Speciál 2022

ŽIVOT ZA OKNY

Václav Kučera: Spolupráce inovativních přístupů a zákona

Umělá inteligence v prevenci kriminality

Hackerské útoky: Nevyhnutelnost nebo jen důsledek zanedbání?

Co je to zločin? Jakou roli hraje svědek?

Tepelná čerpadla

Až 4x účinnější tradiční formy vytápění

Tepelná čerpadla jsou vhodná jak do domácností a firem ale i do průmyslu. Mají velmi tichý chod a nízký dopad na životní prostředí. Oproti konkurenčním konceptům vytápění je větší počáteční investice, tato je ale vyvážena prakticky nulovou obsluhou a velmi nízkými provozními náklady.

Tepelná čerpadla vzduch/voda

- Pro vytápění a ohřev teplé vody, volitelně také chlazení
- Využívá 75 % tepelné energie ze vzduchu a pouze 25 % elektrické energie
- Volitelná solární podpora
- Pracují při venkovních teplotách až do -22 °C
- Vysoká teplota výstupní vody až +65 °C

Tepelná čerpadla země/voda

- Získávají energii ze země
- Využívá 80 % geotermální energie a 20 % elektrické energie
- Nejsou závislá na okolní teplotě vzduchu
- Vyšší pořizovací náklady

Tepelná čerpadla vzduch/vzduch

- Využívají 80 % energie odebrané ze vzduchu a 20 % elektrické energie.
- Jsou vybaveny technologii invertoru
- Rychlý způsob vytápění i v přechodném období
- Nejnižší pořizovací cena v porovnání s ostatními typy tepelných čerpadel
- Velmi rychlá instalace

V naší nabídce najdete tepelná čerpadla vzduch-vzduch, vzduch-voda a země-voda.
Kontaktovat nás můžete přes webové stránky **https://abclima.cz/cs/**
nebo přes telefon na čísle: **800 022 830**.

Vážené dámy, vážení pánové,

otázka bezpečnosti a s ní související oblast prevence kriminality patří v dnešní době mezi ožehavá a často diskutovaná témata.

Moderní prostory Magenta Experience Center v pražském obchodním centru Arkády Pankrác se staly dějištěm Kulatého stolu na téma Využití umělé inteligence v oblasti prevence kriminality. Organizátorem a pořadatelem akce, která proběhla pod záštitou brigádního generála JUDr. Václava Kučery, ředitele Krajského ředitelství policie Středočeského kraje, se stal náš časopis Život za okny. Kulatého stolu se zúčastnili starostové a vedoucí sekcí bezpečnosti, inovací a IT měst a obcí Středočeského kraje a se zajímavými přednáškami na něm vystoupili zástupci Policie ČR, Ministerstva vnitra, Krajského úřadu Středočeského kraje a specialisté na kybernetickou bezpečnost a umělou inteligenci.

V tomto speciálním vydání najdete reportáž z akce a můžete si přečíst rozhovory se všemi přednášejícími.

Patří mezi ně nejpovolanější osoby a odborníci, kteří se dané problematice dlouhodobě věnují:

1) O prevenci kriminality z pohledu Policie ČR a významu využití softwarů a umělé inteligence v úvodu pohovoří Brig. gen. JUDr. Václav Kučera, PhD., MBA – ředitel Krajského ředitelství policie Středočeského kraje

2) S dotačním programem Ministerstva vnitra na pořízení technologií pro prevenci kriminality účastníky setkání vás seznámí JUDr. Michal Barbořík – ředitel odboru prevence kriminality Ministerstva vnitra České republiky

3) O aktuálních aktivitách Středočeského kraje v oblasti prevence kriminality včetně bezpečnostní infomační platformy Bezpečný Středočeský kraj se dočtete v rozhovoru s Mgr. Filipem Gundzou – vedoucím oddělení prevence kriminality Krajského úřadu Středočeského kraje

4 Konkrétní ukázku využití umělé inteligence v oblasti prevence kriminality představí na konkrétním příkladu - severočeského města Bílina Pavel Kuka, Idea a Project Manager ve společnosti Gatum Group a Jan Čulík, Project Manager ve společnosti Innovis

5) S možnostmi ochrany infrastruktury veřejné správy před kybernetickými útoky vás seznámí Ing. Pavel Meletzký, MBA – IT specialista na kybernetickou bezpečnost

6) Ing. Kateřina Kulíšková – Business Development Manager ve společnosti Innovis představí elektronickou recepční, moderní řešení pro administraci vstupů do budovy.

REDAKCE

ŽIVOT ZA OKNY: Vychází 4x ročně | Ročník IV., 3/2022 | Toto číslo vyšlo 30. 12. 2022
VYDÁVÁ: MODERN LIVING s.r.o., Fakultní 2652, 250 01 Brandýs nad Labem-Stará Boleslav, Česká republika, IČO: 086 42 729
JEDNATEL: Ing. Lucie Doležalová, mail: l.dolezalova@zivotzaokny.eu
REDAKCE: Yeva Bartkiv | redakce@zivotzaokny.eu
GRAFICKÁ ÚPRAVA: Život za okny

TISK: fronte s.r.o.
DISTRIBUCE: ADLEX, spol. s r.o.
INZERCE: marketing@zivotzaokny.eu
WEBOVÉ STRÁNKY: www.zivotzaokny.eu
MK ČR E 23804

Finanční podpora projektů spojených s implementací umělé inteligence za účelem prevence kriminality

JUDr. Michal Barbořík
ředitel odboru prevence kriminality Ministerstva vnitra ČR

Vystudoval práva na Univerzitě Karlově v Praze a již 20 let se věnuje problematice trestního práva, bezpečnosti a prevence kriminality. V rámci Předsednictví ČR v Radě EU byl rovněž předsedou Evropské sítě pro prevenci kriminality (EUCPN). Rovněž řídí Poradní sbor Ministerstva vnitra pro situační prevenci kriminality a Republikový výbor pro prevenci kriminality. Je autorem odborných článků a rozhovorů v problematice prevence kriminality, vystupuje rovněž v médiích. Působil a působí jako odborný gestor či ředitel několika úspěšných projektů v oblasti prevence kriminality (Asistent prevence kriminality, Domovník-preventista, Mapy budoucnosti ad.).

Každé město si zaslouží to nejlepší technologické vybavení, které mu následně umožní v mnoha aspektech lepší fungování. Není však překvapením, že zavedení takových inovativních řešení předpokládá značné náklady. Dnes naštěstí existují speciální dotační programy, které města podporují a umožňují jejich pokrok. O jedné z takových možností jsme hovořili s JUDr. Michalem Barboříkem, ředitelem odboru prevence kriminality na Ministerstvu vnitra České republiky.

Můžete definovat klíčové podmínky, jež mají být splněny žadatelem o dotaci?
Klíčové podmínky Programu prevence kriminality na místní úrovni (určený pro kraje, obce a DSO) je možné rozdělit do tří kategorií – věcné, institucionální a formální.
1) K věcným patří zejména soulad s aktuálně platnou Strategií prevence kriminality v ČR, soulad s nastavenými parametry (podporovanými typy) investičních projektů apod.
2) Institucionální podmínky obsahují zejména povinnost
a) pověřit pracovníka zodpovědného za prevenci kriminality (manažera prevence kriminality),
b) vytvořit odborný, multioborový orgán (pracovní skupina / komise manažera prevence kriminality, příp. komise, které je manažer prevence kriminality členem), který se prevencí kriminality zabývá, c) zpracovat svůj vlastní víceletý (min. dvouletý) strategický dokument zaměřený na bezpečnost dle metodic-

kých doporučení, schválený radou nebo zastupitelstvem kraje, obce či řídícím orgánem DSO, d) zpracovat aktuální bezpečnostní analýzu min. za předchozí rok s komentářem k vývoji při porovnání z předchozích let, opět dle metodických doporučení.
Konečně 3) formální podmínky obsahují pravidla jako: žádost musí být podána elektronicky prostřednictvím webového formuláře ve webové aplikaci https://isprofin.mfcr.cz/rispf pro každý projekt zvlášť a odeslána do datové schránky Ministerstva vnitra (6bnaawp) ve Výzvou stanoveném termínu, musí obsahovat strukturovaný popis projektu dle struktury přílohy Zásad, musí být uvedena minimálně 2 kritéria hodnocení efektivity, musí obsahovat povinné přílohy, dodržet min. spoluúčast dle typu projektu, žadatel musí provést jako příjemce dotace s poskytovatelem vypořádání v rámci finančního vypořádání vztahů se státním rozpočtem za minulé období, u investičních projektů též provést závěrečné vyhodnocení akce.
To je ale jen částečný výčet, všechny podmínky a podrobnosti k nim jsou vždy uvedeny v příslušné Výzvě na daný rok a k ní vydaných Zásadách, které zveřejňuje zpravidla v prosinci roku předcházejícího tomu roku, na který jsou dotace poskytovány.

Jak rozlišujete projekty investičního a neinvestičního charakteru?
Investičními projekty se rozumí akce na pořízení, obnovu nebo technické zhodnocení hmotného a nehmotného dlouhodobého majetku, s výjimkou drobného hmotného a nehmotného dlouhodobého majetku dle podmínek daných zákonem č. 218/2000 Sb., vyhláškou č. 560/2006 Sb., o účasti státního rozpočtu na financování programů reprodukce majetku, v rozsahu:
a) kamerové systémy (včetně mobilních a rozšíření stávajících),
b) zabezpečovací soubory,
c) vyhodnocovací soubory,
d) mříže,
e) osvětlení rizikových míst,
f) oplocení rizikových míst,
g) software pro bezpečnostní a preventivní účely,
h) hardware pro bezpečnostní a preventivní účely,
i) sportovní hřiště a plácky.
Projekty, které nelze podřadit pod předchozí větu, jsou projekty neinvestiční.

Pokud se na vás obrátí jednotlivý kraj nebo obec, a přitom jsou již financovány z jiných zdrojů, mohou i tak počítat s potenciální dotací?
Obce a kraje jsou financovány z různých zdrojů, to samo o sobě přiznání dotace nevylučuje.
V předkládaném projektu nesmí být požadováno dofinancování aktivit žadatele financovaných z ESF a IPRM. Na výši minimální spoluúčasti žadatele (ta se může dle typu projektu lišit, zpravidla je 10 %, ale může být i vyšší, ale i nulová) se ale nesmí podílet další subjekty. Projekt může být spolufinancován nad rámec povinné minimální spoluúčasti i z dalších zdrojů, jejichž příjemcem ale musí být žadatel. Duplicitní úhrada stejných nákladů na projekt z různých zdrojů včetně zdrojů ze státního rozpočtu není dovolena.

Jaké byly nejčastější vady v žádostech, jež se podávaly v minulých letech? Na co by si měli žadatelé o dotaci dát při vyplnění žádosti pozor?
Než bylo v r. 2018 zavedeno elektronické podávání žádostí, byly formální chyby velmi časté (chybějící povinné přílohy, požadavky na neuznatelné výdaje či aktivity apod.). V rámci podávání žádostí prostřednictvím webové aplikace a zasláním vygenerovaného formuláře žádosti do datové schránky MV je tak nejčastější to, že žádost není zaslána do datové schránky MV (je pouze vyplněna ve webové aplikaci), případně je do datové schránky zaslána po datu pro podávání žádostí). Další formální chybou bývá nedodržení povinné spoluúčasti žadatele. Nicméně v rámci elektronického podávání žádostí se uvedené příklady vyskytují pouze ojediněle (2-3 žádosti z celkových cca 200 podávaných žádostí).
Z věcného hlediska se pak jedná o nedostatečný popis odůvodnění potřebnosti realizace daného projektu, či potřebnosti projektu v dané lokalitě (není podloženo nebo v souladu s předloženou bezpečnostní analýzou).
Žadatelé si musí hlídat a mít na paměti, že je třeba respektovat priority Strategie PK, dodat požadované povinné přílohy a zejména podat žádost v požadovaném termínu.
Z věcného hlediska pak dostatečně odůvodnit potřebnost daného projektu či jeho aktivit (soulad s bezpečnostní analýzou a jejími statistikami – např. pokud v obci dochází k velkému počtu krádeží jízdních kol, těžko bude na komisi akceptovatelný projekt vzdělávání seniorů na téma tzv. „šmejdů" apod.).

