

**Broadband Competence Office,
Česká republika**

Analýza některých služeb s přidanou hodnotou z hlediska hospodaření obcí

**Bezpečnost v obcích v
rámci projektů Smart Cities**

Obsah

1. Úvod	4
1.1 Význam obecní bezpečnosti	4
1.2 Úloha digitalizace a vysokorychlostních sítí (VHCN)	4
1.3 Cíl analýzy	4
2. Výchozí stav v českých obcích	5
2.1 Současné praktiky v oblasti bezpečnosti	5
2.2 Rozšíření VHCN v obcích	5
2.3 Bariéry a omezení rozvoje	6
3. Možnosti a přínosy chytrých bezpečnostních řešení	6
3.1 Přehled digitálních a chytrých bezpečnostních řešení	6
3.2 Vazba těchto řešení na infrastrukturu VHCN	7
3.3 Hlavní benefity pro obecní rozpočet a obyvatele	8
3.4 Přímé a nepřímé finanční úspory	9
3.5 Bezpečnostní, provozní a společenské přínosy	9
4. Rizika a potenciální nevýhody implementace	10
4.1 Investiční a provozní náročnost	10
4.2 Provozní a technologická rizika	10
4.3 Závislost na dodavatelích, technologie a otázky ochrany soukromí	11
5. SWOT analýza (bezpečnostní management s využitím VHCN v obci)	11
5.1 Silné stránky	11
5.2 Slabé stránky	12
5.3 Příležitosti	12
5.4 Hrozby	12
6. Možné finanční a rozpočtové modely pro obec	13
6.1 Varianty financování (dotace, vlastní rozpočet, partnerství, pojišťovny)	13
6.2 Přímé a dlouhodobé rozpočtové dopady	14
6.3 Ukázkový model návratnosti investice	15
7. Příklady z praxe	15
7.1 Konkrétní případy z ČR a zahraničí	16
7.1.1 Smart City projekty v Písku a jejich přínos v oblasti bezpečnosti	16
7.1.2 Smart City projekty v Amsterdamu a jejich přínos v oblasti bezpečnosti	17
7.2 Co obci konkrétně přineslo zavedení chytrého řešení	Chyba! Záložka není definována.
8. Doporučení a další kroky pro obce	18
8.1 Strategická doporučení	19

8.2 Praktické kroky k zavedení	19
8.3 Spolupráce a zapojení partnerů	19
8.4 Sledování a vyhodnocování výsledků.....	20
8.5 Shrnutí a výzva k akci	20
9. Závěr	20
10. Literatura a zdroje	23
A. Základní a odborná literatura	23
B. Oficiální metodiky, doporučení a právní normy	23
C. Příklady a případové studie.....	23
D. Další zdroje a inspirace	25

1. Úvod

1.1 Význam obecní bezpečnosti

Bezpečnost je jedním ze základních pilířů kvality života v každé obci. Ovlivňuje nejen subjektivní pocit obyvatel, ale také reálnou míru kriminality, schopnost obce chránit životy a majetek svých občanů, rychlost reakce na mimořádné události i ochotu lidí v obci žít a investovat. Bezpečné prostředí přispívá ke soudržnosti komunity, důvěře ve veřejné instituce i atraktivitě obce pro nové obyvatele či podnikatele. Moderní bezpečnost však již není postavena jen na preventivní práci městské policie či tradičním kamerovém systému – do popředí se dostávají chytrá, datově propojená řešení umožňující včasný zásah a minimalizaci škod.

1.2 Úloha digitalizace a vysokorychlostních sítí (VHCN)

Moderní bezpečnostní řešení jsou dnes neoddělitelně spjata s digitalizací a rychlými datovými sítěmi nové generace (VHCN – Very High Capacity Networks). Tyto sítě umožňují v reálném čase přenášet obraz z kamer, informace ze senzorů (pohyb, kouř, narušení), stejně jako zajišťovat okamžité varování obyvatel prostřednictvím mobilních aplikací, SMS zpráv, elektronických sirén nebo chytrých hlásičů na veřejných prostranstvích. VHCN tvoří páteř pro kyberneticky bezpečné a stabilní napojení jednotlivých bezpečnostních technologií, integraci obecních systémů a rychlou komunikaci nejen s městskou policií, ale i s požárníky, zdravotníky nebo krajskými i státními složkami krizového řízení. Bez robustní a spolehlivé sítě by jakákoli chytrá bezpečnostní infrastruktura ztrácela na efektivitě a spolehlivosti.

