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

Hawking group, s.r.o.
Rybná 716/24
110 00 Praha 1
michal.bavsenkov@gmail.com

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

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

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

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

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

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

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

CyberGym Europe, a.s.
Pobočná 1395/1
141 00 Praha 4
www.cybergymeurope.com

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

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

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

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

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

RTH Security, s.r.o.
Jaurisova 4
140 00 Praha 4
www.okoprahy.wa.cz

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

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

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

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

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

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

Ing. Martin Neuschl
Šachetní 391
261 01 Příbram

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI
ČESKÉ REPUBLIKY

ČASOPIS KOMORY PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČR
DUBEN - ČERVEN/2022

BEZPEČNOST
S PROFESIONÁLY

RIZIKA ONLINE RADIKALIZACE DĚTÍ A DOSPÍVAJÍCÍCH

SIMULOVANÝ ÚTOK NA VLASTNÍ KŮŽI

BEZPEČNOSTNÍ VZDĚLÁVÁNÍ

ZÁJEM VEŘEJNÉHO I SOUKROMÉHO SEKTORU

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

Na zadních stranách obálky
členové KPKB ČR

OBSAH

ÚVODNÍ SLOVO

Vážené kolegyně a kolegové,

jak jistě dobře víte, je v tomto období aktuální otázka přípravy zákona, který má upravovat naše podnikání. Zpracovatel, tedy Ministerstvo vnitra ČR (MV), ho nazývá „zákonem o bezpečnostní činnosti podnikajících osob a o změně souvisejících zákonů“. Tento dokument má v budoucnu určovat způsob a podmínky našeho podnikání. Není tajemstvím, že dosavadní snahy zpracovatelů skončily vždy neúspěchem, neboť navrhovaná podoba zákona neodpovídala potřebám a skutečnosti a na základě kritiky zástupců z řad odborné veřejnosti, kde jsme zastoupeni i my, KPKB ČR, či Národní sdružení bezpečnostních společenstev (NSBS), jehož jsme zakládajícím subjektem, nebyl zákon v předchozím volebním období doporučen poslanci Výboru pro bezpečnost Parlamentu ČR k dalšímu projednávání.

Současná snaha zpracovatele o jeho co nejrychlejší prosazení vedla MV k vytvoření tzv. pracovní skupiny 1. náměstka ministra vnitra pro přípravu návrhu zákona upravujícího soukromou bezpečnostní činnost. V ní má vedle zástupců MV, PČR, některých rezortů státní správy a několika dalších profesních sdružení svého zástupce i KPKB ČR.

Doposud proběhly tři porady této skupiny, na nichž jsme měli možnost se k nově předkládanému materiálu vyjádřit. Nový návrh však v podstatě bohužel jen kopíruje návrhy předchozí a pozornost zaměřuje hlavně na zpřehlednění počtu podnikajících subjektů. Na připomínky – a nejen ze strany KPKB – které směřovaly ke skutečnému zlepšování úrovně tohoto odvětví a ke vnímání komerčního bezpečnostního sektoru jako nedílné součásti bezpečnostní architektury České republiky, byla reakce MV i ostatních rezortů vesměs odmítavá, přičemž některé rezorty se v daném tématu evidentně vůbec neorientovaly. Pochopili jsme tedy, že z pozice členů této pracovní skupiny nemáme šanci s našimi náměty a připomínkami uspět, zřejmě proto, že by vyžadovaly pochopitelně hlubší diskusi v širším plénu, než je tato poradní skupina.

V tuto chvíli je materiál včetně dalších souvisejících dokumentů rozesílán Ministerstvem vnitra ČR do tzv. mezirezortního připomínkového řízení. Naše návrhy uplatňujeme společně s podněty NSBS cestou Hospodářské komory.

Co bude následovat, je v tuto chvíli velmi obtížné odhadnout. Nevíme, zda v jednotlivých rezortech vzniknou připomínky či neshody, které se budou muset následně řešit, nebo se zákon vrátí na MV bez problémů. Pak by měla jeho další cesta směřovat přes Legislativní radu vlády na vládu ČR a odtud do Poslanecké sněmovny na podvýbor pro obecní policie a soukromé bezpečnostní služby.

Možná jste v poslední době zaznamenali, že zpravodajem tohoto návrhu zákona bude pan poslanec Králíček, který se netají svými výhradami k dosavadní verzi i způsobu přípravy materiálu. Veřejně deklaroval, že je potřeba, aby tento zákon byl moderním a efektivním nástrojem, podle kterého budeme moci naše činnosti vykonávat efektivně. Zmínil i plán na uspořádání odborných „kulatých stolů“ na půdě parlamentu, jak tomu bylo v minulosti, za účasti všech relevantních subjektů. To nám skýtá naději, že nevypukne zbrklý a ničím nevynucený neefektivní proces, na jehož konci by byl zákon, který nepřinese to, co čekáme.

Aby toto úvodní slovo nevyznělo skepticky, musím konstatovat, že i přes všechny obtíže, které dnešní doba přináší, se nám podařilo 9. června 2022 uspořádat již 4. ročník odborné konference „Ochrana měkkých cílů 2022“. Podle dosavadních ohlasů byla vnímána jako organizačně velmi dobře zvládnutá a výborně připravená i po odborné stránce. Jsem tomu velmi rád a děkuji touto cestou celému organizačnímu týmu, partnerům a hlavně špičkovým přednášejícím. Více informací se dozvíte uvnitř čísla.

Na závěr Vám přeji klidnou a pohodovou druhou polovinu prázdnin, kdy ještě mnozí z Vás budete užívat zasloužený odpočinek na dovolených. Věřím, že načerpáte dostatek sil a elánu pro složité období, které máme před sebou.

S úctou

Ing. Václav Jahodář
prezident KPKB ČR

KONFERENCE

OCHRANA MĚKKÝCH CÍLŮ 2022

Tradiční konference na aktuální bezpečnostní témata s názvem „Ochrana měkkých cílů 2022“ proběhla 9. června 2022 v Kongresovém sále hotelu Olšanka v Praze. Jednalo se o největší pravidelně pořádanou konferenci s tímto zaměřením v České republice. Jejími pravidelnými pořadateli jsou Komora podniků komerční bezpečnosti ČR, z.s., Česká pobočka AFCEA a Fakulta biomedicínského inženýrství ČVUT.

Konference se zúčastnily téměř dvě stovky zástupců odborné veřejnosti, mezi nimiž byli např. bezpečnostní ředitelé z veřejné i státní správy, soukromých firem, nemocnic i vzdělávacích institucí.

Cílem konference bylo sjednocení pohledu státních a soukromých aktérů bezpečnostního systému České republiky na ochranu takzvaných měkkých cílů a zajištění jejich kybernetické, fyzické a personální odolnosti před potenciálními útoky.

Tato témata rezonovala v řadě vystoupení zaměřených nejen do oblasti kybernetické a personální bezpečnosti, ale i na uprchlickou krizi, vzdělávání bezpečnostní komunity, využití dronů a možností antidronové ochrany a další zajímavé oblasti.

Přednášejícími byli profesionálové a uznávaní odborníci jak z oblasti státních institucí a školství, tak ze soukromého sektoru. Nosným motivem konference bylo propojení veřejného a soukromého sektoru při zajišťování bezpečnosti měkkých cílů, což je téma, kterému se dlouhodobě aktivně věnujeme.

Konference ukázala, že ochrana měkkých cílů a další témata spojená s bezpečností České republiky nabývají velmi rychle na aktuálnosti.

Česká republika se ujala 1. července 2022 předsednictví v EU a na zajišťování bezpečnosti zúčastněných osob a probíhajících akcí budou muset spolupracovat nejen bezpečnostní složky státu, ale bude zapotřebí také zapojení soukromých bezpečnostních služeb a nasazení moderních technologií, například v souvislosti s eliminací rizik spojených se stále masivnějším používáním komerčních dronů. Je otázkou, nakolik jsme na to jako stát připraveni.

Česká republika se i za současné složité mezinárodní situace drží stále mezi deseti nejbezpečnějšími státy světa. Nicméně eskalace konfliktu na Ukrajině, neustálé zdražování základních potravin, astronomický nárůst cen energií a pohonných hmot se přímo odráží ve snižující se životní úrovni obyvatel a zvyšujícím se sociálním napětí, množí se odchody zkušených policistů z aktivní služby a narůstají další rizikové faktory… To vše může bezpečnost v naší zemi velmi rychle změnit a my bychom se mohli začít na žebříčku bezpečnosti států velmi rychle propadat.

Za organizátory akce bychom chtěli poděkovat všem, kteří se na přípravě a realizaci této konference podíleli – organizačnímu výboru, přednášejícím, moderátorce akce doc. PhDr. Barboře Vegrichtové, Ph.D., účastníkům a především partnerům – společnostem DATASENSE s.r.o., Trusted Network Solutions, PCS spol. s r.o., firmě Jíša s.r.o., České poště Security s.r.o., Mezinárodnímu bezpečnostnímu institutu, GATUM Advisory s.r.o., HIKVISION CZECH s.r.o., NAM systému a.s., ARBATAX s.r.o., TRIVIS, SYBENAM, MASADA security solutions a časopisu Bezpečnost s profesionály.

Věříme, že všichni zúčastnění byli spokojeni jak s prostředím, tak s odbornou úrovní konference, že se jim podařilo setkat se s kolegy z oboru bezpečnosti a navázat nové kontakty a také že jim získané informace dobře poslouží v jejich práci.

Těšíme se na příští společná setkání na dalších konferencích a odborných akcích.

Za organizátory:

Ing. Václav Jahodář
prezident KPKB ČR, z.s.

Ing. Tomáš Müller
prezident ČP AFCEA

doc. PhDr. Barbora Vegrichtová, Ph.D.
FBMI ČVUT

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI
ČESKÉ REPUBLIKY

AFCEA

FAKULTA BIOMEDICÍNSKÉHO INŽENÝRSTVÍ ČVUT V PRAZE

INTEGRACE JAKO PREVENCE RADIKALIZACE

Integrace, adaptace, integrační politika

To jsou pojmy, které v poslední době často zaznívají v souvislosti s tzv. ukrajinskou uprchlickou vlnou. I v minulosti bylo téma integrace v určitých obdobích často skloňováno, zejména ve spojení s masivní migrací do Evropy před několika lety. Přesto je v českém prostředí integrační politika spíše „popelkou" a tyto pojmy jsou užívány bezobsažně anebo nejsou naplňovány s dostatečnou naléhavostí, vytrvalostí a kontinuitou.

V rámci tohoto příspěvku bych Vás rád přesvědčil, že právě integrační politika je jednou z naprosto klíčových politik k udržení sociálního smíru, a tedy i bezpečnosti v naší společnosti. O to více v dnešním „globalizovaném světě", kde je čím dál tím zjevnější, že příliv nových obyvatel do Evropy, ale i České republiky – navzdory všem relativně funkčním represivním opatřením a bariérám na vnějších hranicích EU, které budujeme a přijímáme ve snaze mu zabránit – je nevyhnutelnou realitou. Tím větší důraz by měl být kladen ze strany vrcholných politiků, institucí a municipalit jako klíčových integračních aktérů na snahu naplnit konkrétní obsah integrační politiky a dát jí jasná východiska a maximální podporu včetně finančního zázemí.

Proces integrace a integrační politika je mimo jiné velmi významným preventivním nástrojem boje proti radikalizaci společnosti. Právě selhání integračního procesu a v jeho důsledku rostoucí pocity odcizení, sociálního vyloučení a rostoucí frustrace skupin či jednotlivců mohou mít fatální následky a stát se jednou z příčin rozkladu společnosti, rostoucí nedůvěry v ni, a nakonec také nárůstu radikalizace, extremismu, či dokonce aktů terorismu.

Pokud budeme vnímat integraci jako nástroj a jako politiku, pak je to v zásadě dlouhodobý proces, který je na první pohled neviditelný a svým způsobem i těžko uchopitelný. Úspěchy v oblasti integrace nezaplňují titulní stránky novin, na rozdíl od důsledků jejího selhání, které jsou často fatální, negativně ovlivňují celou společnost a mohou ji i náhle ochromit.

Viditelné důsledky selhání integrace nevznikají náhle, ale jde o důsledky jejího selhávání v čase, s kořeny často v dávné minulosti. Pokud jde o konkrétní příklady selhání, lze zmínit Německo a zdejší tureckou menšinu, Francii a zdejší původem africké přistěhovalce na sociálně vyloučených předměstích velkých měst, případně Švédsko a zdejší nepokoje mezi gangy imigrantů.

Správa uprchlických zařízení Ministerstva vnitra (SUZ MV)

Správa uprchlických zařízení Ministerstva vnitra je organizační složkou státu s 26 let trvající tradicí. Zjednodušeně lze SUZ MV definovat jako ze zákona klíčového a praktického realizátora velké části migrační, azylové a zejména integrační politiky státu.

Stěžejní úlohou SUZ MV je provoz zařízení a poskytování služeb různým kategoriím cizinců dle výše uvedených právních předpisů. V oblasti integrace provozuje SUZ MV čtrnáct poboček, Center na podporu integrace cizinců (CPIC), v deseti krajích České republiky. Dále je SUZ MV generálním poskytovatelem integračních služeb pro držitele mezinárodní ochrany v rámci Státního integračního programu.

Všechny tyto konkrétní příklady selhávání integrační politiky, které jsou často uváděny předními odborníky na tuto problematiku, mají jedno společné: většina důsledků má příčiny v selhání státu desítky let nazpátek, kdy sem začaly přicházet první generace přistěhovalců, a jsou důsledkem včasného nepodchycení některých budoucích problémů v době, kdy je ještě šlo úspěšně ovlivnit a vyřešit. V současné době tyto státy investují do nápravy obrovské množství nejen peněz, ale i sociálního a politického kapitálu.

Podobnou chybu by Česká republika neměla opakovat. Náš příběh je sice odlišný než v případě zmíněných zemí. Musíme si však uvědomit, že i naše země je součástí vyspělého bohatého světa, máme poměrně stabilní a velkorysý sociální systém, a i proto jsme už od počátku 90. let poměrně atraktivní cílovou destinací pro cizince nejen z kulturně blízké východní Evropy, ale dnes i cizinců z různých koutů světa.

Integrační politika a její cíle

V oblasti integrace lze hovořit o různých modelech, které byly popsány v teoretické rovině i aplikovány v praxi. Mezi základní z nich patří asimilace, kdy se přistěhovalci vzdávají svých původních tradic a zvyků a přizpůsobují se hodnotám a pravidlům hostitelské společnosti. Dnes se v pojetí české integrační politiky tento pojem nepoužívá, vzhledem k tomu, že je považován za politicky nekorektní. Nicméně dalo by se říci, že ve vnímání a praktické aplikaci je jedním z nejběžnějších a preferovaných. Dalším modelem je tzv. tavicí kotlík, kdy dochází k mísení tradic a zvyků, ze kterých vznikají nové. Třetí model lze označit jako kulturní pluralismus, jinými slovy multikulturalismus, který v minulosti pracoval s vyzdvihováním kulturní identity a byl spíše svým způsobem kritikou a reakcí na selhávání asimilace. Multikulturalismus je však dnes již spíše překonaným modelem, zejména v České republice. Hovoříme-li v českém prostředí o integraci, pak se v praxi nejčastěji jedná o asimilaci.

V případě zvolení modelu integrace-asimilace, lze v obecné rovině vytyčit hlavní cíle integrace:

- **Zajištění sociální koheze ve společnosti v důsledku přílivu nových obyvatel.** Dopady a přínosy migrace nejsou často posuzovány ekonomickými ukazateli, ale spíše sociálními důsledky. To vše souvisí s tím, jaké se podaří vytvořit vztahy mezi imigranty a hostitelskou zemí, jaká bude míra angažovanosti přistěhovalců ve společnosti a jak se podaří udržet vzájemný respekt.

- **Prevence negativních sociálních jevů a zabránění zhoršování bezpečnostní situace.** Nově příchozí s sebou mohou přinášet sociálně-patologické jevy i kriminální chování a struktury z domovské země. Cílem integračního procesu by proto mělo být takové zapojení imigrantů do společnosti, aby k šíření těchto jevů nedocházelo.

- **Vytváření vzájemné důvěry mezi různými společenskými skupinami.** Hlavním a klíčovým pojmem je v tomto smyslu důvěra, konkrétně důvěra mezi přijímající společností a diasporou a její budování.

Výsledky integrace by do jisté míry šlo měřit například dle statistik udělení počtu státních občanství cizincům, přestože ani toto neplatí bezezbytku. Na druhou stranu právě proces získání a udělení státního občanství v sobě zahrnuje všechna kritéria k úspěšné integraci, respektive asimilaci. Žije-li přistěhovalec na území státu dlouhodobě v souladu s jeho normami a hodnotami, naučil se na potřebné úrovni jeho jazyk a zná jeho kulturní a historické reálie – není pro stát a jeho obyvatele bezpečnostní hrozbou, ale stává se integrovaným členem společnosti.