Jakým žádostem dává hodnotící komise přednost před tím, než je předá do rukou ministra vnitra?
Komise Republikového výboru pro prevenci kriminality hodnotí projekty podle předem stanovené bodové tabulky, ve které se také hodně odráží hodnocení projektů provedené v 1. kole krajskou odbornou komisí. Mezi další kritéria patří kvalita zpracování bezpečnostní analýzy, jak projekt reaguje na problém zjištěný takovou analýzou, zda je projekt nový, inovativní, komplexní. Konečné bodové hodnocení ovlivňuje rovněž index kriminality a index rizikovosti žadatele.
Komise oceňuje propracovanost projektů a jejich věcné odůvodnění, kde je vidět, že se daný žadatel problematikou zabývá (odráží se to v bezpečnostní analýze), vytváří komplex opatření a aktivit, které na danou situaci reagují a na něž pak zpracovává projekty a předkládá je (a to nejen do PPK MV). Kladné rovněž je, pokud žadatel deklaruje svou prioritu pro projekt také vyšší spoluúčastí nebo ochotou projekt financovat, i kdyby jej Komise např. kvůli nedostatku financí v dotacích nemohla podpořit. Naopak prohlášení typu, že když nebude dotace, nebude projekt, příliš nevypovídají o prioritě projektu pro obec a v hodnocení tak rozhodně nepomáhají. ■

Článek by zpracován i za přispění Mgr. Adolfa Poláka z odboru prevence kriminality MV ČR.

Město Benešov* kompletně na optice

Středočeský Benešov je jedním z prvních českých měst s připojením k internetu přes nově vybudovanou optickou síť.

Z centra až k okrajům města

Více než 16 tisíc obyvatel středočeského Benešova se ještě donedávna připojovalo k internetu prostřednictvím telefonních rozvodů, mobilní sítě nebo přes různé lokální bezdrátové sítě. Během posledních tří let ale prošla síťová infrastruktura Benešova obrovskou modernizací a město se stalo jedním z prvních v rámci ČR, které nabídne kterékoli domácnosti nebo firmě internetové připojení prostřednictvím optického kabelu, zavedeného až do budovy či bytu. Kompletně novou infrastrukturu pro nejrychlejší a nejspolehlivější připojení k internetu buduje v Benešově společnost T-Mobile.

Se zaváděním optické sítě začal T-Mobile ve vnitřním centru města, postupně se ale díky vstřícnosti vedení města podařilo rozšířit projekt na celý Benešov. „*Návrh T-Mobilu na vybudování optické sítě po celém městě se nám velmi zamlouval, protože usilujeme o to, aby byl Benešov moderním a přívětivým městem pro obyvatele i firmy – a dostupnost kvalitního připojení k internetu tomu jistě napomůže,*“ říká Ing. Roman Tichovský, místostarosta Benešova.

Bez zatížení městského rozpočtu

Většina optických kabelů je vedena v zeleni nebo případně v chodnících, které byly po provedení výkopových prací kvalitně předlážděny. Postup budování nové optické infrastruktury se také podařilo do značné míry sladit s plány radnice na rekonstrukce komunikací a chodníků ve městě. Ve výkopech byla navíc položena i nová, oddělená síťová infrastruktura na propojení budov v majetku města, ve kterých sídlí úřady a další veřejné organizace, stejně jako rozvody pro kamerový systém. „*Každé omezení kvůli výkopovým pracím samozřejmě obyvatele obtěžuje. Spolupráce s T-Mobilem pro nás ale znamenala i uspíšení rekonstrukcí některých silnic a chodníků, na které by jinak došlo třeba až za několik let,*“ pochvaluje si benešovský místostarosta Tichovský.

Budování moderní síťové infrastruktury společností T-Mobile neznamenalo pro městský rozpočet žádné další investice. T-Mobile navíc ve svých plánech od začátku počítal i s připojováním rodinných domů na optické rozvody. Těch je dnes už bezmála 400 a další budou připojovány v budoucnu. Přípojky jednotlivých domů jsou pro jejich majitele zřizovány zdarma – na náklady společnosti T-Mobile.

„Po našich zkušenostech bych určitě i dalším městům doporučil, aby se bez obav do podobného projektu pustili.“

Ing. Roman Tichovský, místostarosta Benešova

Optická infrastruktura v Benešově

Projektování a získání povolení	2 roky
Zahájení výstavby	2019
Délka optických kabelů	80 km ≈ 2 000 km optických vláken
Vybudováno přípojek	5 287
Další fáze	2023–2025
Plánováno přípojek ve druhé fázi	1 650

Přínos pro obyvatele i celé město

- ☑ Nejrychlejší a nejspolehlivější způsob připojení k internetu pro obyvatele, firmy i úřady
- ☑ Nejmodernější technologie, připravená na desítky let do budoucna
- ☑ Podpora zavádění technologií pro inteligentní města – smart cities

Hackerské útoky: Nevyhnutelnost nebo jen důsledek zanedbání?

Ing. Pavel Meletzký, MBA
Specialista na kybernetickou bezpečnost, s 30 letou praxí v informačních a komunikačních technologiích, posledních 10 let se zaměřením na kybernetickou bezpečnost a služby bezpečnostního dohledového centra.

V letech 2018 až 2022 předseda komise informatiky rady Statutárního města Opavy.

Jsme součástí neustále se digitalizujícího světa. I přes nespočet výhod, jež nám nabízí, je nadále aktuální i to, že každá mince má odvrácenou stranu. V rozhovoru s Ing. Pavlem Meletzkým, IT specialistou, budeme rozebírat téma kybernetických útoků, kterých je v dnešní době čím dál tím víc. Podrobněji se seznámíte s druhy hackerských útoků a o možnostech, jak jim čelit.

Můžete nám v kostce svou činnost a servis představit?
Téměř 30 let se pohybuji v oblasti informačních a komunikačních technologií a posledních 10 let se zaměřuji na kybernetickou bezpečnost. Přesněji řečeno řešení kybernetické bezpečnosti formou služby s využitím profesionálního bezpečnostního centra, se kterým se dnes setkáte většinou pod názvem SOC. Jednoduše lze říci, že stejně, jako strážní služba zajišťuje vstup do podniku, hlídá celý areál, reaguje na incidenty a hrozby, SOC obdobným způsobem nepřetržitě hlídá informační a komunikační systémy a technologie zákazníka a zajišťuje kybernetickou bezpečnost. A nejen to, tím, že společně se zákazníkem díky našim odborným znalostem a zkušenostem neustále systémy odladňujeme, výrazně snižujeme možnost úspěšného kybernetického útoku.

Jaké jsou běžné příznaky kybernetického útoku?
Přesně v tom je problém. Kybernetický útok nemusí být, a mnohdy není, pro mnoho organizací na první pohled patrný. A když se jej podaří odhalit, bývá již mnohdy pozdě. Nejhorší scénář je, že ráno v práci nezapnete počítač a všechna vaše data jsou zašifrována. Pak už těch možností moc nezbývá. Principem služby je nacházet všechny anomálie, které se v systému objeví a důsledně je prověřovat, zda se jedná o možné bezpečnostní riziko, nebo se jedná např. o provozní problém či lidskou chybu.

Jak často je vyžadována diagnostika serverů?
Pro nás je velmi důležité mít přehled o tom, jak pracují servery v rámci infrastruktury. Proto je vhodné a doporučujeme využívat minimálně nástroj na provozní monitoring pro aktuální informace o stavu serverů či služeb. Také je vhodné mít přehled o nových aktualizacích či dostupných bezpečnostních záplatách po objevení nové zranitelnosti. Samozřejmě přehled nestačí a je nutné aktualizace a záplaty neprodleně aplikovat. I s těmito činnostmi může

„Svět je nebezpečné místo k životu, ne kvůli lidem, kteří jsou zlí, ale kvůli lidem, kteří s tím nic neudělají.“– Albert Einstein

pomáhat služba bezpečnostního centra. A na otázku jak často, dokážu odpovědět jenom slovíčkem permanentně.

Můžete prozradit jaká přesně odvětví jsou nejvíc riziková z hlediska hackerských útoků?
Jeden z významných odborníků v oblasti kybernetické bezpečnosti a zakladatel několika bezpečnostních dohledových center pan Karel Šimeček vždy říkal, že v oblasti kybernetické ochrany existují pouze dvě cesty, buď být marketingově naprosto ale naprosto nezajímavý, nebo se účinně bránit. Samozřejmě jsou odvětví, která jsou ohroženější a velmi často se stávají terčem sofistikovaných kybernetických útoků, např. zdravotnictví, ale útočníci si dnes už moc nevybírají. Prostě zkoušejí, kde se jim podaří prolomit zabezpečení a v okamžiku úspěchu pokračuje útok dál s cílem poškodit napadený subjekt. I motivace může být různá, nejčastěji se jedná o finanční motivaci, ale setkáváme se i se snahou se zviditelnit, konkurenčním bojem, nějakou formou msty či snahou dehonestovat konkrétní osobu. Nemyslím si tedy, že by dnes existoval subjekt, který si může dovolit kybernetickou ochranu neřešit.

Jak by se dalo chránit před potenciální hrozbou bez zasahování specialistů?
Je nutné si uvědomit, že nákup zařízení pro kybernetickou bezpečnost je krok správným směrem, ovšem nikoliv poslední. Musíte kybernetickou ochranu aktivně řešit především v oblasti personálního zajištění. Prostě musíte mít vlastní specialisty, kteří se budou bezpečnosti věnovat. V praxi to znamená mít několik technicky zdatných specialistů v různých odborných rolích, kteří budou nepřetržitě monitorovat vaši síť, vaše zařízení a aktivně řešit všechny anomálie. A ano, takové řešení je velmi drahé. Druhou variantou je nákup této ochrany formou služby, kde profesionální bezpečností centrum přebírá tuto práci za zákazníka. Jelikož se vlastně bavíme o sdílení odborných specialistů mezi několik uživatelů, je taková služba i ekonomicky přijatelnější. A z mých zkušeností také sofistikovanější.

Setkáváte se také s žádostmi o pomoc, že je klient pod silným kybernetickým útokem a nefungují mu žádné systémy?
Toto slyšíme hrozně neradi a většinou je na jakékoliv řešení již pozdě.
Pokud je subjekt chráněn kybernetickým bezpečnostním centrem, žádosti a požadavky většinou směřují opačným směrem, tedy od služby směrem ke klientovi. Specialisté bezpečnostního centra sledují, co se v síti klienta děje, vyhodnocují všechny anomálie a při zjištění nedostatků ať již bezpečnostního, nebo také provozního charakteru, směřují požadavky včetně návrhu opatření směrem ke klientovi. Tento postup právě výrazně napomáhá k eliminaci budoucích bezpečnostních incidentů.
Pokud nastává situace, kdy samotný klient nedisponuje dostatečným množstvím technicky znalých odborníků, i v tomto případě jsou služby bezpečnostního centra výrazným přínosem a certifikovaní specialisté centra mohou přímo pomáhat s konfigurací některých zařízení, případně s požadavky jiného charakteru z technické oblasti.