1.3 Cíl analýzy

Cílem této krátké analýzy je:

- **Ukázat současné možnosti a přínosy** zavádění digitálních bezpečnostních řešení v obci s využitím sítí VHCN.
- **Pojmenovat hlavní benefity** pro obecní rozpočet i občany, včetně možnosti snížit dlouhodobě pojistné na nemovitosti díky nižší míře rizika.
- **Představit rizika a úskalí** spojená s technologickou implementací (např. otázky soukromí, ochrana dat, investiční náročnost, kybernetická bezpečnost).
- **Naznačit konkrétní doporučení a postupy** pro zavádění chytrých bezpečnostních systémů v souladu s potřebami a možností konkrétní obce.

Tato analýza je určena vedení obcí, pracovníkům veřejné správy, technickým službám i všem dalším aktérům, kteří se podílejí na plánování rozvoje Smart Cities a zodpovídají za bezpečné a udržitelné fungování samosprávy.



2. Výchozí stav v českých obcích

2.1 Současné praxe v oblasti bezpečnosti

Většina českých obcí v současnosti sází především na tradiční opatření: fyzickou přítomnost městské nebo obecní policie, spolupráci s Policií ČR či základní kamerové systémy na vybraných místech. Tyto systémy bývají často oddělené, využívají zastaralé technologie s omezeným dosahem a nižší kvalitou záznamu. Řada obcí zajišťuje monitoring ručně nebo bez pokročilé analytiky, což znamená, že reakce na incidenty je pomalejší a vyžaduje více lidské práce.

Používají se také klasické způsoby varování obyvatel – místní rozhlas či plakáty, případně telefonní kontakty na seniory a další zranitelné osoby. Moderní integrační technologie, které by propojovaly kamerové systémy, senzory a jednotný dispečink, bývají v menších obcích vzácností stejně jako digitální napojení na složky integrovaného záchranného systému (IZS). Omezené možnosti spolupráce, chybějící sdílení dat a nízká míra automatizace tak představují významné limity stávajících řešení. Přesto, jakékoliv zavedení moderních řešení může (nebo bude) narážet na otázky ochrany soukromí a na hledání konsensuální hranice

2.2 Rozšíření VHCN v obcích

Pokrytí vysokorychlostními sítěmi VHCN se v Česku v posledních letech zlepšuje, ale mezi obcemi i regiony panují výrazné rozdíly. Nejlepší je situace ve větších městech a aglomeracích (Praha, Brno, Ostrava), kde jsou k dispozici optické sítě nebo moderní 5G připojení pokrývající důležité veřejné prostory i úřady.

Naopak v menších městech a venkovských obcích často nalezneme pouze základní internetové připojení, někdy i s problémy v kvalitě či dostupnosti služby. Náročnější bezpečnostní technologie (například online přenos videa v HD rozlišení, SDI streamy, rychlá analytika v cloudu) proto nelze bez robustní sítě implementovat v plném rozsahu.

Do budování VHCN zasahují i dotační programy Evropské unie či státu, například projekty financované z Národního plánu obnovy nebo Modernizačního fondu. Tyto programy mohou pomáhat s rozvojem infrastruktury, stále ale hrají roli i technická, administrativní a rozpočtová omezení.

Velice důležité je si uvědomit, že vybudování sítě VHCN není samo sobě cílem, ale prostředkem, který umožňuje vstavení Služeb s přidanou hodnotou, VAS, právě nad robustní datovou komunikací.

2.3 Bariéry a omezení rozvoje

- **Finanční náročnost:** Moderní bezpečnostní technologie, komplexní kamerové systémy či chytrá varovná zařízení znamenají výraznou investici, kterou si menší obce často nemohou dovolit bez externích zdrojů.
- **Legislativa a ochrana osobních údajů:** Nařízení GDPR i národní legislativní rámec kladou přísné podmínky pro provozování sledovacích systémů. Zpracování osobních údajů, ukládání a sdílení záznamů i cílové využití dat musí být přesně vymezeno a správně zabezpečeno.
- **Technologická a personální náročnost:** Obce mnohdy postrádají potřebné know-how a odborný personál pro správu moderních chytrých systémů a datové infrastruktury. Provoz složitějších systémů proto často vyžaduje externí zajištění.
- **Odpor části veřejnosti:** Zvyšující se míra monitoringu je citlivým tématem a může vzbudit obavy o ztrátu soukromí. Bez kvalitní včasné komunikace a transparentnosti hrozí nesouhlas nebo nedůvěra obyvatel. **Je to především o komunikaci s obyvateli – musí vědět, jaké jsou přínosy, ale i omezení, které jim takové řešení nabídne.**
- **Nedostatečná dostupnost VHCN:** V některých oblastech, zejména v odlehlých částech republiky, stále není možné zajistit kvalitní, spolehlivé a rychlé datové spojení. Jedním z důvodů (z hlediska operátora) může být nedostatečný počet potenciálních uživatelů (zákazníků).