Principy migrace a integrace

Pro správné nastavení integrační politiky je zásadní porozumět principům migrace a integrace, tedy tomu, co imigranty do hostitelské země přivádí a jaké faktory ovlivňují jejich začleňování do společnosti. Mezi nejdůležitější faktory a principy integrace patří:

Velikost diaspory

Čím větší je konkrétní diaspora v hostitelské zemi, tím více migrace zrychluje a roste počet migrantů. Zároveň může vysoký počet členů diaspory míru integrace do hostitelské společnosti zpomalovat, a to zejména pokud jde o diasporu, která je z nějakého důvodu vyloučená nebo uzavřená do sebe. Příkladem na území ČR může být svým způsobem vietnamská komunita.

Kulturní blízkost

Přestože je kulturní blízkost či vzdálenost obtížné měřit, velkou roli hraje blízkost jazyková, která má výrazný vliv na intenzitu interakcí mezi majoritou a diasporou. Kromě jazyka se jedná i o další aspekty, například náboženství. Pro ilustraci odlišné kulturní blízkosti lze srovnat integraci uprchlíků z Ukrajiny a z Afghánistánu v České republice, která bude probíhat přirozeně jinou rychlostí.

Sociální model v domovské zemi migrantů

Častým důvodem migrace bývá právě nefunkčnost sociálních modelů v domovské zemi. V zásadě platí, že migrace probíhá nejčastěji mezi nefunkčními, a naopak vysoce funkčními sociálními modely. Cílem je, aby nedocházelo k přenosu těchto nefunkčních sociálních modelů do přijímajících společností.

Kognitivní kompetence

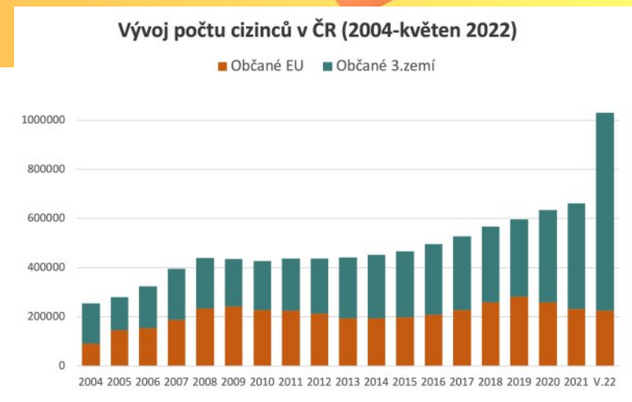
Jinými slovy schopnost získávat nové dovednosti a učit se. Extrémem absence kognitivních kompetencí je například negramotnost, kdy je důležité zamezit jejímu přenosu z rodičů na potomky. Právě v tomto duchu hraje významnou roli vzdělávání a vymáhání povinné školní docházky.

Ochota přistěhovalců se přizpůsobit hostitelské společnosti

To, jak příchozí migranti vnímají svoji ochotu se angažovat ve společnosti a zapojovat se do ní. Jaký obraz chtějí vytvořit a jaký důraz kladou na uchování svých vlastních kulturních vzorců. Zda respektují pravidla hostitelské země a nevytvářejí paralelní struktury. Extrémním příkladem je aplikace práva šaría či sňatkové dohody.

Přístup a politika hostitelských zemí

Je naprosto legitimní a legální, že si hostitelské země určují svou vlastní migrační a integrační politiku. Jedná se o bariéry, kterými mohou ovlivňovat právě dynamiku a velikost migrace a přílivu migrantů do země. To však neplatí v případech velkých uprchlických vln.



Schopnost ovládat jazyk hostitelské země

Čím více musí přistěhovalci používat jazyk a čím lépe ho ovládají, tím více se identifikují s majoritou.

Schopnost přinášet ekonomický užitek hostitelské společnosti

Z pragmatického pohledu je integrace investicí – jak ze strany migrantů samotných, tak hostitelské země. Čím lepší podmínky stát vytváří pro jejich integraci, tím více jim napomáhá při zapojení do aktivního ekonomického života, což přináší ekonomické benefity pro obě strany.

Migrační a integrační situace v ČR

Málo zdůrazňovaným faktem je, že v ČR dochází kontinuálně ke strmému nárůstu počtu cizinců. V důsledku aktuální uprchlické vlny z Ukrajiny jsme poměrně nedávno překročili hranici 1 milionu cizinců na našem území, což představuje téměř desetinu počtu obyvatel ČR.

Již před aktuální uprchlickou vlnou počet cizinců na území ČR výrazně narůstal. Na konci roku 2021 bylo v ČR registrováno 660 tisíc cizinců, což představovalo nárůst o více než 30 % v posledních pěti letech. Jednoznačně největším důvodem pro příchod takového množství cizinců byla pracovní migrace. Naopak počet žadatelů o azyl (mezi 1–2 tisíci ročně) se v tomto množství jeví jako zanedbatelný. Největší podíl na tomto čísle pak měli občané třetích zemí (mimo EU), zejména občané Ukrajiny.

Z naší práce s ukrajinskými komunitami – s přihlédnutím ke snaze většího množství Ukrajinců o vstup na náš trh práce anebo k počtu dětí již dnes přicházejících k zápisům do základních škol či školek v rámci povinné školní docházky – lze usuzovat, že se počet cizinců na našem území spíše dlouhodobě zvýší. Ve prospěch této predikce hovoří jednoznačně i jedno z dalších pravidel migrace, které zní: „Čím větší je diaspora na území přijímacího státu, tím větší je dynamika migrace a tím více se zrychluje." Možná právě proto, že na území ČR nebo Polska byla poměrně početná diaspora již v minulosti, se počet Ukrajinců zvyšoval. Obdobně to v případě ČR může platit i u jiných komunit cizinců, které již lze považovat za poměrně typické, ať už jde o Vietnamce anebo například v posledních letech Mongoly.

Velké množství cizinců s sebou může logicky přinášet i celou řadu výzev, včetně plíživých, anebo naopak zcela otevřených obav společnosti nebo její části. Již v minulosti se objevily četné průzkumy veřejného mínění, ze kterých jasně vyplývalo, že určitá část obyvatelstva má z důsledků migrace a přílivu cizinců obavy. Tyto obavy, sympatie či antipatie se logicky mění v čase a velmi závisí na politizaci a medializaci migrace. Největším rizikem je radikalizace společnosti v důsledku negativního vnímání přistěhovalců/cizinců, přičemž naprostým extrémem je pak iracionální spatřování viníků jakékoli krize v nich, což může ve svém důsledku vyústit v tzv. fenomén obětního beránka. Společnost může hledat viníka v určité skupině obyvatelstva či cizinců, aniž by to mělo faktický základ. Tady by mohlo jít o tzv. radikalizaci naruby, kdy se radikalizuje většina vůči menšině.

Na vyhodnocení důsledků uprchlické vlny z Ukrajiny je samozřejmě ještě brzy, jelikož je velmi složité fakticky zjistit, kdo z příchozích bude chtít na našem území setrvat a kdo se bude chtít vrátit. Ale už dnes je jasné, že do určité míry došlo ke zhojení některých důsledků migrační politiky ČR z minulosti a je také zjevné, že primárně do ČR mířilo větší množství osob, které buď měly předchozí migrační zkušenost z ČR, anebo zde měly příbuzenské vazby a fakticky došlo jen ke sloučení rodin.

Této situaci by mělo odpovídat masivní posílení jednotlivých nástrojů v oblasti naší integrační politiky a zejména zapojení většího množství integračních aktérů, jako jsou na prvním místě obce, neziskový sektor v oblastech mimo Prahu, ale v neposlední řadě zaměstnavatelé, kteří se často chovali v této oblasti velmi nezodpovědně až přezíravě, ačkoli mají zdaleka nejvíce nástrojů k integraci.

Právě zaměstnávání cizinců musí stát věnovat zvýšenou pozornost. Není možné nechat tak velkou skupinu napospas agenturám práce bez dostatečné kontroly. Některé z nich jsou totiž bohužel pouze zástěrkou pro vykořisťování a nelegální praktiky, jako je odebírání pasů, zaměstnávání bez smlouvy, nezákonně dlouhé (až 18 hodin trvající) směny, ubytovávání několika pracovníků na jednu postel, přeprodávání pracovníků, prostituce, vydírání atd. Přesun masivního počtu ukrajinských uprchlíků do šedé zóny pravděpodobně posílí i ukrajinskou mafii a další organizované kriminální struktury, což následně může vést k vytváření paralelních struktur a míst, kde budou bydlet společně bez kontaktu s českou společností, jako to vidíme v západních zemích.

Již dnes je zjevné, že takovýto masivní příliv uprchlíků/cizinců zahýbe některými strukturálními oblastmi české společnosti, jež jsou dlouhodobě přetížené – jako je bydlení, dostupnost zdravotní péče, škol a školek a další.

S ohledem na to, že poslední tři roky událostí překonávají fantazie zřejmě nás všech a čelíme nejrůznějším výzvám – v podobě pandemie, mezilidských vztahů, ekonomické krize, vysoké inflace, energetické chudoby – bychom měli o to větší pozornost věnovat právě problematice integrace cizinců. A to zejména proto, abychom nevytvářeli ještě větší napětí a byli jsme schopni udržet ve společnosti potřebnou důvěru a sociální smír a zabránit její ještě větší polarizaci. To by měl být jeden z hlavních úkolů, který před námi stojí. Jistě si všichni klademe otázku, jak to udělat.

Mgr. et Mgr. Pavel Bacík
ředitel
správa uprchlických zařízení
Ministerstva vnitra

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI

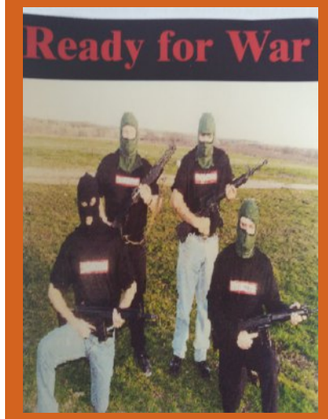
RIZIKA ONLINE RADIKALIZACE DĚTÍ A DOSPÍVAJÍCÍCH

Radikalizace dětí a dospívajících je téma řešené aktuálně na mezinárodní úrovni, protože představuje celosvětově závažný sociální a bezpečnostní problém. Tento článek je dílčím výstupem projektu Detekce radikalizace v kontextu ochrany obyvatelstva a měkkých cílů před násilnými incidenty (Vi20192022117).

Radikalizace je v podstatě procesem, během něhož jedinec – pod vlivem určitého světonázoru, ideologického proudu či jiného přesvědčení – začne akceptovat násilí, podporovat ho, ospravedlňovat či přímo se v něm realizovat. Radikalizační proces může v konečných důsledcích vyústit v akt extrémní agrese, masovou vraždu, či dokonce teroristický útok.

Dominantní platformou, kde radikalizace začíná či je umocňována, je v současné době kyberprostor. Různé online platformy a komunikační kanály slouží často extremistickým hnutím a teroristickým organizacím jako rekrutační základna, prostřednictvím níž se snaží náborovat nové přívržence. Pozornost těchto organizací je již dlouhodobě soustředěna na mladou generaci, přičemž věkový rozptyl se v posledních letech stále více rozšiřuje směrem ke spodní hranici dětského věku, a v některých případech neváhají tyto skupiny manipulovat i dětmi velmi malými.

Nebezpečí radikalizace dětí a mládeže spočívá v jejich značné vulnerabilitě (zranitelnosti), která vyplývá z neznalosti potencionálních rizik, a stejně tak v přílišné důvěřivosti či naivitě. Extremistické a teroristické organizace si často vybírají jedince, kteří se nacházejí ve složité životní situaci, jsou z neúplných nebo dysfunkčních rodin, trpí určitými duševními problémy, různými druhy frustrací, úzkostí, depresemi anebo jsou oběťmi školní šikany či jiné formy útisku.



Online prostor je prostředí anonymní, prostřednictvím něhož je možné šířit různé závadové a toxické ideje relativně snadným způsobem, s nízkými finančními náklady a v globálním měřítku. Taktiky a strategie extremistických skupin se umně přizpůsobují novým podmínkám, legislativě a v neposlední řadě i společenské situaci.

Flagrantní ukázkou je proběhnuvší pandemie Covid 19, která v dramatických kontextech změnila rytmus a kvalitu života prakticky celého světa. Většina sociálního, profesního a vzdělávacího spektra lidstva byla během pandemie přesunuta do virtuálního prostředí internetu. Na toto bezprecedentní dění extremistické a teroristické subjekty pružně zareagovaly změnou přístupu, rétoriky, a především metod rekrutace. V době pandemie došlo k poměrně masivní expanzi teroristické propagandy a protisystémových narativů.

Kromě dětí a mládeže představuje ohrožený segment společnosti i heterogenní spektrum široké populace. Finanční dopady pandemie, restriktivních opatření a omezení výkonu různých profesí uvrhlo značnou část obyvatel do ekonomické krize a existenční nejistoty. Všechny tyto atributy představují v souhrnu významný akcelerátor radikalizačních procesů.

Online diskusní fóra s extremistickým obsahem se tak stala a dozajista nadále budou ventilem frustrací, současně však i radikalizační platformou, která může vybrané senzitivní či psychicky labilní jedince přimět k akceptaci, či dokonce realizaci násilí. Proběhnuvší pandemie, její dopady a stejně tak probíhající válečný konflikt na Ukrajině jsou významnými sociálními faktory, které radikalizaci umocňují. Tyto události představují ve svém souhrnu živnou půdu pro vznik a šíření konspiračních teorií, které se rovněž staly mocnou zbraní v rukou teroristů a dalších hybridních formací.

Cílová skupina dětí a mládeže zůstává stále velmi ohroženou skupinou. Extrémní agrese a násilné incidenty páchané dospívajícími a mladými dospělými mají zásadní dopad na vnímání bezpečnosti ve státě. Tyto činy ve většině případů nastolují otázku, jak těmto útokům zabránit či ještě lépe – jak jim cíleně předcházet. Zvýšená míra osvěty o problematice radikalizace na internetu a o nástrojích a postupech, jak tyto případy včas detekovat, představuje jednu z účinných cest efektivní prevence.

Pachatelé masových vražd si často vybírají za cíle svých útoků objekty, které lze nazvat jako měkké cíle, tedy místa s nízkou či nulovou intenzitou bezpečnostních prvků, vyznačujících se vysokou kumulací osob. Režimová opatření, technické a elektronické bezpečnostní prvky jsou přirozeně jedním ze způsobů, jak tyto incidenty minimalizovat či eliminovat.

V kontextu radikalizačních procesů a přípravy násilného činu je ovšem třeba věnovat pozornost identifikaci varovných signálů radikalizace, a to včetně online prostoru. Zde bezpečnostní i preventivní praxe stále vykazuje, a to zejména v českém prostředí, absenci dostačeného povědomí o úskalích a rizicích tohoto fenoménu, a to především v rámci pedagogických a pomáhajících profesí.

Ve snaze zabránit expanzi násilí mezi dětmi a dospívajícími je nezbytné zacílit systematickou osvětu a vzdělávání právě i na sektor učitelů, vychovatelů, speciálních pedagogů, sociálních pracovníků, kurátorů, psychologů a dalších profesionálů, kteří s dětmi a mládeží dlouhodobě pracují. Je třeba též zvyšovat digitální gramotnost rodičů, a především vhodným způsobem poučit děti a mládež o rizicích spojených s radikalizací ze strany extremistů.

Jak již bylo naznačeno výše, náborování a snaha o extremizaci mladé generace probíhá v etapách, za použití moderních a atraktivních formátů, jako jsou videa, hudba, počítačové hry, humorné hry a koláže a široké palety memů, kterými je onlline prostor doslova zahlcen. Znovu se obnovuje téma symboliky spojené s extremismem, jako je užití alfanumerických kombinací, notorických sloganů, například We must secure existence of our people and a future for white children (Musím zajistit existenci naši lidí a budoucnost pro bílé děti), militarismus a potřeba rozpoutat rasovou svatou válku.

Tato témata rezonují zejména v rámci radikálního jádra pravicových extremistických hnutí. Džihádistické teroristické organizace se na mladou generaci zaměřují již dlouhodobě a potvrzují tak skutečnost, že právě děti a mládež jsou hybnou silou transformace světa, i za cenu užití násilí. Anarchoautonomní scéna zdůrazňuje nutnost zacílení svého působení na děti již od raného věku v rámci výchovy, např. ve formátu Anarchist Parenting (anarchistického rodičovství).

