rozšiřuje možnosti. Vzdělávejme proto sebe i děti o digitální gramotnosti. Prvním krokem je si uvědomit potenciální rizika a negativa online prostoru.

„Společně můžeme podporovat zdravý přístup k technologiím, aby se naše děti mohly stát silnými, sebevědomými a odolnými jedinci v digitální době. Klíčové je nebránit se pokrokům a vymoženostem dnešního světa. Ale snažit se jim porozumět a pomáhat dětem se v nich zorientovat, a především bezpečně používat. I to je misí Nadace O2, která pomáhá rodičům a pedagogům se zorientovat v rychle se měnící digitální éře a poskytovat jim odborné podklady, užitečné informace i souhrnné materiály,“ zakončuje manažerka Nadace O2 Dominika Herdová, která doporučuje portál O2 Chytrá škola a web Bezpečně v síti.cz.

PSYCHOLOGICKÉ PORTRÉTOVÁNÍ NEZNÁMÉHO PACHATELE TRESTNÉHO ČINU

Psychologické portrétování (profilování) neznámého pachatele je vyšetřovací metoda z oblasti forenzní (soudní) psychologie, která je u nás využívána sporadicky.

Používá se především u trestných činů, které jsou příliš složité pro použití běžných vyšetřovacích metod.

Vyšetřovatelé se snaží pomocí informací o lidském chování a prožívání vytvořit si obrázek o neznámém pachateli. Cíleně se jedná nejen o celkový obrázek, ale především o informace o pachatelově motivaci k trestnému činu. Portrétování je tedy pomocníkem pro identifikaci pachatele.

Vychází z toho, že jisté rysy osobnosti pachatele se promítnou nejen do jeho celkového chování, ale projeví se i ve velmi jemných nuancích při jeho zločinném jednání. Psychologické portrétování nevede vyšetřovatele přímo k pachateli, ale jeho pomocí se zúží okruh podezřelých. Na sestavování psychologických portrétů pracují v týmech jak policisté, tak forenzní psychologové a experti z jiných oborů.

Princip psychologického portrétování vychází z množství nashromážděných informací. Jedná se především o důkladné ohledání místa trestného činu, a to jak v užším, tak širším slova smyslu. V užším pojetí jde přímo o místo, kde se skutek stal, v širším pojetí se jedná o široký okruh dalších míst a o vzájemné souvislosti mezi nimi a místem činu. Vycházíme z toho, že v jednom prostoru pachatel zaútočil a do jiného oběť umístil.

Významná jsou rovněž fakta (jsou-li známa) o způsobu spáchání činu a o všech stopách zanechaných všemi účastníky. Jedná se o stopy daktyloskopické, mechanoskopické, trasologické, biologické, grafologické, věcné a další. Každý člověk má ve svých projevech jisté miniaturní stereotypy, aniž by si je aktuálně uvědomoval a analyzoval je, pachatele samozřejmě nevyjímaje, a tyto stereotypy se promítnou do jeho jednání. Takové zdánlivé drobnosti pak vyšetřovatelům přinášejí informace o osobnosti pachatele, o jeho pravé motivaci, a mají hluboký psychologický význam.

Díky důkladnému vyšetřování lze stanovit, které stopy vznikly spontánně a které jsou. inscenované neboli nahrané. Jde třeba o časové údaje, o vzájemné vazby mezi všemi účastníky trestného činu, o doprovodné předměty, použití síly apod. To všechno může posloužit k doplnění charakteristiky místa trestného činu.

Všechny tyto podklady pomáhají kriminalistům při jejich práci. Mohou pak lépe zhodnotit tři důležité fáze pachatelova jednání. A sice, jak se pachatel choval před činem, při činu a po činu. To vše směřuje k odhalení pravé pachatelovy motivace. Zjistíme-li mezi uvedenými fázemi diametrální rozdíly, dokresluje to obrázek o pachateli. V první fázi třeba usoudíme, že pachatel má rád zvířata, že některá vlastní a je na ně hodný. Při činu však projevil zřetelné prvky nadměrné agrese s projevy sadismu. Po činu se tedy lze domýšlet, že pachatel zvířata ani jejich blízkost nesnáší.