Shrnutí kapitoly:

Výchozí stav bezpečnostních řešení v českých obcích je často limitovaný jak možnostmi připojení, tak technologickým zázemím. Bez rozvoje VHCN a modernizace tradičních přístupů nelze naplno využít potenciál chytrých bezpečnostních systémů, které mohou zásadně zvýšit bezpečnost, informovanost i komfort občanů.

Přesto, a to je nutné zdůraznit, jsou taková řešení především limitována nedostatkem kvalifikované diskuse o přínosech, ale i případně i omezeních. Z tohoto důvodu byla tato analýza zpracována v rámci projektu BCO, jehož úkoly jsou i v oblasti popularizace a propagace vysokorychlostních komunikací.

3. Možnosti a přínosy chytrých bezpečnostních řešení

Moderní přístup k bezpečnosti obce se výrazně opírá o integraci digitálních technologií, jejichž funkčnost v plné míře umožňuje právě infrastruktura VHCN. Následující kapitola popisuje konkrétní digitální řešení, vazbu na síťovou infrastrukturu a prezentuje klíčové benefity – jak přímo finanční, tak společenské a provozní.

3.1 Přehled digitálních a chytrých bezpečnostních řešení

Mezi hlavní digitální bezpečnostní technologie, které mohou obce zavádět s oporou o moderní síť VHCN, patří zejména:



- **Chytré kamerové systémy s AI analýzou obrazu:**

Pokročilé kamery umí v reálném čase detekovat pohyb podezřelých osob, vozidel, vandalismus či podezřelé aktivity, automaticky rozpoznávat SPZ, vyhodnocovat davy a odesílat varování.

- **IoT senzory pro monitoring prostředí:**

Senzory detekující pohyb, otevření dveří, kouř, únik plynu, zvýšenou teplotu atd. Rychlé předávání dat umožňuje okamžité vyhodnocení a zásah.

- **Chytré veřejné osvětlení:**

Lze využít nejen pro zvýšení bezpečnosti v noci, ale také jako nosiče senzorů, kamer či reproduktorů pro hlášení.

- **Mobilní a webové aplikace pro hlášení mimořádných událostí a varování občanů:**

Aplikace umožňující rychlou komunikaci mezi občanem, samosprávou a složkami IZS, včetně funkce SOS tlačítka.

- **Elektronické sirény a hlásiče:**

Možné je centrálně spustit varování prostřednictvím pevné nebo mobilní sítě na základě automatického vyhodnocení události (požár, únik chemikálií, živelné události).

- **Propojení na složky IZS, městskou policii a další subjekty:**

Digitální systémy umožňují automatizovaný přenos dat při poplachu, sdílení obrazu a potřebných informací v reálném čase nejen pro obec, ale i navazující záchranné složky nebo pojišťovny.

3.2 Vazba těchto řešení na infrastrukturu VHCN

VHCN (Very High Capacity Networks) představuje základní předpoklad pro zavádění moderních, datově náročných bezpečnostních systémů. Jejich přínos spočívá především v:

- **Spolehlivém a rychlém přenosu velkých objemů dat** (HD video, kontinuální streamy, tisíce senzorických zpráv za den)

- **Nízké latenci:** nezbytné pro reálný čas – bez zpoždění ve vyhodnocení a reakci na incident
- **Možnosti cloudové analytiky a vzdáleného dohledu:**

Neomezený přístup k datům pro všechny potřebné aktéry, možnost rychlých zásahů na dálku.

- **Zajištění vysoké dostupnosti a kybernetického zabezpečení:**

Moderní VHCN podporují šifrování dat a redundantní připojení, čímž minimalizují riziko výpadků a útoků.

- **Možnosti integrace a rozšiřitelnosti:**

Infrastruktura umožňuje postupně zapojovat nové senzory, kamery nebo softwarové možnosti bez nutnosti zásadních stavebních úprav.

Tyto komponenty je ovšem třeba zpracovat do systému. Samy o sobě nemají velký přínos. A vytvoření systému je podmíněné definicí účelu, pro který chceme takovou službu (VAS) realizovat. Tedy definicí cílů a přínosů takového systému. Preferovaně měřitelných cílů a přínosů, ale přesto i tzv. „měkkých cílů“, kterými je např. komfort a spokojenost obvatel.

3.3 Hlavní benefity pro obecní rozpočet a obyvatele

Implementace chytrých bezpečnostních řešení s využitím VHCN přináší obcím zásadní finanční i nefinanční benefity:

- **Snížení přímých i nepřímých škod a nákladů:**

Rychlejší detekce a zásah při incidentu (krádež, požár, vandalismus) znamená menší materiální ztráty a nižší náklady na opravy.