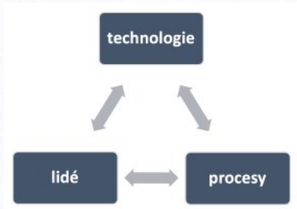
Samotná indoktrinace toxickými ideologiemi a legitimizace násilí bývá podsouvána zákeřnou manipulací prostřednictvím přikrášlování, lichocení, slibování, depersonalizace a dehumanizace různých skupin a jedinců, apelem na svědomí, hraním na city, či dokonce vydíráním a výhrůžkami. Jedná se o velmi propracovanou strategii, která se v průběhu času a společenského vývoje progresivně mění a adaptuje na nové podmínky.

Nejúčinnější prevencí je tedy včasné poučení dětí a mládeže o rizicích radikalizace v online prostoru, rozvoj kritického myšlení a schopnosti práce s informacemi. Cílovým adresátem těchto kampaní může a musí být pochopitelně i široká veřejnost. Vzdělávací aktivity tohoto druhu jsou proto vítaným a smysluplným postupem, jak předcházet radikalizaci nejen mladé generace, ale i celé společnosti. Detabuizace vybraných témat, inspirace k občanské solidaritě, otevřená debata, spolupráce s odbornou akademickou sférou a multioborový přístup se ukazují jako klíčové protředky v boji proti terorismu, aktům extrémní agrese a radikalizace v online prostoru.

doc. PhDr. Barbora Vegrichtová, Ph.D., MBA
Fakulta biomedicínského inženýrství
České vysoké učení technické v Praze

BEZPEČNOSTNÍ VZDĚLÁVÁNÍ

Je společným zájmem veřejného a soukromého sektoru? Těm, kteří nemají čas číst celý článek, odpovím na tuto otázku hned na začátku: ano, je.



Trojúhelník, nikoli bermudský

Každý bezpečnostní profesionál ví, že při navrhování, plánování, budování a provozu bezpečnostního systému má k dispozici pouze tři okruhy aktiv. Těmi jsou technologie, procesy a lidé. Většina z nás také ví, že všechny tyto skupiny zdrojů je třeba trvale udržovat, zlepšovat, zabezpečovat jejich růst a modernizaci. Klíčová je jejich schopnost odolávat novým typům hrozeb, novým scénářům útoků a lépe pečovat o chráněný zájem, ohrožovaný novými zranitelnostmi.

Technologie lze testovat, upgradovat, obměňovat nebo integrovat. Procesy je možné optimalizovat, algoritmizovat, automatizovat. Výkonnost lidského faktoru nelze obvykle zvýšit instalací aktualizace firmware nebo výměnou zastaralé periferie. Vzhledem k tomu, že všechny tři strany zmíněného trojúhelníku procesy-technologie-lidé jsou stejně důležité, respektive jejich selhání může mít stejně drtivý dopad, je třeba myslet nejen na kvalitu čidel a zámků, ale také na kvalitu personálu.

Pro některé bezpečnostní disciplíny existují konfekční kurzy. Typicky jde o oblasti BOZP, PO, bezpečnostní doprovody nebo výkon činnosti strážného. Výhoda těchto rolí je, že jsou strukturovaně popsané a relevantní hrozby se příliš dramaticky nemění. Existuje však široké spektrum bezpečnostních činností, které podléhají změnám rychleji než složení vlády. Pro takové případy je třeba vždy zvažovat, zda jsou naše vzdělávací programy stále ještě platné, efektivní a zda chrání správná aktiva proti aktuálním hrozbám.

Běžně se také setkáváme s tím, že i standardní (a tedy snadno vzdělatelné) role, jako je recepční nebo strážný, nemají pražádnou povědomost o hodnotách, které chrání – například jak důležité procesy běží na počítačích v serverovně, co by znamenalo přepnutí několika ovladačů na panelu, nebo jak nebezpečný by byl únik látek z nádrže ve skladu. Je zcela normální, že strážný detašovaného objektu si nikdy v životě nevyzkoušel použití hasicího přístroje a respondeři, kteří mají ke své obraně používat slzotvorný prostředek nebo teleskopický obušek, ho nejen neumějí použít bezpečně, ale mají ho zabalený v krabičce a pohozený v zásuvce, protože stejně nevědí, co s ním. Existují bezpečnostní manažeři, kteří neznají zrádná zákoutí krizových procesů, protože je „zdědili po předchůdcích".

Pokud tedy máme k dispozici technologie a procesy, ale tak trochu nám to kazí lidé, případnou krizi pravděpodobně nevyřešíme na jedničku.

Nutnost kvalifikace bezpečnostních pracovníků

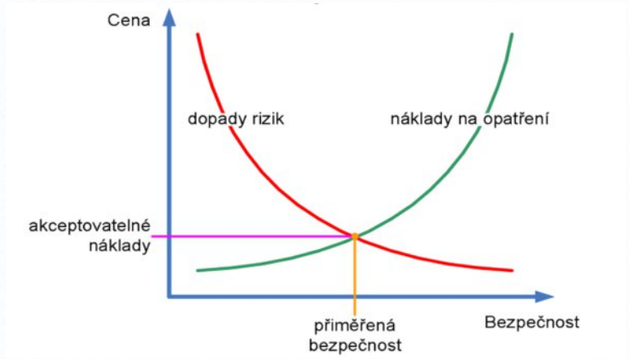
Bezpečnostně relevantní pracovníci chrání, tedy předcházejí škodám a reagují na bezpečnostní události při ochraně životů a zdraví (klientů, zaměstnanců, třetích osob, speciálních osob), ale také mobiliáře, infrastruktury, dalších provozních aktiv, dostupnosti služeb /schopnosti poskytovat služby, životního prostředí nebo reputace.

Proti čemu/komu jsou tyto zájmy chráněny? Není to složité. Nejčastěji zvažovanými hrozbami jsou teroristický útok, krádež, loupež, loupežné přepadení, vandalismus, běžná kriminalita, havárie s dopadem na provozní aktiva, havárie s dopadem na aktiva klientů, nedostupnost aktiv, panika, krize, emoce, provozní okolnosti (například nečekaný peak).

Vědí to bezpečnostní pracovníci? Zní to neuvěřitelně, ale často nikoli. Podstatu, hodnotu a možné způsoby ohrožení, stejně jako správný způsob ochrany, by měli všichni pracovníci znát a jejich znalosti by měly být pravidelně a včas přezkušovány, ověřovány a aktualizovány. Pokud tomu tak není, nelze očekávat, a dokonce ani spravedlivě požadovat nějaký extra super pracovní výkon, o motivaci ani nemluvě.

Akutní stres jako specifická okolnost

Problém s výkonem bezpečnostních činností zpravidla nastává, pokud se náhle změní provozní a bezpečnostní podmínky. Zde narážíme na základní problém vzdělávání – drtivá většina kurzů a školení je koncipována tak, že jejich absolventi jsou fajn v době klidu a míru. Nikoli pak při násilném útoku, při požáru, když zvoní telefony, ječí vysílačky a padá strop. To jsou však situace, kdy je jejich úloha v reaktivním procesu nejdůležitější. Kde je zakopán pes? Zpravidla v příliš komplikovaných procesech a nerespektování potřeby výcviku a vzdělání pro stavy krize. Skutečná krize přináší akutní stres. Ten se projeví, ať chceme nebo ne, kromě jiného také tunelovým viděním, inhibicí sluchu, bušením srdce, nárůstem krevního tlaku, svalovým napětím, strachem, napětím, úzkostí, agresí, ztrátou flexibility, přijímáním překotných rozhodnutí, nevhodným výběrem priorit, poruchami paměti, poruchami logického myšlení, poruchami koncentrace, nebo dokonce zmrazením. To není výčet vlastností a stavů, které bychom si přáli u bezpečnostního experta, jenž má bleskově zasáhnout – dostat lidi z budovy do bezpečí a poskytnout informace policii. Akutní stres zásadně snižuje schopnost bezpečnostního pracovníka vykonávat nejen složité, ale často zcela triviální činnosti, jako je nalezení a použití zásahových pomůcek, správně provedený hovor na tísňovou linku nebo vyhlášení nebezpečí a evakuace. Většina vzdělávacích programů tento problém fakticky ignoruje. Výkon bezpečnostních činností ve fázi prvotní reakce na incident je však tím, co zachraňuje životy, zdraví nebo majetek ještě před příjezdem složek IZS. Vrací nás to opět k trojúhelníku, který je naznačen výše, tedy lidé-technologie-procesy. Procesy musí být transformovatelné do obsahu vzdělávání. Musí podporovat triviální prioritizaci a algoritmizaci. Pod vlivem akutního stresu se může okamžitá mentální výkonnost průměrného zaměstnance propadnout v mnoha ohledech na úroveň dítěte.



Je kurzů a certifikací dost?

Kurzů je sice dost, ale stále ne dostatek. Existují solidní východiska pro jejich tvorbu. Některé role jsou velmi dobře popsány v systému profesních kvalifikací. Většinou však mohou posloužit pouze jako interní firemní vodítka, protože ověřování kvality a výkonnosti, případně provedené vzdělávací aktivity jakéhokoli typu narážejí velmi často na údaj: „K této profesní kvalifikaci nejsou přiřazeny žádné autorizované osoby." Některé bezpečnostní kvalifikace lze získat na velkých marketech se vzděláváním, jako je například Udemy. Ovšem tam, kde se nevyžaduje akreditovaná certifikace, jsou všechny vize o kvalitě jen naivním přáním.

Personalista, kterému přeloží uchazeč slibně znějící certifikát s titulem „bezpečnostní konzultant" (do roku 2021 navíc šlo o kvalifikaci s platným standardem), si snadno najde popis takového kurzu. V něm se dozví, že kurz provádí akreditovaná vzdělávací instituce a absolvent kurzu je předurčen k tomu, že provádí „... nezávislé posouzení úrovně zajištění bezpečnosti aktiv..., zpracování koncepcí a metodik v oblastech bezpečnosti, krizového řízení, ochrany kritické infrastruktury a navazujících prováděcích postupů..., posouzení úrovně zpracování bezpečnostní politiky společnosti a její realizace..., posouzení smluvních vztahů s dodavateli bezpečnostních služeb v uvedených oblastech..., zpracování dokumentace a návrh opatření v oblasti ochrany informací, vč. utajovaných informací, ochrany osobních údajů, fyzické ochrany, bezpečnosti informačních systémů, krizového řízení a kritické infrastruktury..., vyhotovení bezpečnostních auditů, bezpečnostních posouzení a studií, analýz hrozeb a rizik..." Personalista zahýká radostí a uchazeče přijme. V certifikátu se však nedočte, že celý kurz, včetně přivítání a rozloučení, trvá pouhých 20 hodin. Navíc student, pokud dostatečně rychle kliká, může na zmíněném Udemy kurz s podobným titulem absolvovat za neuvěřitelných 60-90 minut. Neméně děsivé je, že některé, dříve relevantní kvalifikace lze nyní získat také „nově" online. Ještě nedávno jsme kroutili hlavou nad titulem MBA v oboru „bezpečnost a ochrana obyvatelstva", který lze získat za jeden semestr a 39 tisíc Kč. Dnes na takový koncept můžeme hledět s nostalgií jako na Škodu Rapid 1.2, které jsme se také posmívali. Za méně než 15 tisíc Kč a méně než 10 osmihodinových „vyučovacích dní" dnes totiž můžeme MBA získat pohodlně pomocí patnáctiminutových videobloků. To rozhodně nejsou námitky proti online vzdělávání, existuje řada titulů, které fungují dobře a skýtají jisté záruky kvalifikace. Autor jich absolvoval řadu a nad některými blednul závistí.

Nedostatečnost akreditačního a certifikačního ekosystému tak v České republice vede k tomu, že se běžně vzájemně certifikují kamarádi, kteří potřebují vylepšit svůj profesní životopis. „Chceš certifikaci na teamleadera? Vydrž, stačí pdf?"

Principy vlastního bezpečnostního vzdělávání

Vzít to do vlastních rukou je jistě dobrá cesta, ale... Musíte najít někoho, kdo rozumí vzdělávání. Musíte najít někoho, kdo rozumí příslušnému obsahu vzdělávání. Musíte najít někoho, kdo rozumí projektovému řízení. Musíte najít někoho, kdo rozumí vzdělávacím platformám. A to všechno stojí čas a peníze. Zcela jistě se dostanete do bodu, kde se setkají zelená a červená křivka, které můžete vidět na obrázku. Je to prosté. Náklady na bezpečnostní vzdělávání musí být prostě úměrné výstupům z analýzy rizik. Nemáte to tak? Pak se vám nemůže podařit nastavit vzdělávací systém správně. Máte to tak? Pak jste schopni sestavit si smysluplnou strategii bezpečnostního vzdělávání, která vám umožní definovat cíle a metriky vzdělávacího systému. Východiskem vzdělávací strategie samozřejmě nemůže být jen onen primitivní zeleno-červený graf, ale především hluboké poznání kontextu.

Je to do jisté míry složité a komplexní. Ještě složitější je měřit výkonnost, úplnost a efektivitu takového vzdělávacího systému. Pokud to však myslíme s bezpečností vážně, nevyhneme se tomu. Sami nebo dodavatelsky, ale vážně a cílevědomě. Existuje řada dobrých standardů. Akreditace vzdělávacích institucí, akreditované certifikace lektorů, normy typu ISO9001, ISO17024 a mnoho dalších.

Společný zájem státu a soukromého sektoru

Zaměstnanci soukromých organizací jsou v první linii. Jsou těmi, kdo se primárně starají o prevenci a odstrašení, o detekci a prvotní reakci. Jsou těmi, kdo zachraňují životy, informují bezpečnostní autority státu, brání poškození důkazů, nebo je dokonce zajišťují. Jsou to většinově zaměstnanci soukromých organizací, kteří se starají o to, aby se děti pokaždé vrátily v pořádku ze školy, z kina nebo festivalu.

Je v zájmu státu, aby společně se soukromým sektorem dbal na kvalitu vzdělávacího systému v oblasti bezpečnosti, respektive se zasadil o skutečný vznik takového systému a řízení životního cyklu jeho prvků.

Oním společným zájmem by mělo být společné budování důvěry, standardů, metrik a sdílení smyslu práce s lidským faktorem bezpečnosti.

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.

ZAMĚSTNANCI JAKO SOUČÁST KYBERNETICKÉ OCHRANY ORGANIZACE

O počítačové kriminalitě slýcháme často, dokonce i našich médiích se stále častěji objevují články o podvodech, zašifrovaných discích, ukradených bitcoinech a podobných kybernetických zločinech. Velmi dlouho převládal názor, že jsme příliš malá země (organizace, jednotlivec), že se tato problematika týká jen velkých firem a zemí. Bohužel nic není tak vzdáleno pravdě, jako předchozí věta. Oprostíme se v dalším textu od specializovaných a vysoce sofistikovaných útoků vládami podporovaných kriminálních skupin, které útočí a získávají data označovaná jako velmi citlivá.

VÝNOSNÁ POČÍTAČOVÁ KRIMINALITA

Od roku 2018 je znatelný masivní nárůst malware a ransomware. Malware je termín, označující jakýkoli typ škodlivého kódu nebo softwaru, který může poškodit počítač nebo mobilní zařízení. Ransomware je typ malware, který zašifruje soubory nebo znemožní používat počítač, dokud není zaplaceno výkupné. Pokud je počítač připojený k síti, ransomware se může rozšířit i do dalších počítačů a úložišť v síti.

Oba dva typy výše popsaného software využívají bezpečnostních zranitelností nebo neopatrnosti uživatele. A především na neopatrnosti uživatele je založen tento typ „podnikání" – rozeslání tisíců podvodných emailů náhodným (či pečlivě vybraným) koncovým uživatelům a poté jen čekat, kolik z nich se nechá nachytat a následně zaplatí požadované výkupné. Úspěšnost takových „kampaní" se pohybuje od 5% v případě relativně standardních emailů, až po desítky procent v případě podvodného emailu sestaveného na míru. Proč se tomu tak děje?

Že Internet není úplně bezpečné místo pro otevřenou komunikaci, ví v současné době snad každý, i když je stále překvapující, kolik interních, osobních a citlivých dat jsou o sobě uživatelé ochotní sdělit v zásadě anonymní síti. Dlouhodobě organizace (a stále častěji i jednotlivci) chrání svůj přístup do Internetu pomocí různých zařízení, především pomocí firewallů (specializované zařízení schopné kontrolovat a případně omezovat provoz mezi koncovým zařízením a Internetem). Nicméně není schopno ochránit proti emailu, který je poslán z legitimní adresy na emailovou adresu koncového uživatele. A zmíněný firewall chrání především komunikaci z Internetu do vnitřní sítě. Od koncového počítače směrem do Internetu bývá komunikace většinou neomezená, nebo pouze nedostatečně. A pokud je koncový počítač ovládnut nějakým typem malware, tak mu již téměř nic nebrání v navázání komunikace s útočníkem, který je ukryt „někde" na Internetu. Více než 90% všech počítačových útoků začíná útokem na koncového uživatele pomocí zmíněného emailu, nebo pomocí metod sociálního inženýrství (snaha podvodem vylákat od uživatelů jejich osobní informace, jako jsou hesla nebo bankovní údaje, případně získat přístup k jejich počítači).