Je třeba říci, že vytvoření prvotního portrétu pachatelovy osobnosti není statické. Neustále se rozšiřuje a doplňuje o nové poznatky získané vyšetřováním. Ve chvíli, kdy máme k dispozici veškeré údaje, všechny protokoly o vyšetřovacích úkonech, lékařské a biologické rozbory, fotodokumentaci, záznamy rozhovorů, lze přistoupit k tzv. behaviorální analýze, tedy analýze chování pachatele.

Vyšetřovatelé rovněž provádějí tzv. srovnávací analýzu, kdy čin srovnávají s činy z minulosti, jež mají podobné prvky jako aktuálně vyšetřovaný trestný čin. Patří sem zvláštnosti, jako např. odstranění částí lidského těla (genitálie, nos, ústa, zuby, konečky prstů, srdce apod.), což je i pro otrlé vyšetřovatele nepochopitelné. Ale pro pachatele mají všechny tyto prvky zřejmý rituální či symbolický význam.

Někdy nechá pachatel oběť na místě, kde čin spáchal, jindy svou oběť přemístí jinam, do jiného prostředí, a upraví ji do zvláštní polohy (ucpaná ústa, svázané končetiny, sundané oblečení, nápisy na těle oběti, prvky kanibalismu, šperky, svíčky, amulety apod.). V tomto případě hovoříme o tzv. oběti vystavené. Např. agrese sadistického pachatele se projevuje spíše než použitým násilím a zuřivým útokem chováním se znaky promyšlenosti, pachatel se soustředí spíše na mučení než na samotný útok.

Tím vším chce pachatel něco sdělit, ale co, to ví jen on sám. Kriminalisté po tom musejí pátrat, musejí jeho počínání zkoumat a vyvozovat z něj závěry.

Psychologické portrétování se užívá pouze u vybraných činů, hlavně však násilných, které mají pachatelův neobvyklý rukopis. Jde třeba o vraždy z vilnosti, o pomstychtivost či posmrtné útoky na oběť. Jedná se o skutky, které vykazují jisté psychické anomálie pachatele. Rovněž sem můžeme zařadit bombové útoky, žhářství či zdánlivě nemotivované činy.

Odborná literatura říká, že nemotivované trestné činy neexistují, pro vyšetřovatele existuje pouze momentálně neznámá motivace.

Psychologické portrétování se začalo šířeji používat asi v 70. letech minulého století v USA, kde v té době nápadně vzrostla řada sexuálně motivovaných činů, bombových útoků a vydírání. Z USA se tato metoda rozšířila do Kanady, Velké Británie, Německa a dalších zemí. V roce 1999 vznikla Mezinárodní akademie behaviorálního profilování (ABP), jejímiž členy je řada vyspělých států. Tato organizace má za úkol sdružovat odborníky ze všech oblastí využitelných při profilování.

Cílem výše uvedených řádků nebylo do detailu vyčerpat, co vše psychologické portrétování neznámého pachatele obsahuje. Spíše šlo o vytvoření reálnějšího a nezkresleného pohledu na tuto metodu, její tvorbu a využitelnost.

Mgr. Zoja Kalivodová, CSc.
psycholožka

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI
ČESKÉ REPUBLIKY

EVROPSKÝ DEN PROTI VLOUPÁNÍ 2023

Evropský den proti vloupání letos doprovází ve všech členských státech zapojených do Evropské sítě prevence kriminality (EUCPN) nový videospot. Cílem spotu je informovat občany, že mohou zabezpečit svůj majetek proti vloupání a že to nemusí být drahé. Použití certifikovaných zámků na dveřích, vnějšího osvětlení pomocí pohybových senzorů, odolných okenních zámků a vnitřního spínače světla je nejúčinnější kombinací, která zabraňuje vloupání do domácností.