- **Optimalizace práce městské policie a IZS:**

Díky přesnějším údajům dochází k efektivnějšímu nasazení hlídek a snížení zbytečných výjezdů.

- **Snížení pojistného občanů i obce:**

Pojišťovny často zohledňují vyšší bezpečnost a nižší četnost škod – vybavené obce mohou prokázat nižší rizikovost a získat výhodnější sazby.

- **Zvýšení atraktivity pro nové obyvatele a podnikatele:**

Bezpečná obec je vnímána jako vhodné místo k investicím i bydlení.

- **Zjednodušení administrativy a transparentnost:**

Digitální systémy umožňují jednodušší zpracování dat, reporting a vyhodnocení incidentů.

- **Efektivní komunikace s občany:**

Okamžité varování, rychlá informovanost, vyšší důvěra ve vedení obce.

3.4 Přímé a nepřímé finanční úspory

Přímé úspory:

- Snížené náklady na škody díky včasnému zásahu (méně oprav majetku, vozového parku, nižší náhrady za škody)
- Úspora na provozu a organizaci bezpečnostních služeb (vybavení, mzdy, pohonné hmoty díky cíleným zásahům)
- Možné snížení nákladů na pojistné pro obec i její občany (větší bezpečnost = nižší riziko = nižší pojistka)

Nepřímé úspory:

- Vyšší důvěra obyvatel a atraktivita obce vede k vyššímu zájmu o bydlení/investice (vyšší příjmy z daní)
- Omezení následných soudních sporů a negativních PR dopadů (efektivní předcházení krizím)
- Zvýšení hodnoty nemovitostí díky bezpečnějšímu prostředí

3.5 Bezpečnostní, provozní a společenské přínosy

- **Rychlejší a přesnější reakce na mimořádné události:**

Lepší napojení na složky IZS (policie, hasiči, zdravotníci) umožňuje okamžitě reagovat na incidenty i hromadné události.

- **Prevence kriminality a vyšší pocit bezpečí:**

Viditelné využívání moderních technologií může odrazovat od páchaní trestné činnosti a zvyšuje subjektivní pocit jistoty obyvatel.

- **Možnost evidence a analýzy incidentů:**

Data ze systémů slouží pro zpětnou analýzu a plánování preventivních opatření.

- **Efektivní komunikace s občany, včetně zranitelných skupin:**

Rychlá informovanost o nebezpečích i upozornění (“chytré varování”), možnost včasného zásahu (např. evakuace, uzavření lokalit).

- **Posílení image a prestiže obce:**

Moderní a transparentní přístup k bezpečnosti posiluje důvěru k samosprávě a zvyšuje pověst obce i navenek.

Shrnutí kapitoly:

Propojení chytrých bezpečnostních řešení s robustní VHCN umožňuje nejen zásadní zvýšení úrovně bezpečnosti a komfortu, ale generuje také konkrétní finanční i nefinanční benefity – od úspor na škodách a pojistném až po posílení komunitního života a důvěry v obecní správu. Klíčovou podmínkou je dostupnost a kvalita datové infrastruktury i komplexní přístup ke správě dat a komunikaci s občany.

4. Rizika a potenciální nevýhody implementace

Zavádění moderních bezpečnostních systémů přináší řadu výhod, avšak obcím je třeba věnovat pozornost také možným rizikům a nevýhodám, které s sebou nese nejen samotná technologie, ale i provozní či legislativní rámec.

4.1 Investiční a provozní náročnost

- **Vysoké počáteční investice:**

Pořízení chytrých kamerových systémů, IoT senzorů, specializovaného softwaru a budování či rozšiřování VHCN je finančně náročné. Návratnost těchto investic se může projevit až ve střednědobém nebo dlouhodobém horizontu.

- **Náklady na údržbu a obnovu:**

Technologické vybavení vyžaduje pravidelný servis, kalibrace, obměny a aktualizace softwaru. S růstem složitosti systémů stoupají i požadavky na kvalifikovaný personál či externí správu.

- **Skryté provozní náklady:**

Datové přenosy, licence software, cloudové služby či kyberbezpečnostní opatření znamenají další zatížení obecního rozpočtu, na které je třeba pamatovat již při plánování.

4.2 Provozní a technologická rizika

- **Výpadky systémů:**

Nespolehlivá infrastruktura, špatný signál nebo napájení mohou znamenat nedostupnost služeb v kritickém okamžiku. Výpadky síťového připojení (např. při silném větru, výpadku proudu) mohou znemožnit přenos dat mezi senzory a dispečinkem.