Proč je složité se útokům vyhnout?

Vyjmenujeme několik důvodů, proč jsou tyto útoky tak úspěšné:

Jde o vysoce ziskové podnikání s malými vstupními náklady. Proto se mu věnují jako specializované kriminální skupiny, tak jednotlivci. Všechny potřebné nástroje a návody lze snadno získat přímo na Internetu.

Uživatelé neradi mění své zvyky, které si přinášejí z předchozích zaměstnání, z minulosti (vždy mi stačilo jedno heslo, vždy jsem to dělal takto ...), každý si rád zjednodušuje svůj život.

Rizika na Internetu jsou komplikovaná, každý má svých starostí nadbytek, pracovního vytížení a ještě se k tomu učit, jak se bránit stále sofistikovanějším pokusům o podvod – na to nikdo nemá čas

Hesla, stále stejná hesla, která jsou jednoduchá, snadno zapamatovatelná, nalepená na papírku na monitoru, případně uložena v mobilu v kontaktech, využívání generování hesel pomocí webových prohlížečů – to jsou všechno velmi rizikové způsoby „ochrany" našich největších tajemství i přístupů na jednotlivé webové stránky vyžadující přihlášení. Specializovaný software na generování bezpečných hesel stále využívá jen každý pátý uživatel (a přitom jde v naprosté většině případů o bezplatný software v případě použití jednotlivcem či rodinou).

Školení na kybernetickou bezpečnost v naprosté většině případů připravují IT pracovníci, případně bezpečnostní specialisté – problém je v tom, že nejsou uzpůsobena koncovým uživatelům, pro které jsou tím pádem příliš technická, nebo nesrozumitelná, nebo dlouhá – důvodů lze vyjmenovat vícero.

Křivka zapomínání. Funguje u každého. Lze ji připodobnit je sjezdovce (v závislosti na tématu od sjezdovky modré až po černou), každopádně když se uživatel podrobí jednorázovému, většinou vícehodinovému školení v lednu a zeptáte se na naučené za půl roku, většina uživatelů bude dlouho lovit v paměti vše, co se v lednu naučila. K tomu si připočtěme pracovní nároky související s pracovním zařazením uživatele, zvyšující se tlak na výkon, málo času ... poté stačí chvilka nepozornosti a neštěstí je téměř na světě.

Důvody proč se nevzdělávat systematicky v oblasti kybernetické bezpečnosti lze slýchat poměrně často a v různých variacích:

- Máme limitovaný rozpočet, použijeme něco zdarma, případně naše IT něco připraví. Odpověď je jasná: věci zdarma nikdy nefungují dle předpokladů, jednorázové IT školení se nevyrovná celoročnímu systému vzdělávání.
- Limitovaný čas, uživatelé jsou přetížení vlastní prací, nemůžeme jim naložit ještě hodiny vzdělávání... odpověď na tyto námitky: pokud je použit správný systém vzdělávání, jde o krátké, srozumitelné bloky zaměřené na konkrétní problematiku, rozložené v čase, přizpůsobené času.
- Limitované zdroje, nemáme, kdo by se o to staral, nezvládneme (nebo nechceme) další složitý nástroj, software. Odpovědí je: ve většině případů jde o webové rozhraní, použitelné na libovolném zařízení, administraci zvládá IT, HR, případně vždy partner.

Jediná možná odpověď

Na začátku se sluší říci, že stoprocentní ochrana neexistuje. Respektive existuje, ale je natolik finančně náročná, že není únosná pro žádnou organizaci, která to myslí s bezpečnostní vážně. Pomineme ochranu typu být „odpojen", to je v současné době pro naprostou většinu firem a jednotlivců nemyslitelné.

Celkovou bezpečnost organizace si lze představit jako takovou zjednodušenou trojnožku, která sestává z těchto nohou:

Technologie. Používání správných technologií, správně nastavených, pravidelně aktualizovaných nám pomáhá snižovat riziko.

Procesy. Vědět, jak se chovat, co mohu a co už nesmím, jak nakládat s daty, přístupem, využitím techniky, jak se zachovat v případě havárie je velmi důležité a pomáhá předcházet mnoha incidentům, nejen bezpečnostním.

Lidé. Správně vzdělaní uživatelé v oblasti kybernetické bezpečnosti, znalí procesů a používání technických prostředků jsou stejně důležití, jako předchozí dva pilíře. Konec konců – pokud budete sedět na trojnožce, jejíž jedna noha bude kratší, bude to vždy o štěstí, než spadnete ...

Cílem je tedy udržet tyto tři pilíře v souladu, a pokud možno eliminovat slabé články celého řetězu.

Jedinou možností je pravidelné vzdělávání uživatelů, a to způsobem, který jim umožní se vzdělávat v době, kdy jim to vyhovuje, jazykem, kterému rozumí, a na úrovni, která je potřebná pro výkon jejich vlastní práce. Takový ucelený vzdělávací systém je souhrnem mnoha disciplín, které jej naplňují společně (IT, bezpečnost, pedagogika, psychologie ...).

Z čeho se takový systém má skládat?

- Vzdělávací moduly, které jsou zaměřeny vždy na jednu konkrétní problematiku (například: používání hesel, ochrana proti sociálnímu inženýrství, jak rozpoznat škodlivý email...).
- Modul musí být dostatečně obsažný a zároveň krátký, aby bylo možno jej absolvovat ve standardní pracovní době. Průměrná doba na absolvování modulu by neměla přesáhnout 15 minut.
- Modul v sobě má obsahovat rovnou i kontrolní a testovací otázky, které uživateli „beztrestně" pomohou problematiku pochopit a vyzkoušet.
- Zpětná vazba musí být „vlídná", vysvětlující a pomáhající uživateli se správně v problematice zorientovat.
- Moduly by měly být modifikovatelné – žádná organizace není stejná.

Reporting. Je podstatné pro řídící pracovníky, pro pracovníky bezpečnosti vidět, jak uživatelé vzdělávacím procesem procházejí. Pokud se najde skupina uživatelů, kteří bojují s některou problematikou více než jiní, díky reportingu je snadnější tuto skupinu identifikovat a buď ji dát ke školení jinak koncipovaný modul se stejnou problematikou, nebo si ji prostě sezvat do zasedací místnosti a vyložit ji problematiku jinými slovy – a opět zacelit jeden slabý článek řetězu.

Testovací modul. Správně sestavené testovací sady pomáhají opakovat naučenou problematiku a zároveň dle vědomostí uživatelů umožňují vzdělávání zacílit dle výsledků testů.

Platforma by měla být schopna fungovat na libovolném zařízení, v lokálním jazyce dle preference koncového uživatele. Školení musí být cílené, schopné posílat moduly napříč celou organizací, případně na specifická oddělení, nebo individuálně na jednotlivé uživatele.

Pokud shrneme hlavní požadavky na takovou platformu, tak:

Platforma musí umožnit uživatelům stát se poslední obrannou linií a měnit se z uživatele "rizikového" na uživatele "připraveného".

Platforma musí poskytnout jednotlivým uživatelům správné školení ve správný čas.

Učení hrou – již od dětství víme, že je to nejlepší způsob výuky.

Délka lekcí a jejich skladba – schopnost se soustředit na konkrétní problematiku je limitovaná – lekce nesmí být příliš dlouhá.

Uživatel musí snadno pochopit myšlenku učitele a vzdělávání si „užít" natolik, aby se těšil na další lekci.

Zpětná vazba musí být motivující a „vlídná".

Lidský firewall

Cílem uceleného systému vzdělávání je, jak již bylo řečeno, umožnit uživatelům stát se poslední obrannou linií a měnit se z uživatele „rizikového" na uživatele „připraveného".

Jak taková změna probíhá? Po úvodním testování je připraven minimálně roční vzdělávací program, proložený testy a kontrolními body, které umožňují flexibilně reagovat na aktuální změny situací ve světě a v ČR (covid, válka, ekonomická krize – libovolné téma, a který bývá okamžitě zneužito útočníky), který je zaměřen na konkrétní potřeby a úroveň znalostí každého jednotlivého uživatele.

Jak můžeme pomoci?

Jsme partnerem společností ProofPoint a SoSafe, pomocí jejichž produktů sestavujeme vzdělávací programy na míru pro libovolný typ a velikost organizace. Mezi naše zákazníky patří státní správa i soukromý sektor, firmy o velikosti 20 uživatelů i organizace čítající stovky koncových uživatelů.

Vzhledem k důležitosti této problematiky jsme podstoupili akreditační proces u MV ČR a v současné době poskytujeme tyto vzdělávací kurzy i jako akreditované. Samozřejmostí je naše podpora po celou dobu vzdělávacího procesu.

Kromě výše uvedeného uceleného programu nabízíme našim zákazníkům:

- Jednorázová specializovaná školení (pro IT, pro management společnosti, pro konkrétní problematiku).
- Testování uživatelů pomocí simulovaných phishingových útoků s následným vyhodnocením a návrhem kroků ke snížení rizika.
- Testování uživatelů pomocí metod sociálního inženýrství.
- Vulnerability a penetrační testy celého IT organizace. Výstupem bývá vždy podrobná zpráva s návrhem opatření pro snížení případných nalezených rizik.

Pro více detailů nás prosím kontaktujte na emailu info@datasense.cz

Božetěch Brablc
Managing Partner
DATASENSE

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI

SIMULOVANÝ ÚTOK NA VLASTNÍ KŮŽI

PRAKTICKÝ TEST ODOLNOSTI UŽIVATELŮ JAKO NOVÁ FORMA ŠKOLENÍ IT BEZPEČNOSTI

Víte, že pro úspěšný průnik do vaší interní sítě stačí jediná oběť, která útočníkovi podlehne? Zamyslete se nad tím, zda byste vy nebo vaši uživatelé techniky útočníka včas odhalili.

Nejslabší článek

Všichni víme, že odolnost jakéhokoli systému je tak silná, jak silný je jeho nejslabší článek. Máte představu, kolik uživatelů sítě by podlehlo cílenému útoku na vaši organizaci? Nebo zda by vůbec kontaktovali IT oddělení v případě podezření na phishing nebo jinou hrozbu? Znají vůbec, jak podobný incident rozpoznat a koho kontaktovat? Profesionálové totiž záměrně útočí na běžné uživatele internetu coby nejslabší článek bezpečnosti. Jak vypadají následky takového útoku, jsme se všichni mohli přesvědčit v medializovaných případech jedné české nemocnice a těžební společnosti. Obě organizace byly v důsledku nerozpoznaného phishingu a následné řetězové reakce dalších selhání infikovány kryptovirem a přinuceny zastavit provoz až na několik dní. Způsobené škody se v obou případech počítají v desítkách milionů korun.

Psychologický nátlak

Při útocích zaměřených na uživatele sítí nejde jenom o technickou připravenost v podobě sofistikovaného malwaru. Neméně důležitá je i tzv. back story, tedy jakási série smyšlených argumentů, díky kterým útočník vyvine na uživatele dostatečný psychologický nátlak. Oběť pak snadněji podlehne. Vyhoví jeho požadavkům a poskytne mu třeba i své přihlašovací údaje.

Zkušený útočník pracuje s emocemi. Zejména se strachem či s radostí, případně se zvědavostí. Využije strachu ze špatně odvedené práce, kontroly úřadu, nedoplatku dlužné částky. V radostných případech zneužije touhu po kariérním postupu, pochvalu, finanční prémii nebo jiný lákavý bonus. Útočník dobře ví, že pokud informace zpracováváme pod vlivem emocí, zapomínáme kriticky myslet a jsme snáze zranitelní.

Útok

Útočník nejčastěji využije oslovení e-mailem. Jde stále o efektivní a účinný vektor pro zahájení útoku. Použije perfektní češtinu. Dokonce věrohodně napodobí i styl firemní komunikace. Vydává se např. za zaměstnance personálního oddělení a žádá od svých kolegů, aby si prostřednictvím odkazu ve zprávě zkontrolovali výplatní pásku kvůli možným chybám v počtu odpracovaných hodin apod.

Uživatel se tak rázem ocitne ve stresové situaci. Aby nepřišel o část své výplaty, na odkaz bez delšího uvažování klikne, zadá své přihlašovací údaje do podvodné stránky, která ovšem všechny údaje ukládá přímo na server útočníka. Ten tak získá heslo, které zaměstnanec možná používá i pro přístup do dalších interních systémů. Pokud je obětí zaměstnanec, který je zároveň administrátorem, útočník získal cenný úlovek a může si směle vytvořit tzv. backdoor – zadní vrátka pro trvalý přístup do vnitřní sítě organizace.

Arzenál útočníka

Mezi oblíbené a vysoce účinné prostředky útočníka patří reverzní proxy, která funguje jako podvržený prostředník pro spojení s legitimním portálem. Ale pozor, ukládá si všechna autentizační data a je plně pod kontrolou útočníka. Tímto způsobem je možné překonat i dvoufaktorovou autentizaci.

Často zneužívanými nástroji jsou také makra v programech Microsoft Office. Malé pomocné programy uložené standardně ve Wordu nebo Excelu, které je možno naprogramovat tak, aby kontaktovaly server útočníka a stáhly si z něj sadu programů pro vytvoření již zmiňovaného backdooru nebo kryptoviru. Ten se v kombinaci s dalšími zranitelnostmi následně rozšíří již za pár vteřin po celé interní síti.

V poslední době jsme svědky také tzv. zero-day zranitelností dostupných v běžném programovém vybavení, mimo jiné i v nejpoužívanějších prohlížečích a programech Microsoft Office. V případě těchto zranitelností stačí často pouhé kliknutí uživatele na odkaz nebo na přílohu a nejhorší scénář může být ihned realizován.

Pozor na telefony a USB

Vektor útoku může být uskutečněn také mnohem aktivněji prostřednictvím telefonu nebo flash disků, které patří mezi další hojně zneužívaná zařízení. Stačí, když takových pár disků útočník jen tak zanechá ve veřejně dostupných prostorách kanceláří. Je vysoce pravděpodobné, že některý z uživatelů disk najde a vloží do svého počítače. Takový flash disk může být naprogramovaný jako klávesnice, začne chrlit stovky znaků a otevře tak za pár sekund zadní vrátka útočníkovi pro přístup do interní sítě.

V případě telefonátu pak dokáže útočník simulovat například služební hovor a vystupovat v roli nadřízeného. Podvrhne oběti telefonní číslo ředitele společnosti, kde dotyčná osoba pracuje. Telefon přiřadí k číslu shodné jméno ze svého telefonního seznamu, případně i uloženou fotografii, a zobrazí příchozí hovor jako standardní volání pana ředitele. Pak se stačí útočníkovi vymluvit na okolní hluk, horší signál nebo nachlazení a následky takového hovoru si už nemusíme ani vysvětlovat.

Praktický test uživatelů

Nejinteraktivnější z možností, jak snížit šance útočníka při podobných útocích, je vyzkoušet si takový útok na vlastní kůži a zjistit, jak se uživatelé skutečně zachovají. Nechat se nachytat v simulovaném útoku nemá vliv na fungování společnosti a má pozitivní edukativní účinek pro všechny.

Základem takového útoku – odborně penetračního testu s využitím prvků sociálního inženýrství – je detailní scénář realizace. Zahrnuje použitou identitu útočníka, seznam obětí, kanál pro jejich oslovení i podrobnosti o škodlivém balíčku. Samozřejmostí je na míru vytvořená zpráva a forma oslovení, která je společným výsledkem týmu etických hackerů a zadavatele tak, aby přesně odpovídala zkušenostem a kladeným nárokům na testované uživatele.

V průběhu testu pak sledujeme jejich reakce a chování. Zda otevřeli e-mail, stáhli přílohu, klikli na odkaz, případně poskytli i přihlašovací údaje. Můžeme tak efektivně vyhodnotit odolnost uživatelů vůči reálné hrozbě – jestli útok vůbec vzbudil podezření nebo jej někdo nahlásil jako bezpečnostní hrozbu.

Zároveň můžeme otestovat reakci vašich detekčních mechanismů od kontrol na koncových stanicích v podobě EDR řešení až po vaše security operační centrum nebo SIEM. Získáte tak přehled o reakci IT oddělení a další užitečné informace.

Motivujte k bezpečnosti

Při návrhu scénáře je vhodné myslet na to, jak simulovaný útok propojíme se zpětnou vazbou pro uživatele. Pracujeme vždy s pozitivní motivací. Uživatele, kteří v testu úspěšně obstojí nebo podezřelou aktivitu nahlásí, můžeme směle odměnit. Naopak uživatele, kteří se stali oběťmi, zásadně netrestáme.

Školicí efekt můžeme navíc posílit edukativní stránkou, na kterou budou uživatelé přesměrováni v případě, že podlehli etickým hackerům. Ta je názorně informuje o důsledcích útoků využívajících metod sociálního inženýrství a poskytuje rady, jak podobným útokům příště čelit.