Jakými způsoby se dá preventivně kybernetickému útoku zabránit?
Útoku je nutno aktivně předcházet! K tomu právě slouží odborné znalosti, správné technologie a jejich správné nastavení a důkladné odladění. A samozřejmě, pokud se začne ve vaší síti dít cokoliv podezřelého, musíte rychle reagovat, zjistit příčinu a zvolit adekvátní reakci. Buď si tyto činnosti musíte zajistit sami, nebo využijete službu složenou z týmu operátorů, kteří nepřetržitě monitorují vaši síť, z týmu analytiků, kteří vyhodnocují všechna zjištění, analyzují je a navrhují opatření a z týmu dalších technických specialistů, kteří jsou certifikovaní odborníci na různé technologie. Extrémně důležitý je nepřetržitý monitoring, kybernetickou bezpečnost prostě nemůže zajišťovat IT specialista na půl úvazku. Tedy může, ale musíte se modlit, aby k útoku došlo v době jeho pracovní doby.

S jakými přesně druhy kybernetických útoků se v rámci své činností setkáváte?
Typové množství útoků je tak obrovské, že je ani nelze všechny popsat. V poslední době jsou poměrně časté útoky DDoS, tedy útoky, kdy obrovské množství útočících zařízení posílá dotazy na vaše technologie a tím je fyzicky vyřadí z provozu. Mnoho organizací se mylně domnívá, že jsou napadeni DDoS útokem, než se ukáže, že se jedná o horší variantu ransomware útoku, který vám šifruje data. Tento typ útoku zažila např. Nemocnice Benešov nebo v poslední době ŘSD. Škody takových útoků jsou následně ve vyšších desítkách miliónů korun, oproti tomu jsou vynaložené náklady za kybernetickou ochranu minimální. Ale setkat se můžete např. i s problematickým zaměstnancem, který vám krade data, nebo je jeho cílem se zaměstnavateli za něco pomstít.

Jak odlišovat důvěryhodné internetové zdroje od těch zavádějících i přes to, že na první pohled vypadají řádně?
Je nutné kontrolovat, zda je připojení bezpečné, což můžeme rozpoznat ze zkratky HTTPS v URL a zda certifikát, který určuje bezpečnost takové stránky, není podvržen a je platný. Kontrolovat legitimitu odkazů, zda to, na co mám kliknout, je opravdu to, kam klikám a nejedná se o podvržený

odkaz. Také je vhodné si všímat případného výskytu množství gramatických chyb, číst recenze, bezhlavě nepovolovat cookies, neklikat na všechno co přijde pod ruku a ověřovat si zdroje a autory. Je toho moc, že? V každém případě se množství kybernetických útoků a bohužel jejich sofistikovanost stále zvyšuje. Je nutné být obezřetný a rozvážný při každém kliknutí na internetu.

Jak postupovat v případech úniku dat? Můžeme dnes důvěřovat aplikacím?
Tak snažím se tady vysvětlit, že k úniku dat by nemělo dojít. Pokud taková situace nastane je nutné se co nejdříve odpojit od internetu. Prostě zamezit dalším škodám. Osobně doporučuji co nejdřív kontaktovat odbornou společnost, která se problematikou zabývá a další postup řešit s nimi. Samozřejmostí je nahlásit incident Policii ČR, a pokud spadáte pod povinné subjekty dle Zákona o kybernetické bezpečnosti, také Národnímu úřadu pro kybernetickou bezpečnost. K dalším obecným doporučením určitě patří vytvoření nových hesel ke všem vašim účtům. Dnes už je samozřejmostí mít nastavené dvoufaktorové ověřování, díky kterému musíte poskytnout více na sobě nezávislých faktorů k potvrzení přístupu. Pokud vám začnou chodit emaily nebo zprávy týkající se úniku dat, neklikejte na žádné odkazy. Mobilní telefony se stávají stále vyspělejšími a jejich používání včetně různých aplikací se stává běžnou součástí života. Bohužel se spousta hackerů posouvá právě do oblasti mobilních aplikací. Dnešní nejrozšířenější platformy iOS a Android negarantují bezpečnost vytvořených aplikací. Opět v rámci obecných pravidel je nestahovat aplikace, které neznám, sledovat recenze, ověřit si autora aplikace, ověřit si název aplikace (zda se neliší od původního). V neposlední řadě je nutné hlavně číst a nepovolovat aplikacím nadbytečná oprávnění, která by s aplikací neměla souviset. Jedná se především o sledování a sdílení polohy, čtení kontaktů a zpráv, přístup k fotoaparátu atd. A samozřejmostí je využívat maximální ochranu mobilního telefonu stejně, jako u notebooku či PC.

Jaká je vaše vize do budoucna?
Pořád mám pocit, že kybernetická ochrana je velmi často brána na lehkou váhu. I přes odstrašující příklady z nedávné minulosti se v mnoha institucích, organizacích a firmách nevěnují kybernetické ochraně vůbec, nebo v minimální míře. V komerční sféře je situace malinko lepší, většina majitelů si dnes umí vypočítat, co společnost stojí den výpadku provozu a podle toho se chová. Přesto se snad blýská na lepší časy, je připravena nová směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii, směrnice NIS2, která přináší mnoho změn v oblasti zajišťování kybernetické bezpečnosti a týká se nejen organizací, které jsou již dnes ze zákona o kybernetické bezpečnosti povinny své systémy zabezpečovat, ale i velkého množství organizací, které budou do regulace spadat nově a do dnešního dne žádné povinnosti plnit nemusely. Takže mým přáním je, aby přibývalo společností, které ke své kybernetické ochraně přistupují zodpovědně, s péčí řádného hospodáře a aby ubývalo množství úspěšných kybernetických útoků. Albert Einstein prohlásil, že „Svět je nebezpečné místo k životu, ne kvůli lidem, kteří jsou zlí, ale kvůli lidem, kteří s tím nic neudělají". ■

Bezproblémový provoz recepcí a možnost vstupu nonstop? Jednoduše s e-Reception.

Ing. Kateřina Kulíšková
Business Development Manager
ve společnosti Innovis

Je nadšencem do inovativních technologií a digitalizace. Ve společnosti M2C působí na pozici specialisty na automatizaci a digitalizaci objektů.

Každá větší budova, ať je to budova administrativní, vysoká škola, úřad nebo obchodní centrum má svou recepci. Ta nám nabízí kromě samotného vstupu do příslušné budovy mnoho dalších užitečných funkcí. Obvykle se tam nachází osoba, jež nám pomáhá se záležitostmi nejrůznějšího rázu. Co když veškerá její činnost bude najednou nahrazena umělou inteligencí? Nejnovější trendy v této oblasti nám přiblížila Ing. Kateřina Kulíšková, Business Developement Manager ve společnosti Innovis.

Můžete prosím našim čtenářům e-Reception blíže představit? Jaké jsou její očividné výhody vůči fyzické recepční?
Naše e-Reception je cesta, jak lze zautomatizovat a zefektivnit vstup do budov. Jedná se o řešení, které dokáže zcela nahradit běžné procesy fyzické recepční, kterými jsou například odbavení návštěv a jejich identifikace, vedení docházkové knihy, video spojení s osobami uvnitř budovy, vydávání vstupních karet či generování QR kódů a mnohé další. Je tak efektivně zajištěna, jak procesní, tak bezpečnostní stránka vstupu do budovy. Mezi očividné výhody e-Reception vůči fyzické recepční nepochybně patří provoz 24/7, nespočetné jazykové mutace a velmi znatelná úspora nákladů. Pozvánky si uživatelé generují pomocí mobilní aplikace či webového rozhraní, tudíž zde lze hovořit i o vysoké přehlednosti pozvaných návštěv. Jedná se o velmi spolehlivého a přívětivého pracanta, jehož ovládání je velmi intuitivní a snadné.

Podle vašeho webového formuláře existují 2 způsoby využití e-Reception – buď jako úplná náhrada stávající recepční, anebo jako její podpora. O co se jedná ve druhém případě? Jakou úlohu by podle vás měla plnit stávající recepční a jakou elektronická?
Často se nám stává, že klienti mají tzv. „zdoublované" recepce, což znamená, že na recepci místo jedné recepční sedí recepční minimálně dvě. Je to primárně z toho důvodu, že se recepční často stará i o provozní potřeby například kanceláří, vykonává tedy i funkci office manažera. V takovém případě by se ovšem nemělo stát, že recepce zůstane zcela prázdná a příchozí návštěvníky nemá kdo odbavit, tudíž musí na příchod recepční čekat. A tohle je přesně práce pro naši e-Reception! Zatímco pracovník recepce zařizuje jinou agendu, návštěvníci se bez problémů a bez čekání odbaví na našem kiosku.

Uvádíte, že kiosek si může zákazník zakoupit nebo mu společnost Innovis kiosek profinancuje. Mohla byste prosím podrobněji popsat, za jakých podmínek může potenciální zákazník počítat s touto variantou?
Uvědomujeme si, že v dnešní nestabilní době může být problém s hledáním většího objemu volných finančních prostředků na projekty, u kterých je nutné vynaložit určitou vstupní investici. V tomto případě dokážeme klientovi s takovouto

investicí pomoci, a to tím způsobem, že prvotní náklady pokryjeme my, jakožto firma, a tuto částku poté klient hradí v rámci měsíčního paušálu. Znamená to tedy, že na počátku projektu klient nemusí vynaložit žádné vstupní náklady, ale začíná řešení hradit až formou měsíčních splátek.

e-Reception může fungovat v rámci různých objektů. Jaký by byl rozdíl mezi e-Reception na vysoké škole a v průmyslu?
Přesně jak uvádíte, naše e-Reception nemá jasně stanoveno, že se jedná o kiosek využitelný např. pouze pro administrativní budovy. Snažíme v tomto směru myslet tzv. „out of the box", což znamená, že systém e-Reception „ohýbáme" individuálně dle potřeb jednotlivých klientů, proto ji lze využít na různých objektech.
Využití e-Reception na vysoké škole je principiálně velmi podobné jako to, které se využívá v administrativních budovách. Dnes je naprostým standardem, že se každý student musí při vstupu na akademickou půdu prokazovat studentským průkazem. V případě příchozích návštěv jsou na recepci, po zjištění důvodu vstupu a po předložení průkazu totožnosti, vydávány vstupní návštěvnické průkazy. A právě s touto agendou si e-Reception hravě poradí, včetně např. video spojení se studijním oddělením či s orientací po budově.
V průmyslu využíváme e-Reception trošičku jiným způsobem. Dokážeme díky ní zautomatizovat logistické procesy na objektech. Nenahrazujeme zde tedy recepční, ale spíše vrátného, případně také minimálně jednu pozici ve spediční kanceláři. Zde je e-Reception propojena s dalšími technologiemi jako je např. kamera se čtením SPZ, automatická závora, LED tabule, ale také se spedičním softwarem používaným na objektu. Právě díky využití e-Reception na takovýchto objektech dochází k daleko efektivnějšímu identifikaci a odbavení řidičů, kteří přijedou ke klientovi na nakládku či vykládku zboží. Abychom vše ještě více zjednodušili, po prvotní registraci mohou řidiči pro vjezd využívat také velmi uživatelsky přívětivou mobilní aplikaci.

Kolik by stál roční pronájem e-Reception?
Vše je velice individuální. Velmi záleží na procesech a funkcích, které jsou třeba na daném objektu. Ke každé poptávce přistupujeme individuálně, tedy ji i individuálně naceňujeme. Je rozdíl mezi cenou e-Reception, u které by byla potřeba vyvíjet nějaké dodatečné funkce a mezi e-Reception, u které postačí základní funkcionality. Mohu však prozradit, že se v základu pohybujeme někde na polovině nákladů např. za fyzickou recepční, takže roční úspora je zde opravdu znatelná.