- **Kybernetické hrozby:**

Chytrá infrastruktura může být cílem hackerských útoků, pokusu o manipulaci s daty, narušení soukromí či zneužití citlivých informací o pohybu osob. Případy ransomwaru, phishingu nebo přímých útoků na kamerové systémy nejsou v Evropě ojedinělé.

- **Poruchy a chybovost technologií:**

Falešné poplachy, nefunkční senzory či špatně kalibrované detektory mohou vést k nesprávným reakcím bezpečnostních složek, případně k otupění pozornosti (tzv. „alarm fatigue“).

- **Neúplná integrace:**

Ne vždy je možné chytrá zařízení plně integrovat se stávajícími systémy městské policie, hasičů nebo složek IZS. Nekompatibilita softwaru či rozdílné standardy mohou omezit funkčnost a snižovat přínos investice.

4.3 Závislost na dodavatelích, technologiích a otázky ochrany soukromí

- **Dodavatelská závislost (vendor lock-in):**

Výběr jednoho hlavního dodavatele znamená riziko složitého a nákladného přechodu na jiný systém v budoucnu, případně problémy v případě ukončení činnosti poskytovatele nebo změny obchodních podmínek.

- **Proprietární řešení a uzavřená data:**

Některé technologie používají nekompatibilní formáty nebo uzavírají data do proprietárního systému, což ztěžuje možnost napojení na další systémy, migraci nebo sdílení dat s partnery a institucemi.

- **Etické a právní aspekty ochrany osobních údajů:**

Chytré kamery a monitoring veřejného prostoru mohou vyvolat obavy o ochranu soukromí (zejména dle GDPR). Občané mohou vnímat nárůst monitorování negativně, což vede ke snížení důvěry v samosprávu a riziku občanské nespokojenosti.

- **Legislativní nejistota:**

Výklad a aplikace zákonů vztahujících se k monitorovacím technologiím, uchovávání a sdílení dat se mohou měnit, což zvyšuje právní nejistotu a potenciální rizika postihu za nesouhlasný provoz.

Shrnutí kapitoly:

Rizika spojená s implementací chytrých bezpečnostních řešení je potřeba zvažovat souběžně s jejich přínosy. Nedostatečná příprava, podcenění ochrany dat či nadhodnocení nasazovaných technologií může vést ke zbytečným nákladům, neefektivitě i ztrátě důvěry občanů. Včasná a otevřená komunikace, odborná příprava projektu a pečlivý výběr partnerů a řešení jsou nezbytné pro úspěšné a udržitelné zavádění těchto systémů.

S ohledem na již výše uvedené, je třeba otevřená a technicky podložená komunikace s občany. Musí si být jisti tím, co jsou přínosy, co omezení a musí vzniknout konsenzus. Je dobré připomenout, že doba postupuje a přináší nová řešení, nové postupy a není zřejmě nejlepším přístupem je pouze ignorovat a apriorně odmítat.

5. SWOT analýza (bezpečnostní management s využitím VHCN v obci)

5.1 Silné stránky

- **Reálné zvýšení bezpečnosti občanů a majetku** – rychlá detekce incidentů, okamžité předávání informací složkám IZS, efektivnější zásahy.
- **Možnost propojení systémů** – integrace kamer, senzorů, varovných systémů a komunikace s policií, hasiči a dalšími institucemi.
- **Vysoká kvalita a rychlost přenosu dat díky VHCN** – podpora HD video streamů, analytiky v reálném čase a vzdáleného dohledu.

- **Zrychlení reakčních časů** – automatizace varovných systémů znamená dřívější zásah a omezení škod.
- **Možné snížení pojistného** – prokazatelně bezpečnější prostředí může vést k výhodnějším pojistným podmínkám pro obec i občany.
- **Vyšší transparentnost a důvěra občanů** – dokumentace incidentů, možnost sdílení dat s veřejností, zvýšení otevřenosti samosprávy.
- **Možnost využití dotací a programů EU** – např. z Národního plánu obnovy, modernizačního fondu, podpory Evropské komise pro rozvoj VHCN.