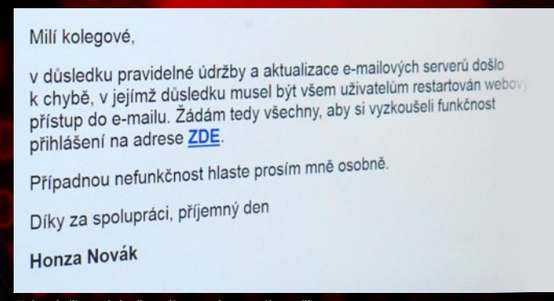
Vsaďte na kritické myšlení

Aplikace principů kritického myšlení by měla být základní technikou každého uživatele. Už jen pouhé pozastavení se a zamyšlení nad adresou odesílatele nebo URL adresou v mnoha případech postačuje pro odhalení útoku.

Mgr. Peter Šinaľ
společnost
Trusted Network Solutions

Nechat se nachytat v simulovaném útoku nemá vliv na fungování společnosti. Ale má pozitivní edukativní účinek pro všechny účastníky testu.

Podvržené číslo si telefon přiřadí ke shodnému číslu ve svém uloženém seznamu a telefonát zobrazí jako běžný příchozí hovor ze známého čísla!



Milí kolegové,

v důsledku pravidelné údržby a aktualizace e-mailových serverů došlo k chybě, v jejímž důsledku musel být všem uživatelům restartován webový přístup do e-mailu. Žádám tedy všechny, aby si vyzkoušeli funkčnost přihlášení na adrese ZDE.

Případnou nefunkčnost hlaste prosím mně osobně.

Díky za spolupráci, příjemný den

Honza Novák

Takový či podobně stylizovaný e-mail patří stále mezi vysoce efektivní a účinné vektory pro zahájení útoku.

Poznámka redakce:

Autor článku Mgr. Peter Šinaľ působí ve společnosti TNS, kde řídí tým etických hackerů a vykonává funkci bezpečnostního manažera pro významné české organizace. Specializuje se na propojení technologií a psychologie při realizaci testů odolnosti uživatelů – sociálního inženýrství.

EFEKTIVNÍ NEDESTRUKTIVNÍ PROHLÍDKY AUTOMOBILŮ

JAK SE VYHNOUT ZBYTEČNÝM ŠKODÁM PŘI PÁTRÁNÍ PO DROGÁCH A PENĚZÍCH

Na silnici jste zastavili podezřelý vůz a po pěti minutách hovoru s řidičem máte jasno. Získali jste souhlas, nebo váš pes vycítil narkotika, takže máte oprávněný důvod vozidlo prohledat. Je zřejmé, že někde tu jsou ukryté drogy – teď jde jen o to, abyste je s pomocí psa a dalších nástrojů také našli. Váš čtyřnohý pomocník reaguje na přední část vozu. Další dvě hodiny tak na krajnici strávíte prohledáváním auta; postupně zkoušíte nárazníky, blatníky, přístrojovou desku. Obuškem proklepete pneumatiky a prohmatáte sedačky. Zkusíte první poslední, ale pořád nic. Už zbývá jen destruktivní prohledání – a když vyjde negativně a žádný kontraband nakonec neodhalíte, může se to vašemu oddělení pěkně prodražit. Nemáte jinou možnost, než zatnout zuby a nechat řidiče odjet. Na tuhle zkušenost ale nezapomenete – vryje se vám hluboko do paměti.

Aktuální výzvy při prohledávání vozidel

V situaci, kdy potřebujete prohlédnout podezřelý automobil, jsou priority jasné: chcete být rychle hotoví a vyvarovat se zbytečných škod. Musíte být pečliví, ale nemáte na to celý den. Najít tu pravou rovnováhu mezi intuicí a bezpečnostními riziky, stížnostmi veřejnosti nebo náklady kvůli způsobené majetkové škodě, může být pořádný oříšek. Jako by toho už tak nebylo dost, dají se v autech kvůli jejich konstrukci drogy či peníze schovat na spoustě různých míst. V područkách, sedačkách nebo přihrádce spolujezdce – všude je dostatek prostoru jako stvořeného pro pašování. Už vůbec nemluvě o všech dalších skrýších, které kreativní pašeráci při maskování kontrabandu umí vymyslet.

Existuje mnoho účinných způsobů prohlížení aut bez sofistikované techniky – od proklepávání obuškem až po nahlížení do štěrbin za pomoci kapesní svítilny. Jenže v rušném a hlučném prostředí, kde není pořádně slyšet a těžko se dostáváte, kam byste potřebovali, může být takový postup dost složitý. Krom toho je potřeba vyzkoušet nejen staré známé triky, ale i novější rafinované techniky ukrývání nezákonných materiálů, s nimiž vynalézaví pašeráci neustále přicházejí. Trvalé zlepšování vyhledávacích postupů je proto nutné pro zaručení bezpečnosti strážců pořádku i možnosti zkontrolovat co nejvíce aut a zachytit maximum kontrabandu.

Nejdůležitější vlastnosti účinných prostředků nedestruktivního prohledávání

První a nejdůležitější podmínkou je, aby příslušné systémy nebo zařízení ochráncům zákona pomáhaly odhalovat drogy nebo hotovost umístěné do některého z běžných úkrytů ve voze nebo speciální skrýše v interiéru vozidla. Jelikož auta mohou být poměrně malá a je v nich řada hůře dostupných míst, měla by manipulace s vyhledávacím prostředkem být co nejsnazší i pro jednu osobu.

Optimální je použití systémů fungujících podobně jako kompaktní fotoaparát – namířit a stisknout spoušť. Zároveň je ale nutné, aby přístroj byl co nejrychleji připraven k provozu; ideální je možnost začít s kontrolou hned po zapnutí a snadno přejít na místa, která budou nejspíše sloužit k ukrytí kontrabandu. Kontroly by měly být co nejjednodušší a nejrychlejší. Nemělo by docházet k mrhání drahocenného času laděním všemožných nastavení, nebo čekáním na vyhodnocení výsledků. Krom toho musí mít systémy, u nichž se počítá s potřebou okamžitého nasazení, také dostatečnou kapacitu baterie tak, aby je bylo možné používat celý den bez nutnosti dobíjení.

Denzimetry jsou rychlé i dobře přenosné, poskytují však pouze číselný údaj bez možnosti blíže určit, co vlastně za výsledkem měření stojí. Nejmodernější systémy pro prohlídky vozidel proto využívají rentgenovou technologii, která okamžitě poskytuje snímek prověřované oblasti. Jedním z takových zařízení je i ruční detektor MINI Z®, který pracuje na principu zpětného rozptylu a nabízí ideální možnost rozlišení konstrukčních součástí vozidla a skutečných anomálií představujících potenciální kontraband.

Po rozhovoru s řidičem a zapojení čtyřnohého pomocníka můžete pomocí systému MINI Z konkrétní části vozu velmi rychle prověřit. Možnost „podívat se" do přístrojové desky, sedaček, područek nebo pneumatik nejen přispívá k rychlému odhalení pašovaných drog nebo hotovosti, ale zároveň umožňuje předem vyloučit „čisté" oblasti tak, abyste se mohli zaměřit na ty správné části těch správných vozů. Ruční prohlídka auta může zabrat až dvě hodiny a při negativním výsledku znamená zbytečné poškození vozu, náklady pro vaše oddělení a spoustu papírování. Použití ručních rentgenových detektorů jako MINI Z zkracuje čas prohlídky v průměru na 20 minut. Nedestruktivní postup omezuje poškození vozu na minimum a předchází pozdějším starostem kvůli zbytečným nákladům i papírování. Na pneumatikách zkontrolovaných tímto postupem může auto hned znovu vyjet na silnici.

Pro mnoho ochránců zákona je prohledávání vozidel podezřelých z pašování drog či hotovosti každodenní rutinou a tvoří kritickou součást boje proti ilegálnímu obchodu s drogami. Při nasazení vhodných detekčních systémů využívajících nejmodernější technologie může být práce na plnění těchto úkolů výrazně bezpečnější, rychlejší a snazší, aniž by při ní docházelo ke zbytečným škodám na vozech nebo k jejich ničení. „Padouši" jsou vynalézaví a neustále přicházejí s něčím novým, proto ani „klaďasové" nemohou zůstat pozadu.

O RUČNÍCH RENTGENOVÝCH KONTROLÁCH

MINI Z® je první a nejvýkonnější přenosný systém pro rentgenové kontroly, který umožňuje odhalování ukrytých organických materiálů a kontrabandu pomocí metody zpětného rozptylu Z Backscatter®. Tvar a kompaktní rozměry detektoru spolu s jednostranným sníláním garantují vynikající přenosnost a nepřekonatelnou flexibilitu. Díky tomu mohou strážci pořádku velmi snadno odhalovat pašované drogy, hotovost, nebo jiné organické materiály a kontraband přímo v terénu.

MINI Z používají celníci, policie, vojenské složky, bezpečnostní agentury a organizace bojující proti obchodu s drogami. Vhodný je ale i při ochraně kritické infrastruktury, vysoce rizikových zařízení nebo pro další použití vyžadující efektivní kontroly širokého spektra předmětů včetně nábytku, zásilek, vozidel, interiérů lodí a letadel. Systém MINI Z je zcela autonomní a nevyžaduje žádné nastavení ani doplňování provozních náplní. Dávky záření jsou z principu velmi nízké a zařízení obsahuje spolehlivé a redundantní bezpečnostní pojistky.

AS&E

TRVALÉ ZLEPŠOVÁNÍ VYHLEDÁVACÍCH POSTUPŮ JE NUTNÉ PRO ZARUČENÍ BEZPEČNOSTI STRÁŽCŮ POŘÁDKU I MOŽNOSTI ZKONTROLOVAT CO NEJVÍCE AUTOMOBILŮ A ZACHYTIT MAXIMUM KONTRABANDU.

IDEÁLNÍM ŘEŠENÍM PRO ÚČELNÉ A ÚČINNÉ NEDESTRUKTIVNÍ PROHLÍDKY AUTOMOBILŮ PŘÍMO V TERÉNU JSOU RYCHLÉ PŘENOSNÉ SYSTÉMY FUNGUJÍCÍ PODOBNĚ JAKO KOMPAKTNÍ FOTOAPARÁT.

POUŽITÍ RUČNÍCH RENTGENOVÝCH DETEKTORŮ ZKRACUJE ČAS PROHLÍDKY V PRŮMĚRU NA 20 MINUT, OMEZUJE NA MINIMUM POŠKOZENÍ VOZU A PŘEDCHÁZÍ POZDĚJŠÍM STAROSTEM KVŮLI ZBYTEČNÝM NÁKLADŮM I PAPÍROVÁNÍ.

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI

UNIKÁTNÍ MOBILNÍ RENTGEN
VE SLUŽBÁCH CELNÍ SPRÁVY

Mobilní zavazadlový rentgen se stal nevětším exponátem bezpečnostní techniky III. ročníku konference Ochrana měkkých cílů 2022, která se konala 09.06.2022 v Hotelu Olšanka v Praze. Autor mobilní nástavby a vestavby, společnost JÍŠA s.r.o., ve spolupráci s Celní správou ČR představili zařízení účastníkům konference, kteří měli možnost vidět a vyzkoušet jeho funkce v praxi. Mobilní rentgen, který slouží při pátrání po zboží uniklém celnímu dohledu, byl postaven jako světově unikátní řešení vestavby dvoupohledového zavazadlového rentgenu Rapi-scan 628DV s velikostí kontrolního tunelu o rozměrech 1 000 mm na 1 000 mm.

Uživatelem mobilního zavazadlového rentgenu (MZR) jsou skupiny mobilního dohledu, které působí jako operativní článek přímého výkonu kontrolní činnosti celní správy. Jejich hlavním úkolem je provádět kontroly přímo v terénu nad zbožím podléhajícím celnímu dohledu nebo spotřební dani a nad výkonem dalších kompetencí.

Významnou pozornost věnují hlídky i kontrole přepravy zboží dvojího užití v rámci Evropské unie. Na pozemních komunikacích kontrolují nákladový prostor a kabiny vozidel, včetně dokladů a dokumentů vztahujících se k dopravovanému zboží, určené trase, či lhůtě prováděné přepravy. Na stanovených úsecích pozemních komunikací vykonávají kontroly plnění povinnosti úhrady poplatku za užívání těchto komunikací. Důležitou pravomocí hlídek mobilního dohledu je i kontrolní vážení a měření jízdních souprav s přípojenými vozidly. Plní rovněž úkoly v oblasti odhalování zboží porušujícího některá práva duševního vlastnictví.

Skupiny mobilního dohledu jsou vybaveny speciálními kontrolnětechnickými prostředky, které slouží k odhalování tajných úkrytů určených k nelegální přepravě zboží a omamných a psychotropních látek. Významným pomocníkem celníků při kontrolách dopravních prostředků a přepravovaného zboží jsou mobilní rentgeny.

Řešením potřeb skupiny dohledu bylo pořízení mobilního zavazadlového rentgenu pro kontrolu zavazadel a zásilek přepravovaných primárně leteckou dopravou, které povede k urychlení a zefektivnění běžných kontrol celníky. Plánováno bylo využití zařízení zejména pro detekci nelegální přepravy tabáku a dalších tabákových výrobků umisťovaných v osobních zavazadlech a v přepravních obalech zásilek menších rozměrů v rámci všech mezinárodních letišť, kde je uskutečňována přeprava z/do třetích zemí, případně tranzit. Vzhledem k tomu, že se jedná o kontrolu prováděnou neinvazivní metodou, bylo očekáváno snížení rizika poškození kontrolovaných předmětů. Cílem bylo zmírnění nedostatku technického vybavení při vykonávání kontrolně-dohledových činností na malých mezinárodních letištích a dalších místech pro mobilní kontrolu.

Výzvy a řešení

„Při realizaci jsme vycházeli z reálných potřeb koncového uživatele. Pokud bych je měl jednoduše shrnout, rozdělil bych je do čtyř oblastí: požadavky na bezpečnostní technologie, efektivní provoz, komfort operátora a požadavky na samotné vozidlo," říká Ing. Milan Krása, ředitel divize Rapiscan společnosti PCS. „Chtěli jsme dosáhnout maximální možné funkčnosti a komfortu. Proto jsme hledali lokálního partnera, který bude schopen postavit nástavbu na vozidle s vestavěným zavazadlovým rentgenem a umožní nám technicky vyjít vstříc specifickým požadavkům objednatele. Partnera, který má bohaté zkušenosti a velmi dobré reference," dodává Krása. „Jsem rád, že naší volbou byla právě firma JÍŠA, která všechny uvedené požadavky bohatě naplnila a byla projektu velkým přínosem."

Bezpečnostní technologie

Vysoký bezpečnostní standard výkonu MZR byl nastaven volbou dvoupohledového zavazadlového rentgenu Rapiscan 628DV s velikostí kontrolního tunelu o rozměrech 1 000 mm na 1 000 mm, který zavazadlo snímá ve dvou pohledech. Rapiscan 628DV splňuje nejvyšší požadavky na kvalitu zobrazení.

Efektivní provoz

„Požadavky pro efektivní provoz byly rozmanitější," odhaluje Krása. „Jednalo se například o mechanické válečkové dopravníky, jejichž použití limitovala maximální povolená šířka vozidla pro provoz na pozemních komunikacích."

„Ano, největší výzvou celé nástavby bylo prostorové uspořádání. Vzhledem k rozměru rentgenu a jeho příčnému uložení, bylo zapotřebí zažádat Ministerstvo dopravy o výjimku na celkovou šířku vozidla a upravit boční výklopy vozidla tak, aby kapsy doléhaly na konec dopravníku. Zároveň bylo nutné posunout vypínací válce dopravníkového pásu blíže ke středu rentgenu a tím celý dopravník zkrátit," vzpomíná na realizaci Josef Jíša, jr., jednatel společnosti JÍŠA s.r.o. „Přídavný sklápěcí válečkový dopravník jsme museli zkonstruovat tak, aby v transportní poloze byl umístěn dovnitř rentgenu a zároveň s hranou vstupního otvoru. Skládací konstrukce dopravníku nyní umožňuje použití buď v plné, nebo ve zkrácené délce a zároveň je možné dosáhnout požadované maximální výšky nakládací hrany dopravníku," dodává Jíša.

Aby bylo, pro případ provozu rentgenu na přídavný akumulátor, minimalizováno riziko jeho vybití pod úroveň, která ohrožuje nastartování vozidla, byl do vozu instalován stálý elektronický monitoring přídavných baterií. Signalizace upozorní obsluhu před hlubokým vybitím baterií a působí jako ochrana startovacího akumulátoru.

Dále byla nástavba vybavena kamerami snímajícími vstup a výstup rentgenu se zobrazováním na samostatném monitoru v kabině operátora tak, aby vedle rentgenového obrazu zavazadla měl operátor při vyhodnocování k dispozici záběr z kamery pořízený při manipulaci se zavazadlem. Operátor má tak pod kontrolou workflow od okamžiku položení zavazadla na pás až po jeho odebrání.