V čem podle vás spočívá hlavní výhoda využití e-Reception? Je to záruka bezpečnosti a zjednodušení procesu odbavení, nebo kontrola jedince prostřednictvím přístupu k jeho osobním údajům?
Hlavní výhodou e-Reception je právě již uvedené zefektivnění procesů a úspora nákladů, kterou v dnešní době ocení nejeden klient. A nesmím zapomenout na takový ten příjemný nádech moderního přístupu.
Řešení e-Reception lze, v jistém slova smyslu, prohlásit zárukou bezpečnosti procesu odbavení osob. Máte skvělý přehled o tom, kdo se vám pohybuje ve vašich prostorách a jaké množství osob se v danou chvíli na objektu nachází, což může být velmi důležité například při evakuaci budovy, a ve spojení s mechanickými zábranami a přístupovým systémem vám, bez vašeho vědomí, nikdo do objektu vstoupit nemůže. Eliminujeme zde také chybovost lidského faktoru a případnou možnost napadení pracovníka recepce za účelem násilného vstupu do budovy.
Neřekla bych zde, že se jedná přímo o kontrolu jedince prostřednictvím přístupu k jeho osobním údajům. Některé budovy ověření totožnosti vůbec nevyžadují. V takových případech nemusí být čtečka ID do řešení zakomponována. Máme však klienty, kteří toto ověření vyžadují, a to primárně z bezpečnostních důvodů. Vše je na požadavcích klienta.

Existuje určitý systém ochrany osobních údajů? Jak se může potenciální uživatel chránit před únikem svých dat? Koneckonců, pokud by si někdo přál, mohl by zjistit, s kým přesně měl člověk schůzku a kdy?
Veškeré procesy e-Reception splňují legislativní rámec zákona o ochraně osobních údajů a souvisejících evropských nařízení. Dbáme na to, aby data našich klientů byla vždy chráněna, a to se nejedná pouze o případ e-Reception, ale je tomu tak u všech našich technologických řešení. Vzhledem k faktu, že provozujeme taktéž dohledové centrum, bezpečnost a ochrana proti úniku jakýchkoliv dat je pro nás naprosto zásadní. Do systému mají přístup pouze ti uživatelé, kterým byl přístup udělen administrátorem. A i sami uživatelé vidí pouze do svých vlastních uživatelských účtů, na bázi tzv. uživatelských oprávnění, nemají tudíž přístup k účtům žádného jiného uživatele. Nemůže se tady stát, aby se někdo dostal k elektronické docházkové knize někoho cizího.

Kolik času obvykle zabere instalace e-Reception včetně implementace požadovaných funkcí? Existuje nějaké testovací období?
Instalace e-Reception na objektu jako taková obvykle trvá pouze několik dní. Naši technici jsou velmi šikovní. Následuje měsíční testovací období, kdy se v rámci implementace systému, napojení na ACS atp., vylaďují veškeré procesy tak, aby byl provoz e-Reception zcela hladký a bez jakýchkoliv problémů.

Může e-Reception zcela nahradit fyzickou sílu? Pokud ano, kdy by k tomu mohlo podle vás dojít?
Určitě může a děje se to již dnes. Vše je však odvislé od nastavených procesů a potřeb jednotlivých objektů. Pokud má společnost na recepci člověka, který zastává i jinou agendu například asistenta či office manažera, jsou zde procesy, které ještě nahradit neumíme (i když věřím, že vše je jen otázkou času a vývoje). Takže ano, e-Reception dokáže zcela nahradit fyzickou sílu a na spoustě objektů je to již realitou. ■

If you see something, say something. Jakou roli hraje svědek?

Mgr. Filip Gundza
Vedoucí oddělení prevence kriminality Krajského úřadu Středočeského kraje

V bezpečnostních činnostech má 10letou praxi, z toho 9 let působil ve sféře komerční bezpečnosti. O ledna 2022 do současnosti je vedoucím oddělení prevence kriminality Krajského úřadu Středočeského kraje a rovněž předsedou dvou poradních orgánů hejtmanky Středočeského kraje. Jako vedoucí odborného oddělení by rád skutečně naplnil vizi „Bezpečného Středočeského kraje“, díky nekonvenčnímu přístupu oddělení prevence kriminality a bezpečnostního managementu.

Co je to zločin? Nepřípustné chování a činy samotného pachatele nebo existují i další viníci? Je to velice složitá síť navzájem se ovlivňujících faktů. Znamená to, že když jsme jen pasivními recipienty, tak že za nic v podstatě nemůžeme? V daném rozhovoru chceme obrátit vaši pozornost na to, jakým způsobem může občan dodržující zákony přispět k potenciálním nehodám svou mlčenlivostí a ignorancí. Podrobněji jsme takové případy probrali s Mgr. Filipem Gundzou, vedoucím oddělení prevence kriminality Středočeského kraje.

Co je podle Vás v rámci vaší agendy nejdůležitější, můžete vymezit tři klíčové body?

Prvním bodem – přehled o aktuálním dění událostí a skutečností v ČR v kontextu bezpečnosti a prevence kriminality. To, co se odehrává ve společnosti se odráží na kriminalitě a mnohdy i na bezpečnostní situaci ve státě. Na tyto proměnné reaguje společnost a vytváří se celková nálada. Proto je bezpečnost vnímána jako sociální fenomén.

Druhým bodem – předávání a sdílení informací, neboť bez informací potřebných k řešení nějaké situace či problému se nelze efektivně obejít a v oblasti bezpečnosti a prevence kriminality tento přístup platí „dvojnásob".

Třetím bodem – kooperace – není důležité pouze delegovat úkoly, ale zároveň aktivně spolupracovat a nacházet řešení na základě „brainstormingu". Nicméně tento mnou zaujímaný přístup není „dogma" a vždy by měl být uzpůsoben aktuální potřebě managementu a momentálního stavu rozpracovaných priorit, úkolů apod.

Takovýchto bodů mám spousta a tři je málo ☺.

Jak motivovat lidi k většímu zájmu o to, co se kolem nich děje z hlediska bezpečnosti? Jakou roli má edukace mládeže?

Společnost nejen v ČR, ale i na jiných místech ve světě zaujímá takový nebdělí až mnohdy laxní přístup k zajišťování bezpečnosti jako stavu entity pro její existenci.

Navzdory tomuto konstatování si však dnes dovolím uvést, že pocit uvědomování bezpečnosti je čím dál tím více vnímán naší společností, a to je velice dobře. Bezpečnost není samozřejmostí a vyžaduje, jak rád uvádím „flexibilní přístup k jejímu zachování".

Soudobý stav mysli společnosti vyvolaný nejen přetrvávajícím válečným konfliktem na území Ukrajiny vyvolaný Ruskou federací, nýbrž případné negativní aspekty migrační vlny. Stále je přítomna dohra frustrace z covidové pandemie, rozevírající se nůžky a disproporce ve společnosti, to vše se odráží, jak uvádím výše na náladě ve společnosti. V konečném důsledku všechny zmiňované okolnosti jsou jistou proliferací možných mimořádných událostí způsobené vůlí člověka.

Z druhé strany úhlu pohledu je dobré to, že lidé v kontextu výše konstatovaného si uvědomují možné hrozby a z nich vyvstalá rizika, a to přináší benefit v podobě větší bdělosti a ostražitosti a také nelze opomenout netečnost vůči svému okolí. V zahraničí (konkrétně ve Spojených státech, ale také i ve Velké Británii) razí přístup „If you see something, say something", pro změnu ve Francii podporují a kladou důraz na přístup, že „každý občan je aktérem bezpečnosti". Máme tedy, kde čerpat inspiraci k těmto efektivním

„Vše co se dnes odehrává v bezpečnostní problematice, začíná u prevence a preventivních opatření“

přístupům a pozitivnímu přístupu k zajišťování bezpečnosti obecně. Edukace mládeže a věnování se jejich výchově je základem prevence prekriminálního chování. Je dokázané, že etalonem toho, aby mládež neinklinovala k trestné činnosti (kriminalitě) je funkční rodina a zkrátka nenarušený proces socializace, který má pozitivní dopad na změnu nepříznivých společenských a ekonomických podmínek, jež jsou považovány za klíčové příčiny páchání trestné činnosti.

Jsem rád, že Středočeský kraj vnímá problematiku primární prevence (první klíčová úroveň preventivních aktivit v prevenci kriminality) realizované ve školách zodpovědně a participuje na ní jak po finanční, tak odborné stránce věci.
V zásadě ve vývoji dětí a mladistvých se odráží stav a funkčnost v rodině. Eventuálně k negativním dopadům v kontextu kriminality přispívá právě kyberprostor a s ním spojená rizika v on-line prostředí.

Proč podle vás drtivá většina občanů raději mlčí, než by reagovala na problém včas a tím předcházela potenciálním zločinům?

Lidé mlčí zejména z toho důvodu, že se „bojí něco udělat, zareagovat či zkrátka nějak zasáhnout apod.“, poněvadž tímto se mohou stát dalším aktérem momentálně probíhající trestné činnosti a mimořádné události a mohou se vystavit nebezpečí své osoby, eventuálně osoby blízké či v neposlední řadě dalších nezúčastněných osob.
S tím jsou však spojené další činnosti, které jsou většinou pro společnost nepříjemné či dokonce „otravné“ např. podání vysvětlení na policii, nebo i poskytnutí svědecké výpovědi, další konfrontace s pachatelem. Při uvědomění se uvedených důvodů, vede právě člověka k nereakci a neřešení, či nepřekážení trest. činu, kdy osoba nechce na sebe vzít určitou zodpovědnost.
Tento aspekt potřebnosti přítomnosti tzv. účinného ochránce je mnohdy problematický z různých důvodů, protože společnost někdy při uvědomění se výše konstatovaného raději skutek přehlíží a je vůči němu netečný, a tak nastává někdy i bystander effect.

Je těžké motivovat, ale myslím si, že stačí, aby si každý uvědomil, „že vše co se dnes odehrává v bezpečnostní problematice, začíná u prevence a preventivních opatření“.
Nikdy nevíte, zda právě Vy budete potřeba někdy v nějaké situaci pomoci a budete doufat, aby nenastal u nezazinteresovaných osob třeba právě zmiňovaný bystander effect.

Jak produktivněji pracovat s vězni, aby u nich po propuštění nedocházelo k recidivám?

Toto je těžká otázka a nejde ji lehce popsat v několika řádcích, každopádně se o to pokusím s odkazem na relevantní zdroje ☺. V prvé řadě je nevyhnutelné změnit přístup justice a realizace trestní politiky, jinými slovy je nutné optimalizovat procesy s touto oblastí spojené. Výhledově to je velice náročný a zdlouhavý proces. K dnešnímu dni je ve výkonu trestu odnětí svobody 19 234 osob. (z toho ve Středočeském kraji, kde jsou 4 věznice je 3 282 osob, celkově to je 17 % z inkriminovaného čísla ČR).

Paní Doubravová (ředitelka neziskové organizace RUBIKON Centrum, z. ú., se kterou spolupracuje Středočeský kraj ve vztahu k resocializačním programům) konstatuje, že ačkoli počet trestných činů i počet vězněných osob dlouhodobě mírně klesá, index uvěznění je v ČR stále jedním z nejvyšších v rámci EU, i nadále se např. zvyšuje počet žen ve vězení.