5.2 Slabé stránky

- **Vysoké počáteční investiční náklady** na technologie a infrastrukturu.
- **Závislost na dostupnosti a kvalitě VHCN** – v některých lokalitách omezené možnosti implementace.
- **Nároky na údržbu, provoz a odborný personál.**
- **Možné provozní komplikace** – poruchy zařízení, potřeba pravidelných aktualizací a servisu.
- **Obavy občanů z narušeného soukromí** – nedůvěra vůči novým technologiím, nutnost kvalitní osvěty.
- **Komplikovaná legislativa a složitá implementace GDPR.**

5.3 Příležitosti

- **Propojení s pojišťovnami a možnost vyjednání výhodnějších pojistných podmínek** (nižší rizikovost znamená nižší sazby).
- **Rozvoj spolupráce s městskou policií, hasiči a složkami IZS** – efektivnější prevence, rychlejší zásah.
- **Možnost rozšíření systému na další oblasti Smart City** – například inteligentní doprava, energetický management, krizové řízení.
- **Využití datové analytiky** – prediktivní modely kriminality, prevence úrazů nebo havárií na základě dat.
- **Získání důležitých zkušeností a image inovativní obce** – lepší postavení při získávání dalších dotací a partnerství.
- **Zapojení občanů do systému bezpečnostních varování** – vyšší míra participace a spolupráce.

5.4 Hrozby

- **Riziko kybernetických útoků a narušení bezpečnosti systémů** – nutnost zajištění vysoké úrovně ochrany dat.
- **Technologická závislost na jednom dodavateli (vendor lock-in)** – obtížná a drahá změna řešení v budoucnu.

- **Rychlé zastarávání technologií** – potřeba pravidelných investic do obnovy systému.
- **Možná změna legislativy či zpřísnění pravidel ochrany osobních údajů** – zvýšení administrativní a právní zátěže.
- **Odpor části veřejnosti vůči monitorování** – snížení důvěry nebo aktivní odpor proti novým technologiím.
- **Potíže s financováním dalšího provozu a rozvoje** – závislost na důsledném plánování a schopnosti čerpat externí zdroje.

Shrnutí kapitoly:

SWOT analýza dokládá, že zapojení sítí VHCN do bezpečnostního managementu obce přináší významné benefity, ale zároveň vyžaduje promyšlené řízení rizik, transparentní komunikaci s občany a pečlivou finanční i technickou přípravu.

6. Možné finanční a rozpočtové modely pro obce

Nasazení chytrých bezpečnostních řešení s využitím sítí VHCN představuje významnou investici, která však při správném nastavení financování a řízení může být dlouhodobě výhodná jak pro obec, tak její obyvatele. Kromě přímé úspory na škodách lze s partnerstvím pojišťoven dosáhnout i snížení pojistného, což je inovativní prvek v oblasti rozpočtového plánování samospráv. Tato kapitola popisuje varianty financování, dopady na rozpočet a nabízí modelový příklad návratnosti investice.

Při čtení této analýzy je dobré si uvědomit, že bezpečnost v obcích není jedinou VAS, kterou mohou její občané využívat. A pokud budeme uvažovat více různých VAS (další analýzy projekt BCO již připravil a bude zřejmě dále připravovat), pak sdílení nákladů na tokové služby je jednou z věcí, které ve finančních úvahách musíme vzít v potaz.



6.1 Varianty financování (dotace, vlastní rozpočet, partnerství, pojišťovny)

Obce mají na výběr z několika přístupů k financování:

- **Dotační programy (EU, stát):**

- Modernizační fond, Národní plán obnovy, IROP a další poskytují podporu na rozvoj VHCN i na nasazení bezpečnostních technologií.
 - Výhodou je vyšší možnost hrazení vstupních nákladů, nevýhodou administrativní náročnost a nutnost splnit specifické podmínky.
- **Vlastní rozpočtové prostředky:**
 - Přímé financování z obecního rozpočtu, případně postupné investování.
 - Vhodné pro menší projekty nebo dofinancování větší investice.
- **Public-Private Partnership (PPP):**
 - Partnerství s komerčními subjekty nebo telekomunikačními firmami umožňuje rozdělení investičního rizika, přístup k inovativním technologiím a případně sdílení nákladů na provoz.
- **Participace pojišťoven:**
 - Při prokázání významného snížení kriminality a výskytu škod lze s pojišťovnami vyjednat zapojení do financování technologií, případně garantované snížení pojistného (příklad: kamerový systém, chytré varování – nižší pojistné pro obec i občany).
- **Oborové a regionální granty:**
 - Často zaměřeny na konkrétní pilotní projekty, inovace či bezpečnostní preventivní programy v obcích.
- **Crowdfunding, participativní rozpočty:**
 - U vybraných projektů je možné zapojit občany – ať už finančně, nebo hlasováním (“Bezpečnější čtvrť prostřednictvím kamer financované z participativního rozpočtu”).