V rámci Evropského dne proti vloupání do obydlí (https://eucpn.org/focus-day), který letos připadá na středu 21. června 2023, je dobré si připomenout základní pravidla zabezpečení objektů, a to mj. z těchto důvodů:

- Podle dlouhodobých statistických výstupů se pachatelé dostávají do obydlí nejčastěji překonáním vstupních dveří, přes balkon nebo okny, která nechávají lidé v době své nepřítomnosti často nezabezpečená.
- K nezvané návštěvě mnohdy napomáhá právě ponechání otevřené okenní ventilace či mikro ventilace. Vloupání se do obydlí a jeho vykradení přes mikro ventilaci může pachateli trvat kolem jedné minuty.

Ministerstvo vnitra ČR, ve spolupráci s Policií ČR, nechalo za účelem kampaně rovněž zpracovat 4 nové na sebe navazující videospoty. První z nich se věnuje obecně kvalitnímu zabezpečení domácnosti. Druhý videospot doporučuje, jak vhodně ochránit domov před odjezdem na dovolenou. Na něj navazuje třetí spot s tématem, jak vzbudit dojem obydlené domácnosti, když nejste doma. Poslední z nich je zaměřený na skutečnost, kdy přece jen došlo k vloupání do domácnosti a jaká základní pravidla v takovém případě dodržovat. K výše uvedeným videospotům byl vytvořen i leták.

Výše uvedené materiály budou postupně zveřejňovány na Twitteru MV ČR (@v-nitro) a po jejich zveřejnění budou rovněž k dispozici na www.stopvloupani.cz a www.prevencekriminality.cz.

I letos je však možné využít osvědčené letáky z minulých let „Dovolená" a „Večeře".

Do Vámi tvořených textů k Evropskému dni proti vloupání lze použít i tyto dvě citace:

„Policisté se dnes a denně setkávají s následky vloupání do různých typů objektů a vnímáme, že pro oběti jsou mnohdy závažnější emocionální dopady těchto skutků, než majetková újma. Dlouhodobě se v rámci preventivních aktivit snažíme vštěpovat veřejnosti jednoduché zásady, jak případného pachatele od vloupání odradit. Základní postupy jsou totiž velmi jednoduché. Například zamknout dveře nebo zavřít ventilačku před odchodem z domova vůbec nic nestojí a může mnohému zabránit, apeluje na důležitost základního zabezpečení zamykáním plk. Mgr. Zuzana Pidrmanová, vedoucí odboru prevence Policejního prezidia ČR.

„Po klidnějších (z pohledu kriminality) covidových letech opět zažíváme nárůst kriminality, kdy největší podíl na celkové kriminalitě má již tradičně kriminalita majetková. Počet vloupání do bytů a rodinných domů se ve srovnání s rokem 2021 zvýšil o více než 10 %. Tato kampaň upozorňuje na skutečnost, že lidé mají k dispozici možnosti, jak své domovy a majetek zabezpečit, a že to nemusí být vůbec drahé. Vyzdvihujeme tak čtyři osvědčená a efektivní opatření a zároveň lidem doporučujeme, jak se chovat bezpečně, jaká zvláštní opatření učinit před odjezdem na dovolenou, ale také to, jak reagovat v případě, že se přece jen stanou obětí vloupání, říká JUDr. Michal Barbořík, ředitel odboru prevence kriminality MV.

Lze také využít aktuální statistické údaje k majetkové kriminalitě.