Aby opakovaně trestané osoby neinklinovali opětovně k páchání trestné činnosti je nevyhnutelné vyřešit tyto aspekty, které stěžují integraci do společnosti:

- Nahromadění sociálního znevýhodnění cílové skupiny (nízká finanční gramotnost a předlužení, náchylnost k závislostem (látkové a nelátkové drogy), sociální nestabilita a mohli bychom pokračovat dále…
- Vnější příčiny představují prisonifikaci = negativní vliv pobytu ve vězení obsahuje např. vliv vězeňské kultury, přetrhání kontaktu s vnějším světem;
- Stigmatizace a nálepkování osob s trestní minulostí a obavy společnosti z této cílové skupiny a mnoho dalšího.

Pokud pomineme výše uvedená současná úskalí, která představují problémy s horizontem řešení několika let, navzdory tomu je možné aktivně přispívat ke snižování recidivy, a to prostřednictvím resocializačních programů předmětné cílové skupiny a v neposlední řadě využívání zaměstnávání osob v rámci obcí, jež jsou ve výkonu alternativních trestů (např. obecně prospěšné práce či peněžitý trest). Tímto můžeme pozitivně motivovat následnou integraci do společnosti a optimalizovat justiční system a v neposlední řadě efektivně využívat princip restorativní justice. V této činnosti se však nelze obejít bez spolupráce s Probační a mediační službou ČR a neziskovými organizacemi, která mimo jiné ve Středočeském kraji funguje velice dobře a jsem za ni moc rád a tímto jim chci i poděkovat ☺.

Pokud byste měl možnost vyslovit tři hlavní teze, které by měl slyšet každý občan ČR, které by to byly?

Budu se opakovat:

- Vše, co se dnes odehrává v bezpečnostní problematice, začíná u prevence a preventivních

opatření a uvědomování si bezpečnosti jako důležitého stavu pro fungování společnosti;
- Převzato z přístupu Francie „každý občan je aktérem bezpečnosti“;
- V současné době hlavně snažit se zůstat v klidu nad věcí.

Jak vnímáte progres v oblasti prevence kriminality v rámci Středočeského kraje z dlouhodobé perspektivy a jaké máte plány na následujících pět let?
Jsme v pozici zatím krátkou dobu, v lednu 2023 to bude jeden rok, co jsem otevřel bránu Krajského úřadu Středočeského kraje ☺.
Proto je zatím brzo hodnotit progres, to ponechám jiným autoritám, ale dostává se mi zpětná vazba, že jsou preventivní aktivity a činnosti preventivně-bezpečnostního charakteru Středočeského kraje vidět a tomu se snažím dále dopomáhat z vlastní inciativy zviditelněním na jednom nejmenovaném profesním portálu směrem k odborné veřejnosti (tedy bezpečnostní komunitě), tak i nezainteresovaným subjektům. Pozitivní vazba je mimo jiné i ze strany Ministerstva vnitra ČR, odboru prevence kriminality, co by partnera na národní úrovni v rámci vertikální úrovně systému veřejné správy.
Každopádně jsem nesmírně rád, že se mi podařilo: rozšířit portál bezpecnystredoceskykraj.cz o zbylé základní složky IZS (HZS ČR Středočeského kraje a Zdravotnickou záchrannou službu Středočeského kraje). Nyní všechny základní složky IZS mohou společně se Středočeským kraje informovat na portálu o informacích bezpečnostního charakteru ve Středočeském kraji.
Dále jsem rád, že se daří plnit vymezený Program prevence kriminality Středočeského kraje na rok 2022, ve kterém mimo jiné byla integrována “troufnu si uvést” úspěšná dvoudenní odborná konference, jejíž název byl: Aktuální bezpečnostní hrozby optikou Středočeského kraje, prevence především. Mimo uvedené konference jsem rád, že se mi dále podařilo vytvořit Regionální platformu metodického setkávání manažerů prevence kriminality působících v obcích s rozšířenou působností Středočeského kraje…

Plány, vize a priority budou v dohledné době k dispozici v chystané Koncepci prevence kriminality Středočeského kraje na léta 2023-2027, nicméně mohu uvést, že ústředních priorit bude 5 a další dvě sekundární priority. Oblastem, kterým se bude připravovaná koncepce věnovat je relativně široká a koresponduje se současným děním ve společnosti a vymezuje opatření k dosažení priorit Středočeského kraje v rámci prevence kriminality a není možné opomenout i výhledově problémové oblasti na které se bude muset kraj zaměřit a věnovat jim pozornost…

Na zbytek si musíte počkat do ledna 2023.

Děkuji za rozhovor… ■

Spolupráce inovativních přístupů a zákona

Čím dál tím víc si všímáme přítomnosti umělé inteligence. Obklopuje nás ze všech stran a je nedílnou součásti naší reality. Existují však oblasti, které se jeví jako podstatné pro náš spokojený život a pro pocit bezpečí, bez něhož by život nebyl tak pestrý a jistý. Právě v daných oblastech jsou inovativní přístupy nejvíc důležité. Jedná se zejména o oblast bezpečnostní. Jak jsme na tom s umělou inteligencí z hlediska prevence kriminality? O tom jsme si povídali s Brigádním generálem a ředitelem Krajského ředitelství policie Středočeského kraje JUDr. Václavem Kučerou.

Brig. gen. JUDr. Václav Kučera, PhD., MBA
ředitel KŘP Středočeského kraje

Začínal u pořádkové police, převážnou část své profesní dráhy se ale věnoval vyšetřování a odhalování závažných zločinů. Následně zastával několik vedoucích pozic, i ve vedení PČR, kde působil jako náměstek policejního prezidenta pro službu kriminální policie a vyšetřování.

Vždy se zajímal, navrhoval a aplikoval do policejní práce inovativní projekty zejména z pohledu digitalizace, a to ke zrychlení a zefektivnění policejních činností. Nejzásadnějšími projekty, které se již využívají rutinně, jsou videokonference v trestním řízení, digitální spis, mobilní bezpečná platforma, digitální asistovaná služba - Pol Point, či využívání dronů k dokumentaci dopravních nehod.
Funkci ředitele největšího kraje v republice vykonává 14 let, u PČR pracuje již 43 let.

Jaké trestní činy se dnes jeví jako největší problém?
Nejčastějšími trestnými činy jsou majetkové trestné činy, zejména krádeže a podvody. V poslední době se stále více vyskytují podvody spáchané prostřednictvím internetového prostředí.

Jak dle vás vypadá dokonala spolupráce policistů a umělé inteligence?
Jelikož se umělá inteligence stává běžnou součástí našeho života, tak pochopitelně i policie umělou inteligenci využívá a pracuje s ní. S postupem digitalizace procesů, kterou v současné době policie prochází, je zcela na místě počítat s využitím umělé inteligence. Nejčetnější využití je v analytické práci a v poslední době i v predikci kriminality, využívané v mapách kriminality. Ale třeba i v náboru nových policistů využíváme umělou inteligenci prostřednictvím chatbota.

Přemýšlel jste o nějaké aplikací, kterou by se dalo využít v případě jakékoli nehody? Aby člověk místo klasického volání poslal žádost na nejbližší policejní stanici?
Ano. To si nejenom dokážu představit, ale v současné době již nabízíme možnost komunikace občana s policií z libovolného místa, třeba prostřednictvím jeho počítače, mobilního zařízení nebo z místa, které je označeno jako POL POINT, aniž by musel přijít na policii. Tento způsob komunikace je videokonferenční a plně nahrazuje osobní kontakt.

Můžete podrobněji vysvětlit, jak by měly být nainstalovány softwary, aby města byla mezi sebou digitálně propojená?
Myslím, že hlavním předpokladem pro digitální propojení měst a obcí v oblasti prevence je shoda na společném postupu při řešení problémů. Mezi vedením měst a obcí by

měla být dohoda o sdílení dat a implementaci technických prostředků. Když bude shoda, není rozhodující, jaké prostředky budou využívány, včetně softwarů. Vždy by se však mělo přihlížet, aby konkrétní řešení bylo alespoň kompatibilní s běžně využívanými prostředky policií pro případné další využití.

Jaká přesně Achillova pata může být redukována prostřednictvím umělé inteligence? V jakých případech by byla produktivnější než fyzická síla?
Zcela jistě to je již zmíněná analytická činnost, ale určitě se najdou další procesy, které nejsou ještě plně digitální. Problém vidím v tom, že se někdy digitalizují analogové dokumenty, aniž by došlo k digitalizaci procesu.

Rozumíte technologiím? Kdo vám pomáhá s praktickou implementací projektů?
Určitou povědomost o nových technologiích mám, ale na programování a implementace nových projektů mám skvělý tým lidí. Na jedné straně oni realizují moje vize, na straně druhé já podporuji jejich vlastní invenci. Bez tohoto týmu si neumím realizace projektů představit.

Jaké teď mate projekty, které se nachází v před-realizačním stavu?
Souběžně pracujeme na více projektech, které souvisí s rozvojem digitalizace. Tyto projekty jsou v různých fázích rozpracování. Některé zavádíme postupně, v pilotních projektech, některé v průběhu rutinního provozu doplňuje a některé jsou v ověřovací fázi. Jedná se zejména o převody analogových procesů na digitální, které usnadňují a zjednodušují práci uvnitř naší organizace nebo například využívání chatbota pro nábor nových policistů. Posledním z projektů, který je preventivní a je zatím v ověřování, je využívání bezpilotních prostředků pro měření bezpečné vzdálenosti a rychlosti vozidel.

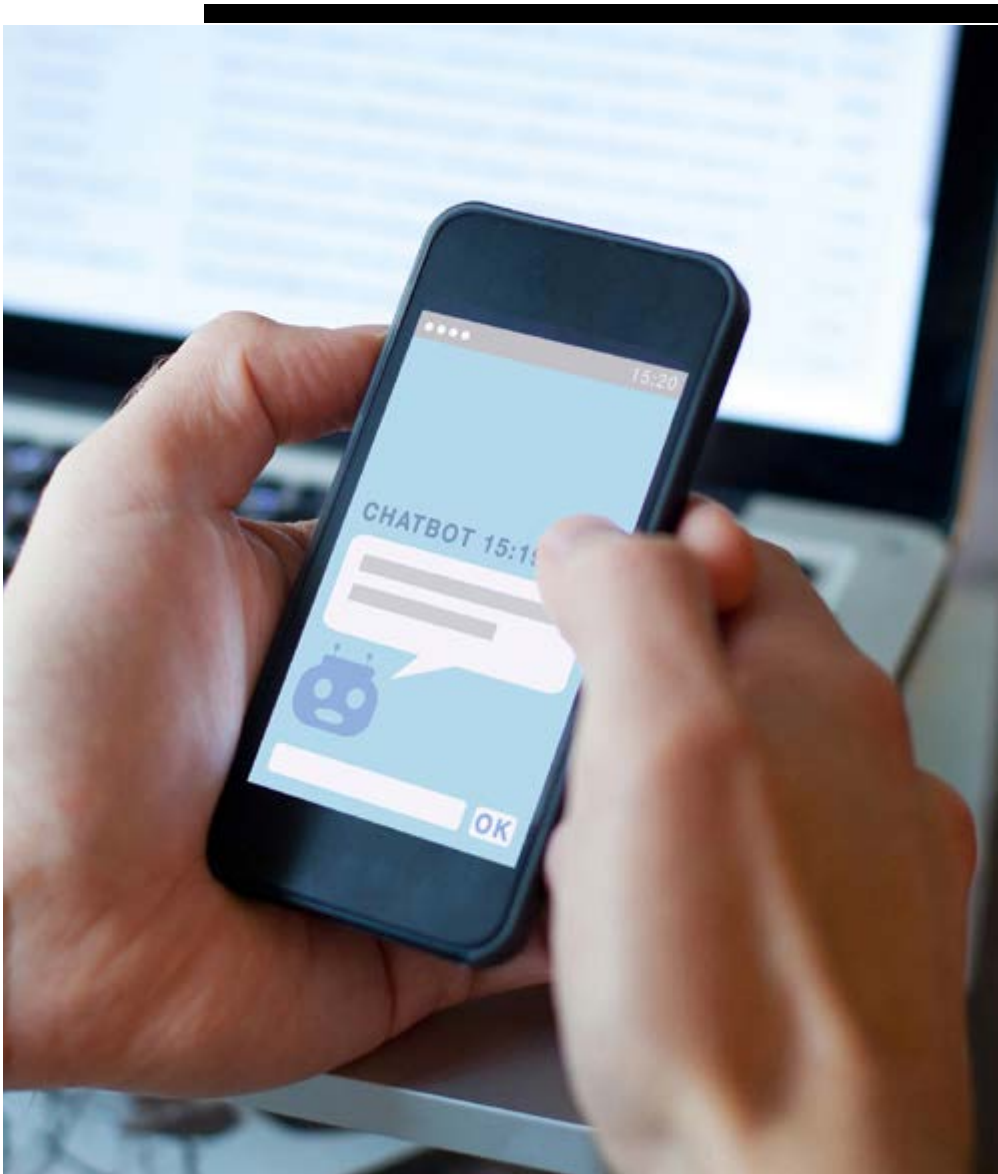
Z jakých zdrojů je digitální inteligence v rámci prevenci kriminality financována?
Nové projekty v PČR jsou financovány jednak z rozpočtu policie, z vyhlášených evropských projektů nebo z darů samospráv a to zejména v případech, kdy se přímo dotýkají bezpečnosti a prevence v konkrétním teritoriu.