6.2 Přímé a dlouhodobé rozpočtové dopady

Přímé náklady:

- Počáteční investice do infrastruktury a zařízení (kamery, senzory, servery, software, rozšíření sítě)
- Provozní náklady (servis, správa systému, školení personálu, datové služby)

Dlouhodobé úspory:

- Snížení počtu škod a nižší výplaty pojistných událostí
- Snížené pojistné díky prokázanému poklesu rizika (např. až o 10–20 % v některých oblastech při pilotních projektech)
- Efektivnější práce městské policie a integrovaného záchranného systému (nižší provozní náklady)
- Vyšší příjmy v důsledku zvyšující se atraktivity obce (noví obyvatelé, firmy)

Dopad na občany:

- Možnost snížení individuálního pojistného na majetek díky vyšší ochraně nemovitostí a veřejného prostoru

6.3 Ukázkový model návratnosti investice

Níže je hypotetický model pro středně velkou obec (5 000 obyvatel):

Tabulka modelu

Položka	Investice (tis. Kč)	Rok 1 (tis Kč)	Rok 2 (tis Kč)	Rok 3 (tis Kč)	Rok 4 (tis Kč)	Rok 5 (tis Kč)	Poznámka
Počáteční investice (VHCN, technologie)	4 000						Investice
Provoz a správa systému		500	500	500	500	500	
Odhadovaná úspora na škodách		800	800	800	800	800	Méně vandalismu, krádeží
Snížení pojistného (obec + občané)		400	400	400	400	400	Méně rizikové pojištění
Efektivnější činnost bezpečnostních složek		200	200	200	200	200	Úspora nákladů
Celkové roční úspory		1 400	1 400	1 400	1 400	1 400	
Roční CashFlow	-4 000	900	900	900	900	900	
Kumulované CashFlow	-4 000	-3 100	-2 200	-1 300	-400	500	

Návratnost investice:

Celková roční úspora 1,4 mil. Kč oproti ročnímu nákladu (podíl investice na jeden z pěti roků + roční provozní náklady) znamená návratnost při započtení dlouhodobých přínosů během 4–5 let. Po této době se realizované úspory i zvýšené příjmy již pozitivně promítají do obecního rozpočtu (resp. do nákladů fyzických a právnických osob, které jsou v systému zapojeny).

Takový model zároveň ukazuje, že přímé finanční úspory lze doplnit i o tzv. nefinanční benefity – lepší pověst obce, spokojenost obyvatel, méně stresu z kriminality či živelních událostí.

Shrnutí kapitoly:

Možnosti financování zavedení chytrých bezpečnostních řešení díky VHCN jsou široké – od dotačních programů, přes PPP, až po jednání s pojišťovnami a participaci občanů. Klíčové je vnímat investici do bezpečnosti jako dlouhodobě návratnou, s významným provozním a společenským efektem.

7. Příklady z praxe

Digitální bezpečnostní řešení propojená s VHCN již fungují v řadě obcí a měst v ČR i v zahraničí. Následující příklady ilustrují rozmanitost použitých technologií, zapojení komunit i konkrétní benefity — od rychlého varování po úspory pojistného.

7.1 Konkrétní případy z ČR a zahraničí

7.1.1 Smart City projekty v Písku a jejich přínos v oblasti bezpečnosti

Písek patří mezi průkopníky konceptu Smart City v České republice a realizuje řadu projektů, které mají přímý i nepřímý dopad na bezpečnost ve městě. Níže jsou shrnuty klíčové prvky a konkrétní opatření týkající se bezpečnosti:

Inteligentní senzory a kamerové systémy

- **Veřejné osvětlení s čidly:** Při výměně starých žárovek za LED technologie jsou sloupky veřejného osvětlení vybavovány chytrými senzory. Tyto senzory mohou monitorovat pohyb, zaznamenávat dopravní situace, sledovat kvalitu ovzduší a přispívat k bezpečnosti v ulicích například detekcí neobvyklých událostí nebo pohybu v nočních hodinách.
- **Kamerové systémy:** Moderní kamery ve městě jsou schopné nejen klasického monitoringu, ale i pokročilých funkcí, jako je čtení SPZ vozidel nebo analýza pohybu osob. Tyto systémy mohou pomoci při prevenci kriminality, rychlém zásahu v případě incidentů a efektivnějším vyšetřování přestupků nebo nehod.
- **Internet věcí (IoT):** Vybudovaná síť LoRaWAN umožňuje připojení různých senzorů a zařízení, která mohou monitorovat různé aspekty městského života, včetně bezpečnosti. Data jsou centralizována a analyzována v datovém centru, což umožňuje rychlejší reakce na krizové situace, například v případě požáru, nehody nebo jiných mimořádných událostí.