Kvalitní komunikační systém pro zajištění oboustranné komunikace mezi stanovištěm operátora a venkovní obsluhou je zásadní. Pracovníci jej ocení zejména v situacích, kdy operátor potřebuje zavazadlo vložit do rentgenu jiným způsobem, než bylo původně vloženo, nebo v případě potřeby zastavení dalšího nakládání zavazadel na dopravník, do doby než budou odebrána zavazadla na výstupu. Pro zajištění hladké komunikace byl do vozidla instalován interkom.

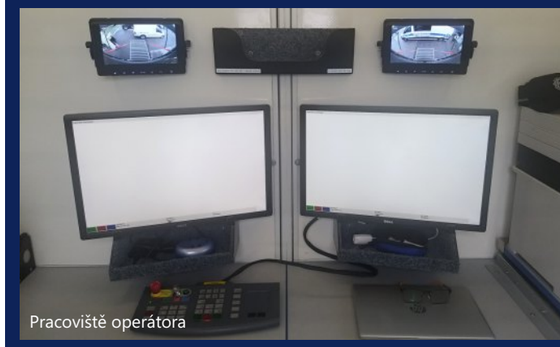
Komfort operátora

„Z řady požadavků ovlivňující komfort operátora byl zcela jistě zásadní požadavek na provoz při extrémně vysokých či nízkých venkovních teplotách. Z tohoto důvodu byla do kabiny operátora instalována nezávislá, elektronicky nastavitelná klimatizace, doplněná o nezávislé topení s možností digitálního nastavení," říká Jíša, jr. „Stejně tak bylo zapotřebí upravit provozní podmínky pro bezpečnostní techniku. Za normálních okolností má rentgen rozsah provozních teplot od 0 °C do +40 °C. Protože klient požadoval teplotní rozsah již od –10 °C, bylo zapotřebí zajistit temperování rentgenu a výhřev motoru dopravníku," říká Jíša, jr.

Za zmínku jistě stojí osvětlení inspekčního tunelu rentgenu, které je řešeno umístěním LED pásky po celém obvodu výklopu rentgenu a zajišťuje tak rovnoměrné osvětlení celého prostoru. Oproti klasickému jednobodovému zdroji osvětlení toto řešení rozptyluje stíny a eliminuje vznik kontrastních ploch, které jsou pro lidské oko náročné a unavující. Zároveň LED osvětlení zajišťuje výrazně lepší světelné podmínky pro kameru snímající vstup a výstup rentgenu.

Dále bylo vozidlo na každé boční straně vybaveno markýzou s plným přesahem na inspekční otvor rentgenu. Markýza slouží jako ochrana před deštěm a zároveň rozptyluje přímé sluneční světlo. I když požadavek zadavatele na aretaci otevíracích přístupových dveří kabiny operátora (v otevřené poloze) může laikovi znít úsměvně, jeho význam pro pracovní komfort je zásadní. Zkuste si představit, co s nimi udělá vítr. V souvislosti s dveřmi, byly také řešeny schody do kabiny operátora, které jsou zkonstruovány jako výsuvné a v transportní poloze zajištěny aretací a signalizací, která upozorní řidiče v případě úmyslu rozjezdu vozidla s vysunutými schůdky.

„Při realizaci takovýchto projektů je klíčová spolupráce, a to nejen mezi uživatelem a dodavatelem, ale také mezi partnery, díky které mohou vzniknout jedinečná řešení, postavená na důvěře a zkušenostech. Příkladem může být právě spolupráce společností PCS a JÍŠA a jejich unikátní řešení," uzavírá Krása.


Pracoviště operátora


Kontrolní pracoviště připravené k provozu

O projektu

- Mobilní zavazadlový rentgen slouží při pátrání po zboží uniklém celnímu dohledu, při kontrolách zavazadel cestujících a zásilek na letištích s mezinárodním provozem. Výhodou zařízení je neinvazivní kontrola a snížení její časové náročnosti.
- Zadavatelem výběrového řízení bylo Generální ředitelství cel. Vítězným dodavatelem zakázky se stala společnost PCS spol. s r.o. Autorem realizace nástavby a vestavby vozidla je společnost JÍŠA s.r.o.
- Zvoleno bylo řešení nástavby na vozidle typu MAN TGE vybavené technologií pro bezpečnostní kontrolu výrobce Rapiscan Systems.
- Mobilní zavazadlový rentgen je světově unikátní vestavbou dvoupohledového zavazadlového rentgenu Rapiscan 628DV s velikostí kontrolního tunelu o rozměrech 1 000 mm na 1 000 mm.
- Pořízení mobilního zavazadlového skeneru bylo spolufinancováno z programu Evrop-ské unie HERCULE III.

Nadace O2 vs. kyberhrozby

Dezinformace, kyberšikana, online podvody, radikalizace dětí na internetu, bezpečnost v online světě… Těmto tématům a ještě mnoha dalším se věnuje Nadace O2 prostřednictvím portálu O2 Chytrá škola a informačního webu Bezpečně v síti.cz. Víte, s čím vším se děti mohou v online prostoru potkat? A s kým?

I firemní nadace se mohou podílet na větší bezpečnosti společnosti. Každý se může zapojit podle svého nejlepšího vědomí, svědomí a možností. Do boje proti hrozbám na internetu, se kterými se může potkat kdokoli, vyrazila i Nadace O2. A zaměřila se na pomoc těm nejzranitelnějším z nás – dětem.

Když se dnes podíváme na web O2 Chytré školy, je těžké uvěřit, že vznikl teprve v roce 2019. Za několik málo let se ve spolupráci s experty povedlo obsáhnout tematicky nejpalčivější oblasti online světa a poskytnout tím pedagogům dobrý základ pro výuku digitálního vzdělávání na školách.

Přestože ve školách tráví děti a dospívající většinu svého času, velký vliv na ně mají samozřejmě i rodiče.

Vedle vzdělávání pedagogů tak Nadace O2 věnuje pozornost i osvětě veřejnosti. Na webu Bezpečně v síti.cz se tak všichni mohou dočíst o aktualitách z online světa. A to prostřednictvím lifestylových článků, které však vždy odkazují na knihovnu O2 Chytré školy, kde je téma rozpracováno více do hloubky a posvěceno odborníky na danou oblast.

Mimo to se společnost O2 podílí na výzkumech, které otvírají někdy opomíjená, ale palčivá témata současné doby. Nejnovější výzkum s názvem Děti a kult krásy v online světě, který společně uskutečnily Centrum prevence rizikové virtuální komunikace (PRVoK) Pedagogické fakulty s Katedrou psychologie a patopsychologie Pedagogické fakulty Univerzity Palackého a O2, přináší překvapivé výsledky.

Každé druhé dítě zažilo šikanu. Kyberšikanu pak každé třetí.

Dnešní technologická doba je do velké míry postavena na vizuálu. Televize, notebook nebo telefon nám prostřednictvím obrázků a videí poskytuje zábavu, ale otvírá tím i dveře možným hrozbám. Podle výzkumu Děti a kult krásy v online světě, kterého se zúčastnilo téměř 10 tisíc dětí a dospívajících, čelila posměškům v digitálním prostředí jedna třetina českých dětí.

Výzkum byl rozsáhlý a zaměřil se na několik aspektů: proč děti upravují svůj vzhled, jestli se respondenti setkali s nějakou formou online zesměšňování a jaký vliv mají tyto faktory na psychiku. A jak to dopadlo?

V online prostředí posměškům čelí nebo čelilo každé třetí dítě, nejčastěji se setkalo s bodyshamingem kvůli vlasům a obličeji. Přibližně deset procent z nich se setkalo se zesměšňováním spjatým s postavou. Sociální sítě jsou nelítostné, protože často ukazují dokonalé postavy, které však mohou být upravené a nereálné. To pak může mít negativní dopad na vnímání vlastního těla i psychiku.

„Přes 7 % dětí se začalo omezovat v jídle a 5 % dětí dokonce redukovalo příjem potravy na minimum," popisuje Jana Kvintová z Katedry psychologie a patopsychologie Pedagogické fakulty Univerzity Palackého v Olomouci. „Závažným zjištěním je pak přiznání přejídání se a následné vyzvracení potravy u 1,3 % dětí. Přes 7 % dětí začalo vnímat své tělo jako "tlusté", přestože je okolí ujišťovalo o opaku," dodává Kvintová.

Děti na internetu mohou najít i návody na sebepoškozování, půl procenta respondentů přiznalo dokonce vytváření takovýchto příspěvků. Stejné množství dětí (0,5 %) vytváří rovněž příspěvky zachycující násilí. Zdá se vám to málo? Pokud toho půl procenta přepočítáme na počet dětské populace, pak číslo signalizuje alarmující tisíce.

Děti si mohou samy nastavit ideální obraz, jak by mělo jejich tělo vypadat. Dříve se dospívající stylizovali do zpěváků, herců nebo bubeníků, dnešní děti mají ale jiné idoly. Youtubery, instagramery a další influencery, kteří však své fotky často upravují nebo se fotí na vícero pokusů. „Jen každé druhé dítě je podle výzkumu spokojené se svým obličejem, spokojenost s vlastním tělem deklarovalo 46 % dětí," říká Kamil Kopecký z Pedagogické fakulty Univerzity Palackého v Olomouci.

Otevírat opomíjená témata je klíčové

Nadace O2 je i partnerem mnoha zajímavých projektů a organizací. Úspěšným příkladem může být dokument V síti, kde je O2 Chytrá škola hlavním partnerem osvětové kampaně. „Ze současných projektů bych ráda vyzdvihla Commandera, který upozorňuje na nepříliš známé, ale nebezpečné téma radikalizace dětí na internetu," přibližuje projekt od souboru Farma v jeskyni manažerka Nadace O2 Dominika Herdová. „Tento projekt je jedinečný, protože v sobě kombinuje uměleckou i edukativní část. Díky tomu se může problematika radikalizace dospívajících v online prostředí rozšířit mezi širší veřejnost a dostat se do povědomí jako potenciální hrozba, kterou je třeba se zabývat," dodává Herdová.

„Radikalizace dětí a dospívajících je aktuálně řešené téma na mezinárodní úrovni, jelikož představuje závažný sociální a bezpečnostní problém," potvrzuje odbornice na extremismus a terorismus Barbora Vegrichtová a doplňuje: „Nebezpečí radikalizace dětí a mládeže spočívá v jejich značné vulnerabilitě, která vyplývá z neznalosti potenciálních rizik, a stejně tak v přílišné důvěřivosti či naivitě."

A právě informovanost a (sebe)vzdělávání může hrozbám v online světě zamezit. Pokud budou rodiče i učitelé předávat základy bezpečného chování dětem a sami dospělí budou tato doporučení dodržovat, bude internet bezpečnějším místem pro všechny.

Důležitost osvěty zdůrazňuje i Vegrichtová: „Ve snaze zabránit expanzi násilí mezi dětmi a dospívajícími je nezbytné zacílit systematickou osvětu a vzdělávání právě i na sektor učitelů, vychovatelů, speciálních pedagogů, sociálních pracovníků, kurátorů, psychologů a dalších profesionálů, kteří dlouhodobě pracují s dětmi a mládeží. Je třeba též zvyšovat digitální gramotnost rodičů, a především vhodným způsobem poučit děti a mládež o rizicích spojených s radikalizací ze strany extremistů."

Nadace O2 aktivně vyhledává a zpracovává témata týkající se bezpečí v kyberprostoru. Na portálu O2 Chytrá škola a přidruženém informačním webu Bezpečně v síti.cz najdete kapitoly a články věnované bezpečným heslům, kyberšikaně, kybergroomingu, stalkingu, sextingu, rizikům spojeným s užíváním sociálních sítí, digitální stopě, phishingu, virům, sociálnímu inženýrství a mnohým dalším neméně aktuálním tématům. Nadace O2 letos oslavila 20 let, během kterých proškolila přes 38 tisíc dětí a profesorů rámci programu O2 Chytrá škola.

Dominika Herdová
manažerka Nadace O2

O2 | Bezpečně v síti.cz

7 TIPŮ, JAK ČELIT KYBERŠIKANĚ

Pokusy bránit se jsou u šikany a kyberšikany zásadní i pro agresory samotné. Chtějí a potřebují, aby oběť reagovala. Proto je potřeba bránit se chytře, strategicky, a zachovat chladnou hlavu. Tady je pár tipů, jak na to.

1. Zajistěte bezpečí a podporu

Jako u každého problému i tady platí, že dítě ve vás potřebuje mít důvěru a cítit se bezpečně. Musí vědět, že za ním stojíte a pomůžete mu. Koneckonců chcete totéž – aby šikana skončila. Podobně to platí i pro šikanující děti. Křik, výčitky a zákazy nefungují. Chce to v klidu si sednout a dítěti vysvětlit, že svým chováním někomu ubližuje.

2. Věc vyšetřete a sdílejte informace

Je jedno, jestli šikanu odhalí rodič nebo učitel. Škola, rodiče dětí, kterých se šikana týká (ať už jde o oběti nebo agresory), a instituce specializované na šikanu jsou dobrým spojencem při řešení problému. Musíte zjistit, co přesně se stalo, kdo byl do kyberšikany zapojený a informovat druhou stranu (školu, rodiče oběti, ale i agresora). Jen tak můžete najít řešení. Pokud je součástí šikany vyhrožování fyzickým násilím, nebo k němu dokonce už došlo, je na místě kontaktovat policii.

3. Sbírejte důkazy

Je potřeba posbírat co nejvíce konkrétních důkazů. Budou se hodit při komunikaci s rodiči agresorů i s rodiči obětí. Vždycky je ale nutné zajistit bezpečí svědků. Nikde by nemělo být vidět nic, co by pomohlo například identifikovat spolužáka, který na šikanu upozornil a poskytl přístup do chatu nebo skupiny, kde kyberšikana probíhala.

4. Nezakazujte dítěti mobil a internet

Zákazy nic neřeší. Ani když zákaz dostane agresor. Dítě si cestu k internetu stejně najde. V šikaně bude postupovat chytřeji nebo přejde na klasickou šikanu mimo digitální svět.

5. Záležitost s šikanou se musí uzavřít

Chtějte vědět, jak byli potrestaní pachatelé a jaká opatření se zavedla, aby k šikaně už nedocházelo. Nenechte problém vyšumět do ztracena.

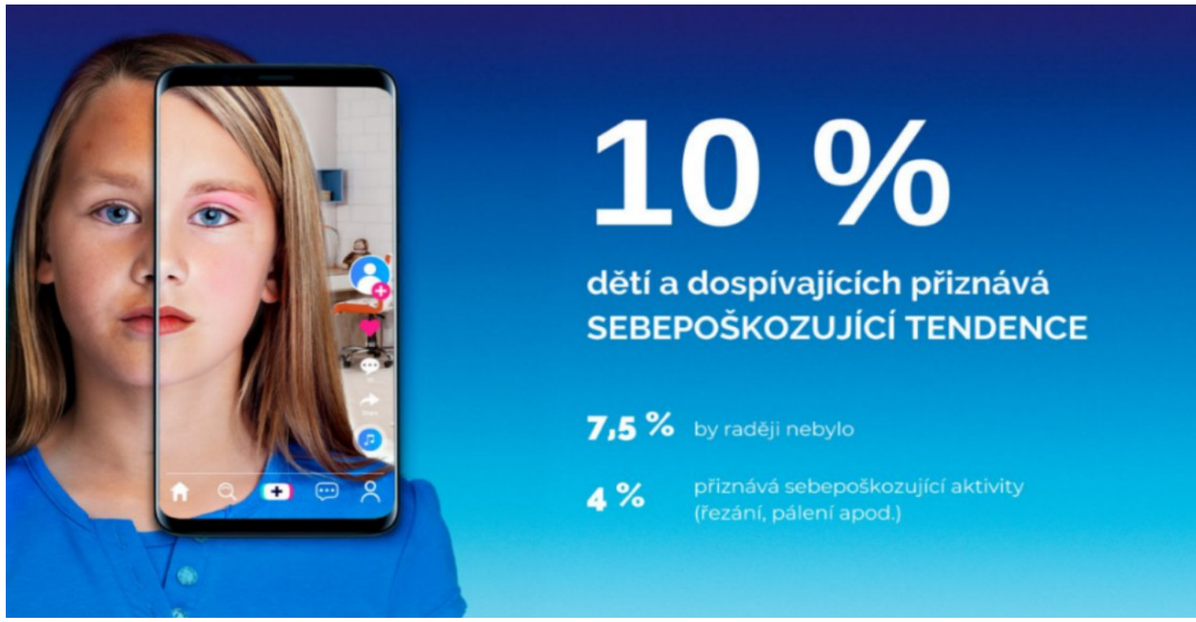
6. Zaveďte vlastní opatření proti šikaně

Pokud dítě někoho šikanovalo, je nutné ho potrestat a vysvětlit mu, že jeho chování ostatním ubližuje. Zároveň je ho ale třeba pozitivně motivovat. Pokud dostane nálepku agresor, bude se jako agresor chovat i v budoucnu. Klíčem k úspěchu je důslednost při dodržování pravidel.