O jakou pomoc je potřeba požadovat stát/vládu? Nemusí se to týkat jen investic.
Myslím, že systém pro čerpání prostředků na prevenci a podporu prevence je optimálně nastaven a je jen věcí správné volby projektů a jejich realizace k naplnění jejich cíle.

Jakým způsobem identifikujete problémové oblasti? Existují nějaká kritéria, dle nichž určujete, co se má řešit nejdřív?
Řešení projektů, zejména v prevenci, je vždy ovlivněno vývojem kriminality a závadného jednání na konkrétním teritoriu. Policie vždy reaguje na různé trendy a s maximálním využitím analytických nástrojů a na základě stanovených hypotéz identifikuje požadované cíle a harmonogram realizace.

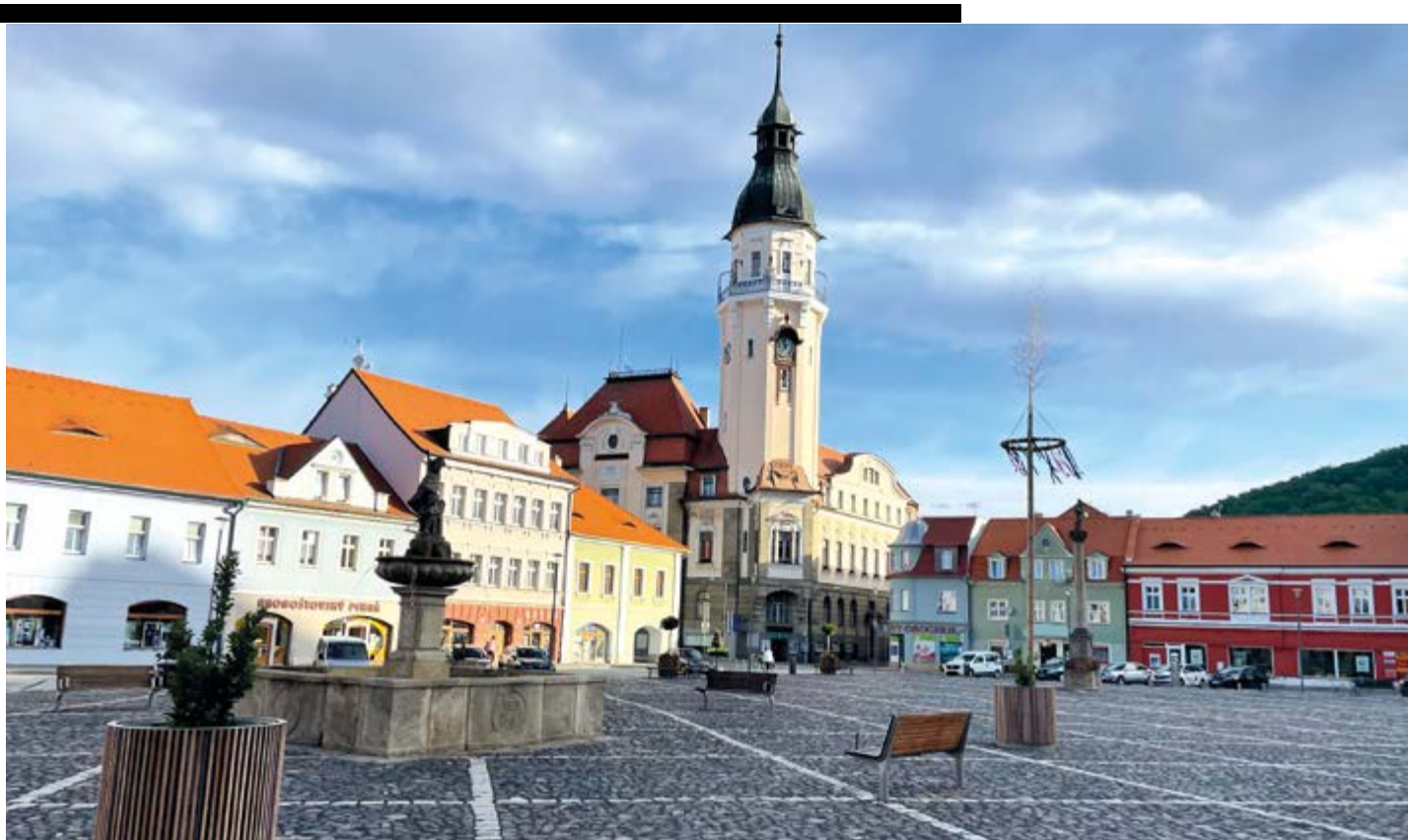
Jak dle vás vypadá stát, jenž se jeví jako „země zaslíbená" z bezpečnostního hlediska?
Česká republika se v různých světových žebříčcích hodnocení umísťuje zpravidla v první desítce zemí, které jsou hodnoceny jako země bezpečné. Vzhledem k tomu, že Česká republika je takto hodnocena již několik let, tak si myslím, že je to dobrá pozice i do budoucna. Z mého pohledu bude pro udržení tohoto stavu nutné více investovat do prevence a zvyšování pocitu bezpečí našich občanů.

Jaká je vaše vize do roku 2030?
Více procesů bez přímé fyzické účasti policistů. ■



Smart Bílina. Jak to vypadá v praxi?

Předmětem následujícího rozhovoru je technologický rozvoj konceptu Smart city ve městě Bílina, které se stalo objektem zájmu odborníků po vítězství v soutěži 5G pro 5 měst. Podrobněji jsme si o aktuální situaci v Bílině popovídali s Pavlem Kukou (PK) a Janem Čulíkem (JČ). Pavel Kuka je Idea a Project Managerem poradenské skupiny Gatum Group, která je strategickým partnerem města Bíliny při implementaci konceptu Smart City a rozvoji integrovaného přístupu k bezpečnosti a odolnosti. Jan Čulík je Projektovým Manažerem ve společnosti Innovis, která dodala a implementovala technologické řešení rozvoje městského kamerového dohlížecího systému a nástroje pro pokročilou analýzu obrazu.



Pavel Kuka
Idea Manager
poradenské skupiny Gatum Group

Zaměřuje se na strategické a technologické poradenství ve veřejné i soukromé sféře, management inovací a rozvoj konceptu bezpečných a odolných měst.

Jan Čulík
Project Manager
ve společnosti Innovis

Narodil se a žije v Praze. Vystudoval Leteckou dopravní školu. Pracoval na vývoji mobilních aplikací pro děti předškolního věku a následně na vývoji analytických softwarů ve společnosti CertiCon.
V roce 2019 nastoupil do M2C na pozici Projektového manažera vzdáleného dohledu Space. Od září 2022 má na starost technický rozvoj ve společnosti Innovis.

Co předcházelo rozhodnutí vaší společnosti zapojit se do konceptu Smart City ve městě Bílina? Proč právě toto město?
PK: Jedna ze společností naší poradenské skupiny Gatum Group v roce 2019 získala veřejnou zakázku zpracování bílinské Strategie Smart City. Měli jsme tedy možnost s městem spolupracovat při implementaci konceptu od samého počátku. V tomto období jsme zjistili, že pocit bezpečí je pro Bílinu a její obyvatele zásadní téma. Po dokončení strategie jsme se proto zaměřili na podporu integrované bezpečnosti a hlavně rozvoj městského kamerového systému.

Jak dlouho trvala samotná příprava projektu? Co bylo jeho ústředním cílem?
PK: Jako reakce na jeden z cílů strategie v roce 2020 spolupracovali na vytvoření studie dalšího rozvoje MKDS Bílina. Provedli jsme kompletní hodnocení technického stavu kamer, zařízení dohledového centra a infrastruktury. Věnovali jsme se také dostupným zdrojům a návazným procesům.

Naše role byla jak odborně-technická, tak projektová. Koordinovali jsme vytvoření technických a provozních standardů, které vznikly za spolupráce Městské policie Bílina a vedení města. Výsledky jsme ještě konzultovali se zástupci Policie České republiky a bezpečnostními experty. Společně jsme také určovali prioritní lokality pro nasazení kamer. Naší přidanou hodnotu bylo mimo jiné i vymezení bezpečnostních scénářů, které měly být řešeny s využitím inteligentních analytických nástrojů. V neposlední řadě ještě v rámci přípravných prací můžu zmínit provedení auditu systému správy a údržby, které vedly k restrukturalizaci kompetenčního modelu.

Všechny tyto aktivity měly za cíl zajistit, aby rozvoj kamerového systému probíhal koncepčně a reagoval na skutečné potřeby města, městské policie a dalších stran, které se podílejí na utváření bezpečnostního prostředí Bíliny. Důležité pro nás bylo, aby rozšiřování kamerového systému probíhalo účelně, v opodstatněných lokalitách a aby obyvatelé vnímali jeho pozitivní přínos.

Důležité je zmínit, že ve stejné době se Bílina účastnila soutěže 5G pro 5 měst se svým projektem využití bezdrátové konektivity 5. generace pro potřeby kamerového systému. Náš tým pomáhal s designem vítězného návrhu, který umožnil celou Smart vizi akcelerovat. Bílina v tu dobu řešila nedostatečnou přenosovou kapacitu mikrovlnných spojů a nízkou dostupnost optické sítě. Krom statických kamer se nakonec podařilo otestovat i připojení tělových kamer strážníků a kamer ve vozidlech městské policie. Hlavní je, že výsledky projektu měly dopad na další uvažování města, zejména si uvědomilo význam a přidanou hodnotu regionální spolupráce.

První fáze projektu kulminovala v lednu 2022, kdy Bílina vysoutěžila realizaci opatření navrhovaných ve Studii rozvoje – byly instalovány nové kamerové body, ve vybraných

lokalitách město nasadilo zvukové senzory, ale hlavně došlo k nasazení pokročilého nástroje analýzy obrazu z kamer. Jeho využití má dopad na další rozvoj konceptu Smart City. Představuje klíčový zdroj informací nejen v oblasti bezpečnosti, ale i mobility či využití veřejného prostoru. Dodávku a implementaci realizovala společnost Innovis.