Obecné rady a doporučení

- Prevence proti vloupání se rozhodně vyplatí, je proto důležité o zabezpečení přemýšlet již při jeho výstavbě.
- Pokud to již není možné, doporučujeme s odborníky konzultovat vhodný systém bezpečnostních prvků pro Váš byt či dům.
- Kombinovat lze mechanické zabezpečení (bezpečnostní dveře, zámky, bezpečnostní folie apod.) s prvky elektronického zabezpečení s oznamováním například na mobilní telefon (alarmy, kamery, detektory atd.).
- Do mechanického zabezpečení spadají bezpečnostní zámky, na trhu je možné vybrat si ze čtyř tříd, vhodné pro vstupní dveře bytů jsou pak výrobky 3. bezpečnostní třídy. Před mechanickým poškozením chrání také bezpečnostní kování a v neposlední řadě jsou klíčové bezpečnostní dveře, které by ideálně měly být z 3. bezpečnostní třídy. Velkým pomocníkem jsou také zárubně proti roztažení.
- Při výběru firmy upřednostňujte společnosti, které se mohou prokázat patřičnými oprávněními, jsou např. členem nějaké odborné asociace či cechu, nabízí komplexní služby a v neposlední řadě se mohou prokázat dobrými referencemi. Solidní firmy Vám sestaví nabídku bezplatně.
- Pokud zvažujete nákup bezpečnostních prvků bez odborné pomoci, rozhodně vždy volte certifikované výrobky.
- Důležité je také udržování přehledného prostoru před domem či bytem. V případě domů je vhodné dobré osvětlení, upravená zeleň, prostor nezakrytý stromy apod.
- K bezpečnostním opatřením patří i ochrana cenností. Máte-li doma něco cenného, nemluvte o tom s cizími lidmi a cennosti uschovejte do trezoru. Nejdražší předměty si uložte do sejfu v bance.
- Praktické je také vytvořit soupis cenností, jejich fotografie a zapište si jejich sériová čísla. Pokud Vám někdo tyto věci odcizí, zvýší se pravděpodobnost jejich nalezení a identifikace.
- Základem prevence jsou také dobré vztahy se sousedy, všímání si pohybu cizích osob v domě nebo okolí. A do své domácnosti pusťte pouze známé nebo důvěryhodné osoby.

Při odchodech či odjezdech z domova mějte stále na paměti pár základních pravidel.

- 1/Neupozorňujte nikdy na svou nepřítomnost na sociálních sítích a nechlubte se ve svém okolí odjezdem z domova.
- 2/ Chraňte své cennosti a pocit osobního bezpečí. Nenechte si vloupáním pachatele narušit integritu Vašeho domova.
- 3/ Nastavte si kontrolu nad svým domovem se sousedy, kteří Vám na něj dohlédnou, pravidelně vybírají poštovní schránku a zalévají květiny.
- 4/ Zabezpečení a dohled velmi pomáhají. Ale nejdůležitější jsou opatření, která Vás nic nestojí - nezapomínejte uzamknout všechny vstupy, zavírejte okna, klíče nenechávejte volně dostupné. Nevěřili byste, kolik lidí takto zlodějům i v dnešní době stále ještě svou nedbalostí napomáhá.

Pokud po návratu domů zjistíte, že se k Vám někdo vloupal, nikdy nevstupujte sami dovnitř. Pachatel může být ještě na místě a Vy můžete znehodnotit případné stopy. Neprodleně proto volejte linku tísňového volání 158.

Více informací k zabezpečení objektů je pro všechny zájemce dostupné na webových stránkách www.stopvloupani.cz. Dále rovněž na webových stránkách projektu „Zabezpečte se" (www.-policie.cz/zabezpectese), kde budete moci hledat potřebné informace a rady v nejbližších dnech. K dispozici je rovněž nový Katalog doporučených výrobků k účinné ochraně osob a majetku v rezidenčních a komerčních objektech všech kategorií, vypracovaný Cechem mechanických zámkových systémů ČR ve spolupráci s OPK MV ČR a PČR, viz https://cmzs.cz/cs/katalog-vyrobku.

Podklady pro tvorbu článků, textů atd. za účelem zveřejnění k Evropskému dni proti vloupání 2023

zpracovalo OPK MV ve spolupráci s Policií ČR

Celoroční statistika nápadu TČ
– vloupání byty, RD v ČR

	Objekt	Počet skutků	Objasněnost
2019	byty	2 144	439 (20,5 %)
	RD	2 748	639 (23,3 %)
2020	byty	1 861	424 (22,8 %)
	RD	2 199	529 (24,1 %)
2021	byty	1 553	401 (25,8 %)
	RD	2 231	556 (24,9 %)
2022	byty	1 745	383 (21,9 %)
	RD	2 528	603 (23,8 %)

Statistika nápadu TČ
vloupání byty, RD v ČR
od 01. 01. - 30. 04.

	Objekt	Počet skutků
2019	byty	683
	RD	803
2020	byty	687
	RD	763
2021	byty	466
	RD	667
2022	byty	575
	RD	868
2023	byty	539
	RD	863