7. Zaměřte se na prevenci

Společné nastavení zabezpečení sociálních sítí a ponaučení o šikaně jsou dobrou cestou, jak předejít dalšímu trýznění. Prevence je v případě kyberšikany důležitá i proto, že si hodně dětí následky svého chování na internetu neuvědomuje. Vyplatí se, pokud si škola ještě dřív, než bude nucená čelit nějakému většímu problému, vytvoří vlastní krizový plán pro řešení šikany a kyberšikany, včetně postupů a trestů.

KPKB
KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI



UKRAJINA A SOUČÁSTI JEJÍHO BEZPEČNOSTNÍHO SYSTÉMU

Kromě Národní policie Ukrajiny a Kriminální policie Ukrajiny, jejichž činnost jsem přiblížil v první části článku (v minulém čísle BsP), disponuje stát v obecné rovině ještě řadou dalších složek bezpečnostního systému.

Národní garda Ukrajiny

Významnou součástí systému je rovněž Národní garda Ukrajiny (Національна гвардія України), propojující policejní i vojenské činnosti a spadající do kompetence Ministerstva vnitra Ukrajiny. Složka je určena pro plnění úkolů směřujících k záchraně a ochraně životů, práv, svobod a jiných oprávněných zájmů občanů Ukrajiny, společnosti a státu. Celkový počet příslušníků tohoto tělesa nemůže podle zákona v době míru přesáhnout 60 000 osob.

Příslušníci Národní gardy musí během služby přerušit členství v politických stranách a odborových organizacích. Součástí tělesa jsou i rezervisté, jejichž příslušníci procházejí průběžným výcvikem. Od srpna 2019 jsou gardisté v daleko větší míře než předtím nasazováni i pro pochůzkovou činnost (районний патруль). Přitom nezřídka zasahují samostatně, bez přítomnosti policistů. Jsou však připojeni na „Informační portál Národní policie Ukrajiny".

Do prosazování práva na lokální úrovni bylo zapojeno asi 2 000 hlídek a 100 vozidel. S modelem souvisí i detailní a veřejně prezentovaná statistika. Například v první polovině roku 2020 zadržely jednotky Národní gardy 1 680 osob pro podezření ze spáchání trestných činů a 20 000 osob pro správní delikty.

Součástí rezortu jsou vedle Národní policie a Národní gardy i další tělesa, a to zejména: Pohraniční stráž, Migrační služba Ukrajiny a Služba pro mimořádné události (ochrana obyvatelstva, brigáda důlních záchranářů, hydrometeorologická služba, letecká záchranná služba, operační středisko linky 112).

Sbory obecní policie a jejich kompetence

Obecní policie (мунпальна варта) ідіv „evropském" smyslu slova není na Ukrajině v současné době zřízena. O tomto konceptu se nicméně uvažuje, a to i za využití zahraničních poradců. Jiní experti s místní znalostí jsou však proti, zejména z obavy z příliš těsných vazeb obecních bezpečnostních složek na místní oligarchy. Ostatně i pojem „bezpečnostní dobrovolník" může v kontextu Ukrajiny znamenat sponzorování projektu regionálním oligarchou. V roce 2015 byl sice v prvním čtení přijat návrh zákona „O obecní stráži", v roce 2019 byl však zákon stažen – jako jeden z oficiálních důvodů takového kroku byla uvedena koronavirová situace.

Iniciativu nicméně převzali namísto státu dobrovolníci, ale i samotné obce. Konkrétně v rámci Kyjeva existují dvě různé dobrovolnické organizace:

Městská bezpečnost (Муніципальна охорона), příspěvková organizace města, zřízená roku 2017, která funguje v souladu s pravidly společnosti poskytujících veřejné služby. Organizace vstupuje do výběrových řízení a nabízí bezpečnostní služby městským a dalším institucím (školy, školky, zdravotnická zařízení atd.), čímž se částečně samofinancuje.

Městská stráž (Муніципальна варта, MunVarta), dobrovolnická iniciativa, jejíž členové nepobírají mzdu ve vlastním smyslu slova.

Členové Městské stráže mohou zastavit pokus o spáchání trestného činu a zadržet pachatele, dokud nedorazí policisté. Nicméně, všichni ostatní občané Ukrajiny, všichni ostatní lidé mohou udělat totéž. Po zpřísnění karanténních opatření, souvisejících s bojem proti šíření koronaviru, byla Městská stráž vyzvána k uskutečňováním kontrol v parcích a v prostředcích hromadné dopravy. Případné prohřešky bylo možno řešit pouze domluvou, případně jejich nahlášením policii nebo organizaci Městská bezpečnost. Někteří členové se zapojili i do roznášky jídla starším obyvatelům.

Soukromé bezpečnostní služby na Ukrajině

Právním základem soukromé detektivní a bezpečnostní činnosti je Ústava Ukrajiny, mezinárodní smlouvy ratifikované Nejvyšší radou Ukrajiny, zákon č. 4616-17 „O bezpečnostních činnostech" z 22. března 2012 a zákon č. 3726 „O soukromé detektivní činnosti" z 13. dubna 2017.

Zákon č. 4616-17 O bezpečnostních činnostech používá tyto pojmy:

Bezpečnostní činnosti – poskytování služeb na ochranu občanů a majetku.

Předmět ochrany – osoba a majetek.

Předmět bezpečnostní činnosti – podnikatelský subjekt jakéhokoli druhu vlastnictví, založený a registrovaný na území Ukrajiny, provádí bezpečnostní činnost na základě licence obdržené v souladu s předepsaným postupem.

Ochrana majetku – aktivity na přípravu a realizaci ochranných opatření zaměřených na zajištění integrity budov, území, vody, vozidel, peněz, cenných papírů a dalšího movitého a nemovitého majetku, k zabránění, nebo předcházení, nebo potlačení protiprávních činů proti němu.

Ochrana fyzických osob – aktivity na přípravu a realizaci ochranných opatření na ochranu osobní bezpečnosti, života a zdraví určité individuální fyzické osoby (skupiny osob), k předcházení a zabránění dopadu protiprávních činů.

Bezpečnostní pracovníci – zaměstnanci, kteří přímo vykonávají funkci ochrany majetku nebo jednotlivců podle své kvalifikační úrovně.

Specialista na organizaci činnosti ochrany – vedoucí předmětu činností zaměřených na zabezpečení, nebo jeho zástupce, vedoucí pobočky, nebo jeho zástupce, jehož povinnosti zahrnují organizaci a provádění opatření ochrany a kontrolu činnosti bezpečnostních pracovníků.

Režim přístupu – představuje režim vytvořený uvnitř chráněných objektů, který je zajištěn souborem organizačních, právních a technických opatření přijatých k vyloučení možnosti nekontrolovaného pohybu osob, vozidel a majetku do a z chráněného objektu.

Režim stanovený v rámci chráněných objektů – řídí se souborem opatření a vnitřními předpisy, jež jsou povinné pro všechny osoby, které se v nich nacházejí.

Zásahové vozidlo – je vozidlo ve vlastnictví bezpečnostního subjektu, které je určeno k zajištění bezprostřední reakce bezpečnostního personálu na protiprávní jednání s ohledem na předmět ochrany nebo na události a okolnosti, které způsobují nebo mohou způsobit škody na majetku nebo mohou ohrozit osobní bezpečnost občanů či bezpečnostního personálu v chráněných objektech.

Technické prostředky ochrany – technické prostředky používané při realizaci bezpečnostních činností (systémy, přístroje a zařízení pro zjišťování existence nebezpečí pro život osob nebo majetku – slouží pro upozornění a varování).

Pult centralizovaného dohledu – je středisko se zaměstnanci, kteří sledují stav zabezpečovacích systémů.

Typy bezpečnostních služeb

Předmětem bezpečnostní činnosti na základě licence obdržené v souladu se zavedeným postupem jsou tyto bezpečnostní služby: Ochrana majetku občanů, Ochrana majetku právnických osob, Ochrana jednotlivců.

Subjekt bezpečnostní činnosti je oprávněn:

- pro zabezpečení bezpečnostní činnosti nakupovat, skladovat a používat zvláštní prostředky, způsobem stanoveným právními předpisy, jejichž seznam určuje kabinet ministrů Ukrajiny;
- pro zajištění rádiové komunikace používat předepsaným způsobem rádiové frekvence;
- používat služební psy v bezpečnostních činnostech;
- používat technická zařízení pro bezpečnostní účely – např. zásahové vozidlo;
- obdržet písemný požadavek zákazníka na ochranu informací a kopie dokumentů nezbytných pro provedení ochranných opatření na předmětu ochrany;
- kontrolovat se souhlasem zákazníka nebo jeho zástupce území, budovy a prostory, které jsou chráněny.

Bezpečnostním pracovníkem může být způsobilý občan Ukrajiny, který dosáhl věku 18 let, absolvoval odpovídající odbornou přípravu nebo školení, uzavřel pracovní smlouvu s podnikem soukromé bezpečnosti a předložil doklady, že není registrován u zdravotních úřadů pro duševní nemoci, alkoholismus nebo drogovou závislost, nemá vykonané nebo pravomocné odsouzení za spáchání úmyslných trestných činů, nemá žádná omezení stanovená soudem, pokud jde o výkon jeho funkčních povinností, nemá zdravotní omezení pro plnění funkčních povinností a je evidován v místě bydliště způsobem předepsaným zákonem.

Zákon č. 3726 O soukromé detektivní činnosti používá následující pojmy:

Soukromý detektiv: fyzická osoba podnikatel, který provádí soukromou detektivní činnost na základě a způsobem předepsaným tímto zákonem.

Soukromá detektivní činnost: činnost, která je povolena národní policií Ukrajiny k podnikání jako soukromý detektiv nebo sdružení soukromých detektivů, poskytovat zákazníkům placené detektivní služby za účelem ochrany jejich oprávněných práv a zájmů na základě a způsobem stanoveným tímto zákonem.

Zákazník soukromých detektivních služeb: fyzická nebo právnická osoba, veřejný orgán, orgán místní samosprávy, v jehož zájmu se provádí soukromá detektivní činnost.

Momentka z doby karanténních opatření v Kyjevě. „Městská stráž" je de facto seskupením několika dobrovolnických skupin veteránů. I z tohoto důvodu je na nich možno vidět různé uniformy.

Zdroj: Що таке «Муніципальна варта» та які повноваження вона має під час карантину. Media Sapiens, 13. IV. 2020. https://1url.cz/iKp07

Sdružení soukromých detektivů: nezávislý subjekt, který prošel státní registrací způsobem stanoveným zákonem „O státní registraci právnických osob", jehož zřizovatelem jsou nejméně dva soukromí detektivové, kteří v době vzniku takového sdružení mají platná potvrzení o právu zapojit se do soukromé detektivní činnosti.

Střet zájmů: je rozpor mezi osobními zájmy soukromého detektiva a jeho profesními právy a povinnostmi, jejichž přítomnost může ovlivnit objektivitu nebo nestrannost soukromého detektiva, který vykonává své profesní povinnosti, nebo se dopustil nebo neplnil své činnosti během provádění soukromé detektivní činnosti.

Subjekty soukromé detektivní činnosti:

Podle výše zmíněného zákona je představují soukromí detektivové (Sdružení soukromých detektivů). Soukromé detektivní služby mohou poskytovat subjekty soukromé detektivní činnosti pouze v souladu s postupem a za podmínek stanovených tímto zákonem.

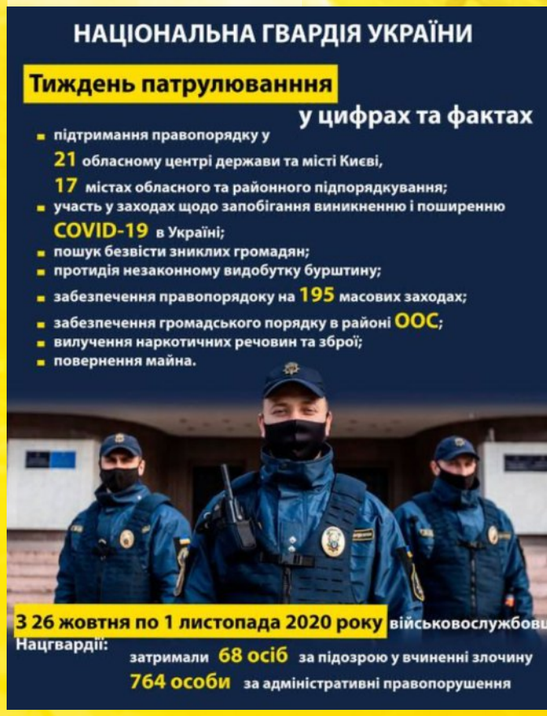
Soukromým detektivem může být občan Ukrajiny, který dosáhl věku 21 let, mluví úředním jazykem, má právnický titul a nejméně tři roky praxe v oblasti operativních služeb nebo orgánů předběžného šetření, případně absolvoval školení pro soukromé detektivy a obdržel osvědčení o právu vykonávat soukromou detektivní činnost v souladu se zákonem stanoveným postupem. Soukromý detektiv přitom nemůže být úředníkem nebo úředníkem orgánů veřejné moci, místní samosprávy, donucovacích nebo soudních orgánů.

Soukromým detektivem se nemůže stát osoba, která má nevykonané odsouzení nebo jejíž odsouzení nebylo zrušeno a nebylo odvoláno postupem stanoveným zákonem, stejně jako osoba, která je soudem zbavena způsobilosti k právním úkonům nebo je její způsobilost omezená, osoba registrovaná ve zdravotnických zařízeních v souvislosti s duševním onemocněním, alkoholismem nebo drogovou závislostí, osoba, která byla propuštěna z funkce soudce, státního zástupce, notáře, z orgánů činných v trestním řízení, ze státní správy nebo ze služeb v orgánech místní samosprávy za porušení přísahy či spáchání trestného činu korupce.

Soukromí detektivové a sdružení soukromých detektivů, kteří při výkonu čin-

Národní garda Ukrajiny propaguje výsledky nasazení gardistů za pomoci řeči čísel (registrované trestné činy, počty zadržených osob, počty zabavených zbraní, objem zajištěných omamných a psychotropních látek apod.).

Zdroj: Національна гвардія України. Facebook, 2. XI. 2020. https://www.facebook.com/NGUmainpage/posts/3590766704278547/



(2. ČÁST)

KPKB KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI

nosti zjistili skutečnosti o trestném činu nebo přípravě trestného činu, musí toto neprodleně oznámit příslušnému policejnímu orgánu a předat mu materiály potvrzující takové informace. Soukromým detektivům je zakázáno shromažďovat informace týkající se osobního života, politického a náboženského přesvědčení jednotlivců.

Ministerstvo spravedlnosti Ukrajiny vydává potvrzení o právu vykonávat soukromou detektivní činnost a Národní policie vede evidenci subjektů soukromé detektivní činnosti. Licence pro poskytování soukromých bezpečnostních služeb se provádí způsobem předepsaným ve vyhlášce kabinetu ministrů Ukrajiny č. 960 „O schválení licenčních podmínek pro provádění bezpečnostních činností" z 18. listopadu 2015.

K žádosti o vydání licence pro poskytování soukromých bezpečnostních služeb musí být přiloženy:

1. Kopie dokladů potvrzujících splnění požadavků na kvalifikaci – žadatel musí mít buď vysokoškolské vzdělání, anebo pracovní zkušenosti v délce alespoň tří let jako důstojník v operativním nebo vyšetřovacím oddělení ministerstva vnitra nebo v policejním útvaru nebo ve státní bezpečnostní službě, anebo praxi v délce nejméně tří let ve velitelské funkci vojenské jednotky nebo ve vzdělávacích institucích ozbrojených sil nebo na pozicích středních a vyšších vedoucích pracovníků orgánů činných v trestním řízení.

2. Pracovník, který je odpovědný za řízení bezpečnostní služby, musí mít vysokoškolské právní vzdělání, nebo nejméně tříletou pracovní zkušenost ve vedoucích pozicích v bezpečnostních službách, nebo alespoň tři roky praxe ve vedoucích pozicích orgánů činných v trestním řízení.

3. Kopii dokladů potvrzujících, že osoba absolvovala povinné předběžné, nebo pravidelné psychiatrické vyšetření a preventivní neurologické vyšetření.

4. Kopii dokladu potvrzujícího neexistenci omezení zdravotního stavu osoby pro výkon funkčních povinností vydaných v souladu se zavedeným postupem.