Jaká kritéria byla rozhodující při volbě specialistů, kteří rozvojovou vizi města technicky zrealizovali? Jak rychle jste se dohodli na spolupráci?

PK: Tady je nutné vnímat a pochopit specifické prostředí veřejné správy a samospráv. Zákonné povinnosti určují poměrně přísné a svazující požadavky pro výběr partnerů a dodavatelů skrze veřejně soutěžené zakázky. Nejedná se tak o přímý a volný výběr specialistů. Město v roli zadavatele může stanovit technické požadavky realizace a minimální úroveň kvalifikace řešitelského týmu. Zájemci následně dodají nabídky, které jsou vybírány na základě předem určených parametrů. Stále platí, že v České republice se soutěží primárně na cenu, což může mít negativní vliv na průběh i výsledek realizace. I proto je podoba technických požadavků naprosto klíčová a jejich význam nemůže být podceňovaný.

Jak probíhala samotná implementace bezpečnostních systémů ve městě? Kolik času uplynulo mezi návrhem vhodného řešení a jeho uvedením do praxe?

JČ: Implementaci je třeba rozdělit do dvou částí. Tu softwarovou, která má za cíl pomoci v preventivním předcházení potenciálních bezpečnostně závadných situací a tu hardwarovou, která v sobě snoubí instalaci kamerových bodů, rozvodných skříní či mikrovlnných spojů. Nasazení obou částí probíhalo v průběhu zhruba dvou měsíců s tím, že samotný návrh architektury, výběru umístění jednotlivých technologií a několika návštěv Bíliny probíhalo podobný čas. Průběh jako takový byl vcelku standardní, oproti původním časovým odhadům jsme se moc nevzdálili a s nastalými drobnými překážkami jsme si operativně věděli rady a vyřešili je na místě.

Jakým způsobem a v jakém rozsahu by podle vás technologie mohly nahradit fyzickou sílu? Jaké funkce by měla zajistit umělá inteligence a jaké lidský faktor?

JČ: Technologie je již několik let vnímána jako všemohoucí nástroj, který fyzickou sílu velmi brzy nahradí. My se k tomuto názoru nepřikláníme a myslíme si, že tento stav je ještě dlouhý čas vzdálený. Nicméně trend tohoto přerodu vnímáme. Ze zkušeností s projekty jak z komerční, tak státní správy a se znalostí dílčích procesů a pracovních postupů víme, kde se již dnes faktor umělé inteligence a dalších technologií dokáže uplatnit. Zejména z pohledu nedostatku pracovní síly není možné sledovat rozsáhlé kamerové systémy 24/7 a zároveň je vyhodnocovat a posuzovat a do toho ještě odbavovat běžné operativní požadavky. Umělá inteligence dnes přispívá právě v běžném chodu např. kamerového systému. Dokáže nahradit běžný monitoring kamer tím, že identifikuje typologii objektů jako osoba, vozidlo, motorka a další a následně dokáže pojmenovat jednotlivé situace (osoba překročila plot, auto vjelo do jednosměrné ulice a mnoho dalšího). Takže systém umělé inteligence dokáže sbírat zájmová data a předávat je uživateli. Na něm je následně to samotné posouzení situace a spuštění dalších procesních kroků.

Jak probíhala spolupráce M2C s městem při implementaci analytických nástrojů?
JČ: Nástroje pro analýzu obrazu jsou vcelku robustní technologické řešení, a tak je třeba k nim přistupovat. Nezbytným krokem je identifikace zájmových míst, kde se očekává největší přínos takového nástroje. Následně vzniká relativně dlouhý a pozvolný proces testování, zkoušení, a to jak z pohledu skutečného přínosu v porovnání s očekáváním, tak zároveň z pohledu uživatele. Pro členy MP je takový nástroj něco zcela nového, s čím je třeba se důkladně seznámit. Spolupráce tedy byla oboustranná a intenzivní hlavně z pohledu samotného nastavení dílčích funkcí na konkrétních kamerách. Tento proces, v souvislosti s rozsahem MKDS v Bílině, stále probíhá a probíhat jistě ještě bude.

Jak efektivně pracovat se systémy MKDS? Co všechno nám nabízejí?
JČ: Základem je vždy systémová platforma pro správu MKDS. Tedy prostředí, které umožňuje pracovat s kamerami, měnit jejich pozici a také možnost stažení záznamů pro další šetření konkrétních situací. Do tohoto prostředí je třeba integrovat jakoukoli nadstavbu typu analytického nástroje. MKDS disponuje různými typy kamer od statických zaměřených na konkrétní prostor. Přehledových, které poskytují širší záběr např. na náměstí. Otočné, tzv. PTZ kamery, kterými může uživatel libovolně pohybovat např. při hledání konkrétní osoby.

Jak na tom byla Bílina s personální a technickou kapacitou?
PK: Instalace a údržba systému a jeho jednotlivých prvků je řešena dodavatelsky. Hlavní výzva je proto na straně uživatelů, kteří pracují s analytickými nástroji. Jedná se o poměrně sofistikované platformy, které pro běžný provoz městské policie a operátorů kamerového systému na začátku představují významnou změnu a může chvíli trvat, než si vše osahají. Nutná je změna přístupu ve vztahu ke kamerám a sledovaným scénám. Jakmile vstřebají, jak analytika funguje a že jim práci nepřidává, ale šetří, je vyhráno. Někde to trvá déle, proto je vhodné nepodceňovat školení, přínosy komunikovat a investovat do rozvoje klíčových pracovníků.

JČ: Tady bych asi řekl to samé, co Vy.

Co kromě inovativních MKDS plánujete v Bílině nainstalovat?
PK: Kromě bezpečnosti v Bílině probíhá široká škála projektů, které vychází ze stanovené Smart City strategie. Město je velice aktivní v oblasti energetického managementu nebo digitalizace. Bílina a další města si postupně začínají uvědomovat význam dat nejen v teoretické rovině, ale také na té praktické, provozní. Jak jsem již zmiňoval, další kroky města směřují k posílení regionální spolupráce. Gatum se například podílí na vzniku bezpečnostního a datového koridoru Ústeckého kraje, který by měl usnadňovat výměnu dat mezi městy, městskými organizacemi a dalšími subjekty.

Z jakých zdrojů byl projekt financován? Jakým způsobem se na tom podílel stát?
PK: Bílina si téměř celý projekt, od přípravných prací až po jednotlivé realizační etapy, průběžně financovala sama. Výjimku tvořili doplňkové aktivity podporované z dílčích dotačních programů. Paní starostka Schwarz-Bařtipánová nechtěla otázku bezpečnosti a rozvoj města vázat na dostupnost externího financování.
Úspěšná účast Bíliny na projektu 5G pro 5 měst a navržená vize rozvoje městského bezpečnostního a situačního managementu v Bílině s podporou sítí 5G však na konci roku 2022 umožnila podat žádost o dotaci z Národního plánu obnovy, která by zpětně měla pokrýt většinu rozvojových investic v této oblasti. Odvážný ale koncepční přístup vedení města se tak vyplatil.

Jak správně vyhotovit odbornou analýzu města?
PK: Ozvěte se nám (úsměv). V každém případě je nutné stanovit přesnou strukturu a mít jasně formulovanou představu o podobě výstupu. Vždy je důležité co nejpřesněji vědět, jaký je současný stav, bez toho logicky nelze nastavit správný postup. Hlavní roli pro nás ale hraje schopnost transparentně komunikovat. Pro vedení je pak mnohem snazší vybudovat si důvěru a následně získat odvahu realizovat komplexnější projekty a upřednostňovat kvalitní řešení.

Co byste doporučoval městům a obcím před samotným nasazením inteligentní analytiky?
JČ: Zde můžeme být konkrétní a doporučením by byl technologický audit, tedy již zmiňovanou úvodní analýzu. Výstupem by měla být komplexní zpráva o potenciálu a možnostech nasazení inovativních technologických řešení do stávající architektury obce. Pod auditem si lze představit analýzu kamerového systému z pohledu jeho technické připravenosti a kvality pro nasazení analytického nástroje. Sílu signálu a datové předpoklady pro implementaci dalších zařízení. Technologickým auditem obec předchází spoustě případných problému při realizaci.

Jaká je vaše vize rozvoje projektu Smart City v Bílině do budoucna?
PK: Vize je dána. Průběžně se vyvíjí nástroje k jejímu naplňování. Nyní je kromě bezpečnosti a subjektivního pocitu bezpečí horkým tématem energetika. Strategicky jako velmi významnou oblast pro všechna města vnímáme digitalizaci, posilování datové infrastruktury a kybernetickou bezpečnost. Také doufáme, že Gatum bude mít příležitost být Bílině i nadále strategickým partnerem.

JČ: Z pohledu dodavatele zde vidím prostor v širším propojování dodaných technologií se systémy městského úřadu např. předávání informací ze SW automaticky do systémů pro generování pokut či korespondence s motoristy. Cílem Bíliny je vybudovat Smart City, ve kterém kamerový systém a data z něj generovaná tvoří pouze část celého ekosystému. Vizí je určitě propojování se systémy veřejného osvětlení, správa veškerých zařízení na jednom místě, kombinování veškerých dat a hledání cest k co nejefektivnějšímu chodu celého města. ■

Kulatý stůl: Využití umělé inteligence v oblasti prevence kriminality

Každý z nás si váží pocitu bezpečí. Ať je tím míněno cokoliv: komfortní bydlení v našich domovech, klidné večerní procházky městem či vnitřní pocit jistoty v každodenním životě. Čím dál tím víc si všímáme, že dnešní svět je plný neočekávaných zvratů osudu, že nic není stabilní. Jsme svědky neustále se měnících okolností a z toho vyplývajících následků, které nás bezprostředně ovlivňují. I přes veškeré komplikace si musíme zachovat chladnou mysl a být připraveni v případě nouze okamžitě reagovat.

V úterý 22. listopadu se v prostorách Magenta Experience Center odehrála velmi přínosná a zajímavá akce, jejímž organizátorem byla náš magazín Život za okny. Jednalo se o diskuzní Kulatý stůl, jenž se stal jakousi platformou, kde se sešli odborníci, aby diskutovali na téma: Využití umělé inteligence v oblasti prevence kriminality v rámci Středočeského kraje. Sedm profesionálů dostalo unikátní příležitost, aby přítomné starosty a vedoucí sekcí bezpečnosti, inovací a IT měst a obcí Středočeského kraje informovali o své činnosti, projektech i relevantních návrzích ohledně toho, jak zlepšit bezpečnostní situaci ve Středočeském kraji. Kromě toho měli možnost otevřít debatu o tom, jak by jejich případná společná budoucí spolupráce mohla přispět ke zlepšení bezpečnostní situace.

První mluvčí, brigádní generál JUDr. Václav Kučera, ředitel Krajského ředitelství policie Středočeského kraje, který převzal nad akcí záštitu, podrobně rozebral otázku inovativních přístupů v rámci prevence kriminality a celkově bezpečnostní situace z pohledu Policie ČR. Představil několik návrhů a projektů nabízejících možnost snížení možných dopravních nehod a zároveň popsal východiska pro řešení trestních činů nejrůznějšího charakteru prostřednictvím neosobní komunikace s policistou.

Poté dostal slovo Michal Barbořík, ředitel odboru prevence kriminality na Ministerstvu vnitra České republiky, aby pohovořil o možnostech financování relevantních projektů. Zmínil podmínky, za nichž může do některého z návrhů ministerstvo investovat. Podrobně se o všech aspektech tohoto tématu dočtete v rozhovoru uvnitř čísla.