5. Kopii pasu občana Ukrajiny.

6. Kopii pracovní smlouvy nebo kopii výpisu z pracovního záznamu osoby certifikované podnikatelským subjektem.

(2. ČÁST)

Národní policie Ukrajiny vede jednotnou evidenci soukromé detektivní činnosti za účelem shromažďování, ukládání, zaznamenávání a poskytování přesných informací o počtu soukromých detektivů a jejich personálu.

V současné době (2019) je na Ukrajině oficiálně zaregistrováno 4 750 bezpečnostních firem, ve kterých pracuje více než 50 000 lidí a asi 2 000 soukromých detektivů a detektivních agentur, což je dvacetkrát více než v roce 2013. V Kyjevě je více než sto detektivních agentur.

Použití fyzické síly a speciálních prostředků je možné v případech:

- kdy jiná opatření nevedla k ukončení protiprávního jednání;
- kdy osoba chrání sebe nebo jinou osobu před útokem, který ohrožuje jejich život a zdraví nebo majetek;
- kdy je potřeba zadržet pachatele, který nezákonně pronikl do chráněného objektu nebo spáchal jiné protiprávní činy a klade odpor;
- kdy je potřeba zneškodnit zvíře, které ohrožuje život a zdraví bezpečnostního personálu nebo jiných osob.

Před použitím fyzické síly a speciálních prostředků je povinnost varovat osobu, proti které mají být tyto prostředky použity. Bez varování mohou být tyto prostředky použity pouze v případě náhlého útoku, útoku nebo odporu s použitím zbraní nebo předmětů, které ohrožují život a zdraví člověka nebo s použitím motorových vozidel.

Je zakázáno používat fyzickou sílu a speciální prostředky proti ženám se zřejmými příznaky těhotenství, proti osobám v pokročilém věku nebo s těžkými příznaky postižení, proti osobám nezletilým, jakož i proti osobám, které jsou v souladu s právními předpisy držiteli zvláštního statutu imunity, ovšem s výjimkou případů jejich útoku, který představuje ohrožení života a zdraví jednotlivců, bezpečnostního personálu nebo ozbrojeného útoku nebo ozbrojeného odporu.

Soukromá bezpečnostní služba má právo použít v průběhu a na místě provádění ochranných opatření služební psy. Mohou být používáni jen služební psi, kteří prošli výcvikovým kurzem uznaným pro způsobilé úřední použití služebních psů a mají veterinární pas pro identifikaci.

Služební psi mohou být použiti, aby zabránili vniknutí do chráněných objektů, nebo při pokusech o vniknutí do chráněných objektů. Služební psi mohou být použiti proti osobám, které se neoprávněně zdržují v chráněných lokalitách.

Speciálními prostředky jsou ochranné přilby, obranné spreje a plynové pistole s náboji 6, 8 a 9 mm, traumatické zbraně, gumové obušky, plastová pouta a elektrické paralyzéry. Z vyjmenovaných speciálních prostředků mohou soukromí detektivové používat traumatické zbraně a plynové pistole.

Soukromí detektivové mohou shromažďovat a zaznamenávat informace, které budou nadále používat v občanských, obchodních, správních a trestních řízeních. Tyto informace dávají další příležitost občanům při ochraně jejich práv a osobních zájmů u soudu. Informace získané činností soukromých detektivů jsou podle zákona profesionálním tajemstvím a neměla by být zveřejněny. Pokud jsou při činnosti soukromých detektivů získány informace nebo důkazy o přípravě nebo pokusu o spáchání trestného činu, informují soukromí detektivové o těchto skutečnostech orgány činné v trestním řízení.

doc. Mgr. Oldřich Krulík, Ph.D.
plk. Martin Bohman, Ph.D.
Mgr. Radek Pospíšil
odbor centrální analytiky Úřadu služby kriminální policie a vyšetřování,
Vysoká škola AMBIS; Mezinárodní bezpečnostní institut,
Policejní akademie České republiky v Praze

Použité zdroje:

- HOLDSWORTH, N. Next Revolutionary Step in Ukraine: Reform the Police. Christian Science Monitor, 28. II. 2014. https://1url.cz/jKT3c
- KRÉDL, Jaromír. Obecní policie ve vybraných zemích postsovětského prostoru. Ochrana a Bezpečnost, 2016, č. 2. http://www.ochab.ezin.cz/O-a-B_2016_B/2016_OaB_B_01_kredl.pdf
- MyPol System. Facebook. https://www.facebook.com/mypolsystem/
- POSPÍŠIL, Roman. Soukromé bezpečnostní služby v postsovětském prostoru. Ochrana a Bezpečnost, 2019, č. 1. http://ochab.ezin.cz/O-a-B_2019_A/2019_OaB_A_02_pospisil.pdf
- State Statistics Service of Ukraine. https://ukrstat.org/en
- Адміністративно-територіальний устрій України. Державний картографо-геодезичний фонд України; Укркартгеофонд. https://kgf.com.ua/
- Військовослужбовці Нацгвардії виходять на самостійне патрулювання вулиць. Права та обов'язки. Телевізійна служба новин, 1. VIII. 2019. https://1url.cz/BKT39
- ГОНЧАРОВА, К. Що таке Муніципальна варта та які повноваження вона має під час карантину. Media Sapiens, 13. IV. 2020. https://1url.cz/iKp07
- Департамент патрульної поліції. http://patrol.police.gov.ua/
- Закон України Про охоронну діяльність No4616-17. Верховна Рада України. http://zakon2.rada.gov.ua/laws/show/4616-17?test=4/ UMfPEGznhhAIj.ZiwJEnQTHI4Z.s80msh8le6
- Закон України Про приватну детективну (розшукову) діяльність No3726. Liga zakon. http://search.ligazakon.ua/l_doc2.nsf/link1/JH2VI00V.html
- Кабінет міністрів України постанова від 18 листопада 2015 р. №960. Київ Про затвердження Ліцензійних умов провадження охоронної діяльності. Верховна Рада України. http://zakon2.rada.gov.ua/laws/show/960-2015-%D0%BF#n99
- Міністерство внутрішніх справ України. In: http://www.mvs.gov.ua/
- Муніципальна варта Києва демонструє реальні результати. Київська міська рада, 20. III. 2018. [cit. 6. VI. 2021] https://1url.cz/wKTTH
- Національна Гвардія України. [cit. 30. VIII. 2021] https://ngu.gov.ua/
- Один день з патрулями Нацгвардії в курортному селищі Приморське. Національна гвардія України, 3. VIII. 2021. https://1url.cz/2KGPo
- Патрульна поліція Миколаєва. https://vk.com/niko_police
- Поліція Києва. Youtube. https://www.youtube.com/user/militiakiev
- Проект Закону про муніципальну варту. Верховна Рада України. https://1url.cz/IKT38

OPTONET COMMUNICATION

DATOVÉ CENTRUM VYSOČINA

Společnost OptoNet Communication poskytuje svým klientům služby už téměř dvě desítky let. V současné době prochází významnou modernizací IT technologií a uvádí do provozu monumentální areál Datové Centrum Vysočina. Při této příležitosti požádala naše redakce o krátký rozhovor ředitele společnosti Rostislava Proseckého.

Na čem v této složité době pracujete a co připravujete pro své obchodní partnery?

Žijeme opravdu v dynamické době, která klade velké nároky na každého jednotlivce i na celý společenský systém. Společnost OptoNet Communication, spol. s r.o., která je součástí „OPTOKON Group", se v rámci telekomunikačních služeb zabývá i provozováním služeb datového centra. Tuto službu nabízíme od roku 2003, kdy jsme uvedli do provozu vlastní optickou infrastrukturu v kraji Vysočina a Jihomoravském kraji. V současné době uvádíme do provozu moderní areál s nejmodernějšími IT a NON-IT technologiemi zaměřené na komplexní bezpečnost dat a procesů – Datové Centrum Vysočina.

Toto centrum bude provozováno dle těch nejpřísnějších mezinárodních standardů pro datová centra, a to v souladu se standardem úrovně TIER IV, s dostupností služeb 99,995 %. Datové Centrum Vysočina bude nabízet komplexní služby v oblasti provozní, kybernetické a s tím související fyzické bezpečnosti. Služby budou provozovány ve spolupráci s předními společnostmi a odborníky z oblasti bezpečnosti, zároveň připravujeme certifikaci dle ISO 27001 management bezpečnosti informací.

V rámci budovaného zařízení je pro Datové Centrum Vysočina navržena tzv. „souběžná správa", což znamená, že údržbu všech částí datového centra lze vykonávat bez výpadku jakýchkoli poskytovaných služeb při plné a maximální funkčnosti po celou dobu údržby.

Hovoříte o Datovém Centru Vysočina, prozraďte nám, kde ho můžeme najít?

Datové centrum Vysočina si zaslouží obdiv nejen pro svou monumentálnost a architektonický ráz, ale bude také ojedinělým projektem v České republice. Je vybudované na strategickém bodu, kudy procházejí hlavní optické trasy společnosti Telia – „Viking Network" a „PAN – European Network". Navíc se Datové centrum Vysočina nachází přímo na hlavní páteřní síti „BackBone" České republiky a je v těsné blízkosti dálnice D1.

Vlastní optická síť zajišťující konektivitu Datového Centra Vysočina je tvořena soustavou dvaceti sedmi HDPE chráničkových tras, které propojují kromě Prahy a hraničního přechodu Hatě do Rakouska i všechna klíčová města Kraje Vysočina v rámci sítě ROWANET.

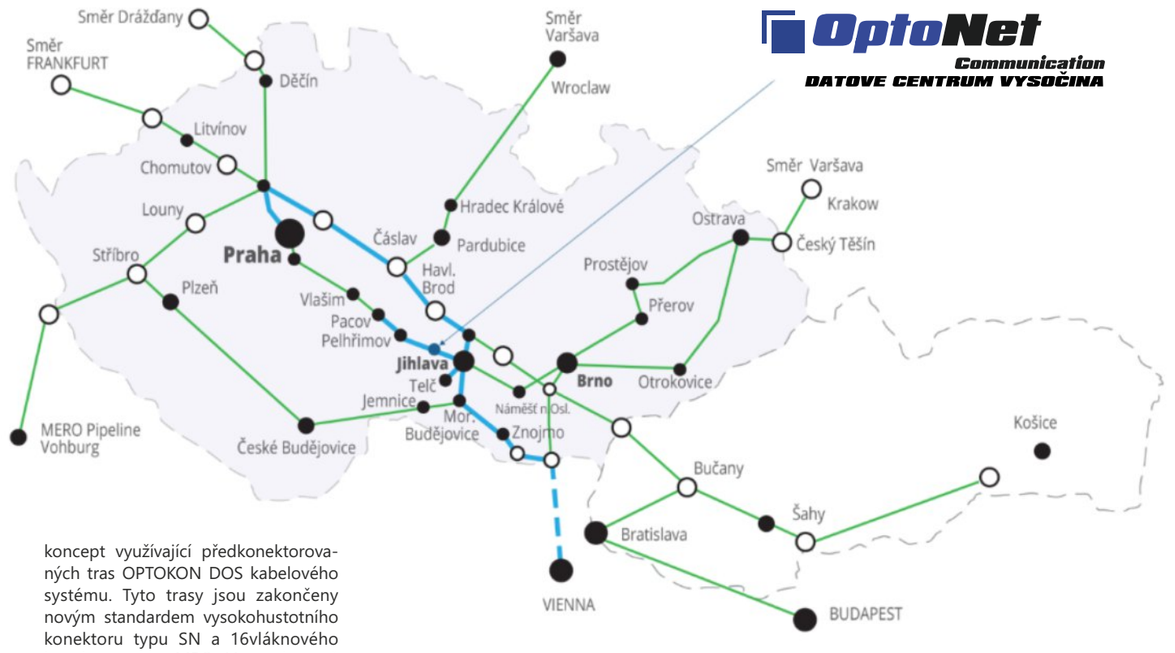
Můžete uvést základní technické parametry objektu datového centra?

Datové Centrum Vysočina je mimo jiné unikátní svojí vysokou energetickou efektivitou. V první etapě výstavby je vybudována zatím jen polovina finální velikosti centra, která je rozdělena do dvou samostatných technologických místností. Současné sály mají celkovou plochu 226 m² se světlou výškou 3,50 m. Jejich mikroklima bude realizováno v souladu se standardy vyžadovanými pro budování nejmodernějších datových center nejen u nás, ale i ve světě.

Objekt Datového Centra Vysočina je vybaven vlastní trafostanicí 22/0,4 kV, 50 Hz, vybavenou dvěma transformátory a napojenou na kruhovou topologii vysokého napětí ze dvou nezávislých zdrojů a tří záložních motorgenerátorů MG s plně autonomním provozem po dobu nejméně 96 hodin provozu bez doplnění paliva. Plánované energetické zatížení objektu je 825 kW.

Jaké technické novinky nabídnete ve Vašem datovém centru?

Základním prvkem vnitřní optické strukturované kabeláže vyráběné společností OPTOKON, a.s., ve spolupráci s japonskou firmou SENKO je unikátní



koncept využívající předkonektorovaných tras OPTOKON DOS kabelového systému. Tyto trasy jsou zakončeny novým standardem vysokohustotního konektoru typu SN a 16vláknového konektoru typu MPO. V první etapě výstavby je tak možno v připravených dvou sálech zakončit celkem více než 9 600 optických vláken, projektovaná kapacita při dokončení celého projektu je však více než dvojnásobná.

Výhodou použití tohoto konceptu kabeláže je velmi vysoká hustota propojení, 100% garantovaná funkčnost optických propojení a jednoduchá překonfigurovatelnost dle zákaznických potřeb.

Jaké služby Datové Centrum Vysočina nabízí a pro koho?

Datové Centrum Vysočina je aliančně zaměřené, snažíme se maximálně naplnit individuální požadavky obchodních partnerů – architekturu našich služeb lze pojmenovat takto:

- speciální zabezpečené služby (aplikace pro ekonomickou a procesní správu),
- speciální zabezpečené technologie (HW a SW pro speciální vývoj aplikací a služeb, využívající např. umělou inteligenci),
- zabezpečené komunikační a multimediální služby (systémy pro sdílení dokumentů, konferenční a videokonferenční služby, včetně šifrované komunikace),
- bezpečnostní služby operačního centra (systémy kybernetické a provozní bezpečnosti zákazníků).
-

Soubor služeb je komplexní z pohledu požadavků na moderní IT, je popsán v katalogu Služeb Datového Centra Vysočina, včetně procesních návazností na straně zákazníka i datového centra:

- Privátní DC
- Privátní cloud
- Virtuální DC
- Virtuální cloud
- Virtuální IT
- RACK/ server housing
- Bezpečnostní monitoring
- Služby SOC
- Služba migrace dat
- Služby Školicího centra OptoNet
- Služby Tréninkového centra IT

Téma služeb je velmi široké, vydalo by na samostatnou kapitolu.

Víme, že se věnujete vývoji a výzkumu v oblasti bezpečnosti. Jaké novinky přinášíte do nově budovaného Datového Centra Vysočina?

Především jde o systém OSMS (OptoNet Secure Monitoring System), který umožňuje zajistit lokální i vzdálenou bezpečnost NOT IT i IT technologií, včetně kybernetických hrozeb a útoků. Tento monitoring všech provozních stavů i veškerých podpůrných technologií využívá také unikátní technologii vyvinutou ve spolupráci firem OPTOKON & SAMM Teknoloji – systém ochrany perimetru pomocí optického vlákna – FOTAS. Tento systém tzv. neviditelného optického plotu pracuje jako kontinuální vibrační a akustický senzor, který dokáže identifikovat během několika sekund alarmový stav do vzdálenosti až 160 km.

Systém OSMS aktivně využívá vícevrstvého systému elektronického vstupového systému EVS s využitím biometrických prvků, prováženého systémem poplachového tísňového zabezpečovacího systému PTZS a CCTV pro monitoring vnějšího perimetru Datového Centra Vysočina i datových sálů s dobou archivace záznamu minimálně 30 dní.

Čím ještě je Vaše firma zajímavá pro zákazníky a odbornou veřejnost?

Společnost OptoNet Communication, spol. s r.o., věnuje velkou pozornost profesionálnímu vzdělávání v oblasti elektronických komunikací s důrazem na kybernetickou bezpečnost. Tento fakt je i důvodem a hnacím motorem zprovoznění Školicího centra OptoNet zaměřeného na poskytování systému vzdělávání pro odbornou veřejnost z IT oborů.

V rámci Školicího centra OptoNet připravujeme, ve spolupráci s partnery, zprovoznění Tréninkového centra IT. Tréninkové centrum bude pomáhat k trénování reakce na incidenty. Reakcí na vlastní trénink může být například úprava školicích programů, či změna nastavení interních procesů uživatele nebo dodavatele.

Velký důraz klademe na spolupráci odborných sdružení a firem z oblasti obranného a bezpečnostního průmyslu, včetně spolupráce s akademickou obcí v kraji Vysočina i v celé České republice.

Děkujeme za rozhovor.
Redakce BsP