Následně se ujal slova Filip Gundza, vedoucí oddělení prevence kriminality Středočeského kraje. Vystoupení pana Gundzy bylo zaměřeno na bezpečnostní aspekty Středočeského kraje, přičemž jako jednu z nejdůležitějších zásad zdůraznil nezbytnost sdílení informací. Měl tím na mysli především ignorování problémů ze strany veřejnosti a vy-

jádřil svou nespokojenost s pasivitou a lhostejností občanů, kteří váhají se obrátit na policisty v případě, když spatří něco podezřelého. Výstižně to shrnul heslem americké kampaně zapojení veřejnosti do bezpečnosti svého okolí: „If you see anything, say something". Co k tomu dodat? Musím souhlasit s tím, že mlčenlivost v podobných případech je pro potenciální zločince jasnou zelenou. Ignorancí jen přispíváme k bezpráví a následnému zoufalství obětí.

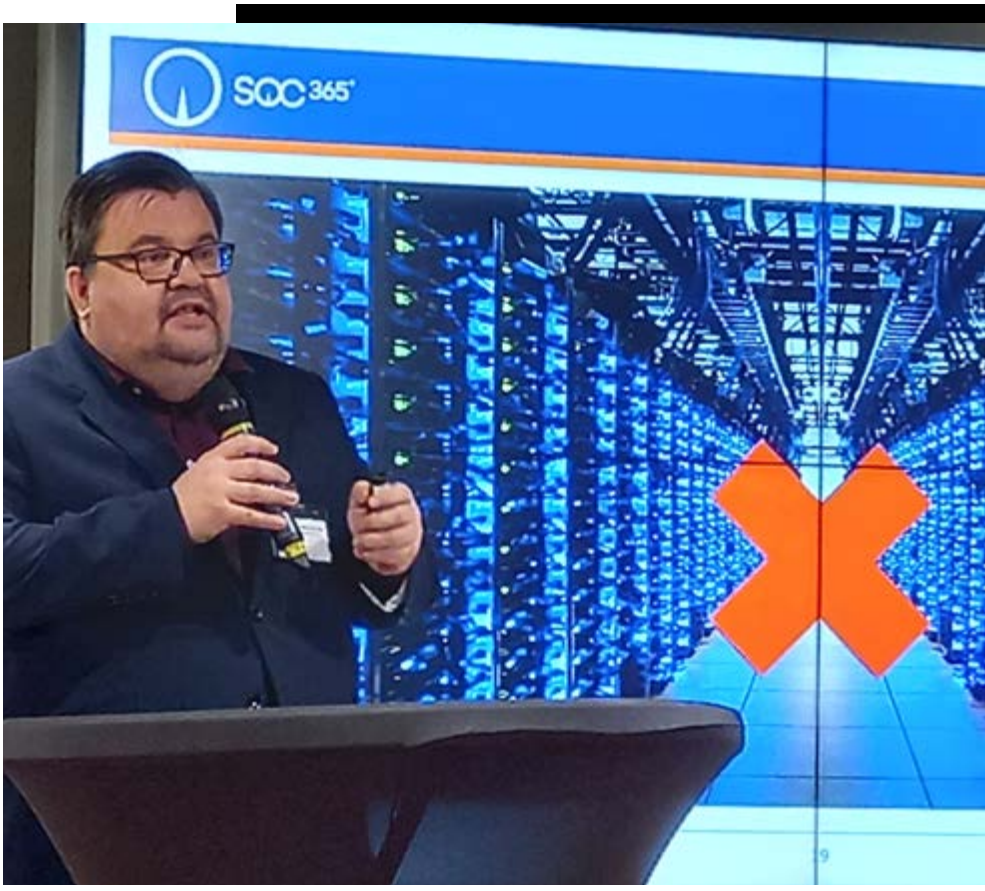
Přítomní na tuto myšlenku ihned zareagovali, což nebylo možné přehlédnout. Je potřeba poznamenat, že události typu Kulatého stolu jsou úrodnou půdou pro komunikaci, pro řešení problémů a sdílení informací.
Dalšími mluvčími byli Pavel Kuka, Idea manager ve společnosti Gatum Group, a Jan Čulík, projekt manager ve společnosti Innovis. I přesto že nepřednášeli spolu, tak se oba se věnovali stejnému tématu a to implementaci prvků chytrého města do správy města Bílina. Pavel Kuka v roli odborníka, který generuje samotnou ideu potenciálních inovací a Jan Čulík jako ten, kdo ji následně zavádí do praxe z technologického hlediska. Hovořili o inovativním systému MKDS, tedy městském kamerovém dohlížecím systému. Jedná se o moderní kamery, jež dokážou zachytit větší plochu a následně ji z různých perspektiv analyzují. Z toho důvodu mohou být použity jak za účelem bezpečnosti, tak jako cenný zdroj umožňující rešerše získaných dat, která lze využít v jakékoli oblasti správy města, což přispěje k jeho prosperitě.

Jejich přednáška mi rozšířila obzory. Pochopila jsem, čím a jak jsou kamery doopravdy přínosné. Setkáváme se s nimi v podstatě všude, avšak málokdy si uvědomujeme, jaké jsou jejich schopnosti a možnosti. Moderní člověk je samozřejmě svobodný, ale zároveň se nachází v prostředí, které je neustále monitorováno, což znamená, že v případě nouze je možné okamžitě zasáhnout. V určitém slova smyslu se každodenně nacházíme v hledáčku kamer a musíme mít vždy na paměti, že jsme sledováni a jakmile se dopustíme jakéhokoli přečinu, můžeme, a pravděpodobně budeme, za to nést společenskou odpovědnost.

Po těchto dvou vystoupeních následovala přednáška Pavla Meletzkého, IT specialisty, která byla věnována tématu kybernetické bezpečnosti. Pavel Meletzký popsal asi nejoblíbenější druh podvodů 21. století, v němž se lidé téměř ztotožňují se svými elektronickými zařízeními. Ta obsahují veškeré osobní informace o nás, naší rodině, činnosti, zájmech, jsou nositeli nejskrytějších stránek našeho života. Problémem, dle mého názoru, je, že lidstvu to přijde v pořádku, zároveň si však uvědomujeme, že už nemáme na vybranou. V období technologického pokroku se svět

digitalizuje, což vylučuje možnost daný model ignorovat. Takový životní styl mě vede k myšlence, či spíše k frázi, již známe z jedné populární hry, tedy: když město usne, probudí se mafie.
Právě o této „mafii“ hovořil pan Meletzký a měl na mysli podvodníky operující na internetu. Všichni účastníci mohli shlédnout, jaké následky může mít jeden hackerský útok. Kromě toho, že vám spadne celý digitální systém, vyprázdní se vám i kapsy. Nebo nemusí? Problém tkví v tom, že během podezřelého chování vašich elektronických zařízení byste měli zachovat klid a v žádném případě do procesu nezasahovat. V případě nehody bych vám doporučila obrátit se přímo na pana Meletzského a on, případně jeho tým, by vám doporučil, jak se v nastalé situaci zachovat.

Celou besedu završila Kateřina Kulíšková, business developement manažerka ve společnosti Innovis. Prezentovala publiku novinku



e-Recepční, která by měla nahradit fyzickou pracovní sílu při výkonu záležitostí spojených se vstupem osob do budovy. Jedná se o skutečně skvělý systém, protože nás zbavuje zbytečných komplikací spojených s registracemi návštěvníků. V digitálním systému se zachovávají data s našimi osobními udají a harmonogramem, tedy kdy a s kým máme naplánovanou schůzku. Ihned mi to připomnělo malý kapesní diář, nezbytnou věc nás všech. Pohodlný způsob, že ano? Více informací o e-Reception načerpáte z rozhovoru s Kateřinou Kulíškovou, který je součástí tohoto vydání.

Musím přiznat, že jako laik v této problematice jsem byla fascinována, s jakým zájmem a entuziasmem každý z mluvčích pojednával o příslušné problematice. Bylo očividné, že svou činnost berou opravdu vážně a touží, aby se jejich odvětví rozvíjelo. Hlavním poselstvím Kulatého stolu byla myšlenka, že pro to, aby se problémy řešily, se o nich musí hovořit. Proti tomu nelze nic namítat, jelikož prvním krokem k nalezení vhodného východiska je nalezení své Achillovy paty.

Po skončení přednášek následovala odborná diskuze, jak lze existující komplikace vyřešit, jak je redukovat, a co je zásadní, jak postupovat, abychom v budoucnu už nechodili po tenkém ledě.

Celá akce se nesla v příjemné přátelské atmosféře zpříjemněné kávovým servisem profesionálních baristů Dallmayr Kaffe. ■

Dallmayr
Nevšední káva pro každou příležitost

KVALITNÍ KÁVA. MODERNÍ DESIGN. ERGONOMIE A MOBILITA. VODA, JUICE A ZDRAVÁ VÝŽIVA V JEDNOM DOCKU. DOCKONALÝ SERVIS

Cafédock: multifunkční řešení centralizovaného občerstvení pro provoz kanceláře, showroomů, hotelových lobby, čekáren, autosalonů a meeting pointů • unikátní design a perfektní řemeslné provedení • mobilní, přitažlivé centrum setkání při krátké pracovní pauze i v rámci openspace • plně ergonomické pro náročný kancelářský provoz • reprezentativní a funkční prvek interiéru s vysokou přidanou hodnotou • individuální firemní vzhled

Dallmayr
CAFÉDOCK

Spojte se s námi: tel. 222 262 155
info@Dallmayr.cz www.Dallmayr.cz

VISITECH

EXPERTI NA KYBERNETICKOU BEZPEČNOST

SOC 365
Security Operation Center

Kybernetická bezpečnost je v současné době často skloňovaný pojem. Každý slyšel o hackerských útocích v lepších případech na webové stránky, v horších na vnitřní infrastrukturu firem, nemocnic či vládních institucí. V případě takového zásahu je v sázce nejen profit společnosti, ale také citlivé údaje mnoha lidí. Není třeba dodávat, že dochází k nenávratným škodám na firemním softwaru i hardwaru.

Vlastnit bezpečnostní technologie nestačí

Jak se proti takovému nebezpečí bránit? Mnoho společností nabízí technologie, které zaručeně ochrání data uložená v kyberprostoru. To ale nestačí. Technologie samy o sobě nejsou k ničemu, pokud nemáte k dispozici lidskou sílu, která s nimi dokáže zacházet, kontroluje je 24 hodin denně a umí z obrovské spousty výstupů vybrat ty nejrelevantnější.

Nad bezpečností dat bdí SOC365

Společnost VISITECH se tématu kybernetické bezpečnosti dlouhodobě věnuje. Již několik let úspěšně provozuje **dohledové centrum SOC365** – v Česku jedno z prvních a k dnešnímu dni největší. SOC365, to je služba zajišťující rychlou reakci v případě detekce bezpečnostních anomálií. Zákazník má záruku **nepřetržitelného provozu** a **pravidelného srozumitelného reportingu**. Unikátní je i možnost ochrany s aktivním dohledem. Vedle SOC365 nabízí VISITECH také další produkty a technologie zajišťující bezpečný síťový provoz firmy.

SOC365 zajišťuje soulad se směrnicí NIS2

SOC365 od firmy VISITECH přináší využití bezpečnostních technologií a dohled nad datovými sítěmi v souladu s aktuálními trendy. Společnost, která využije služeb SOC365, **splňuje směrnici o síťové a informační bezpečnosti NIS 2**, která ve státech Evropské Unie vstoupí v platnost v roce 2024.

VISITECH a.s.
Košinova 655/59, 612 00 Brno, Czech Republic
E: info@visitech.cz, T: +420 538 700 880
POBOČKY:
Praha 4, Michle, Ohradní 1394/61, T: +420 274 776 890
Ostrava - Vítkovice, Ruská 83/24, T: +420 597 317 377

Visitech