Integrace dat a spolupráce se složkami IZS

- **Sdílení dat se záchrannými složkami:** Informace získané ze senzorů a kamer jsou k dispozici nejen správě města, ale i složkám integrovaného záchranného systému (hasiči, policie, zdravotnická záchranná služba). To umožňuje rychlejší zásahy a lepší koordinaci v krizových situacích.
- **Centrální správa dat:** Město využívá cloudovou platformu a moderní informační systémy pro správu a vyhodnocování dat, což zvyšuje efektivitu a transparentnost řízení bezpečnostních opatření.

Další prvky zvyšující bezpečnost

- **Chytré parkování:** Systémy monitorující parkovací místa nejen zvyšují komfort, ale i bezpečnost v dopravě, protože snižují riziko nelegálního parkování a chaosu v ulicích.
- **Inteligentní budovy:** Budovy vybavené senzory mohou včas detekovat požáry, úniky vody či plynu a další potenciálně nebezpečné situace, což přispívá k ochraně obyvatel i majetku.

Rizika a otázky ochrany soukromí

- **Centrální správa a monitoring:** Některé zdroje upozorňují na rizika spojená s rozsáhlým monitoringem a shromažďováním dat o obyvatelích. Moderní kamerové systémy a senzory mohou vést k pocitu ztráty soukromí a obavám z možného zneužití dat. Město i jeho partneři proto musí dbát na dodržování platné legislativy a ochranu osobních údajů.



Shrnutí

Projekty Smart City v Písku přinášejí v oblasti bezpečnosti zejména:

- Rozšíření a modernizaci kamerových a senzorických systémů ve veřejném prostoru.
- Možnost rychlého sdílení a vyhodnocování dat pro efektivnější zásahy složek IZS.
- Zvýšení bezpečnosti dopravy a veřejných budov díky chytrým technologiím.
- Důraz na kybernetickou bezpečnost a ochranu osobních údajů v souvislosti s centralizací dat.

Město Písek tak systematicky využívá moderní technologie ke zvýšení bezpečnosti, ale zároveň čelí výzvam v oblasti ochrany soukromí a transparentnosti správy dat.

7.1.2 Smart City projekty v Amsterdamu a jejich přínos v oblasti bezpečnosti

Amsterdam patří mezi evropské lídry v oblasti chytrých měst a bezpečnost občanů je jednou z klíčových oblastí jeho Smart City strategie. Město realizuje řadu inovativních projektů, které využívají digitální technologie k prevenci rizik, ochraně veřejného prostoru a posílení pocitu bezpečí obyvatel i návštěvníků.

Jedním z hlavních projektů je **Safe Smart (Digital) City Area**, který funguje jako „živá laboratoř“ v několika částech města. V těchto zónách je budována digitální infrastruktura propojující síť, chytrá zařízení a sběr dat podle potřeb místních obyvatel. Cílem je vytvořit prostředí, které je bezpečné nejen fyzicky, ale i z pohledu kybernetické bezpečnosti a ochrany soukromí. Město spolupracuje s etickými hackery, kteří testují odolnost systémů proti neoprávněnému přístupu a navrhuji opatření pro prevenci zneužití dat nebo technologií. Tím Amsterdam aktivně předchází rizikům, jako je zneužití kamer, ovládnutí infrastruktury třetími stranami nebo únik citlivých informací¹.

Velkou pozornost věnuje Amsterdam také **monitoringu pohybu osob a davů**. Systém Public Eye využívá stávající městské kamery a umělou inteligenci pro sledování a predikci velikosti, hustoty a pohybu davů v reálném čase. Tento systém pomáhá předcházet

nebezpečným situacím, jako je přelidnění, riziko násilí nebo nehody (například pády do kanálů). Pokud v některé oblasti dojde k nadměrnému shromáždění lidí, mohou pracovníci města včas přijmout opatření – například zavést jednosměrný pohyb, informovat veřejnost prostřednictvím aplikací či digitálních kiosků a v dlouhodobém horizontu upravit urbanistické řešení daného prostoru. Systém byl využit i během pandemie k zajištění rozestupů a bezpečnosti na veřejných místech.

Dalšími prvky jsou **dynamické veřejné osvětlení** a **inteligentní dopravní systémy**, které v reálném čase reagují na přítomnost chodců či cyklistů a zvyšují bezpečnost v ulicích, například zesílením osvětlení v rizikových situacích nebo optimalizací dopravy pro záchranné složky.

Amsterdam klade důraz na **etiku a ochranu soukromí** – například u kamerových systémů je veřejně vysvětlováno, jak data fungují, a testují se technologie jako „shuttercam“, kde mohou občané dočasně vypnout kameru nebo se z monitoringu odhlásit.

Celkově lze říci, že Amsterdam kombinuje špičkové technologie s participací občanů a důrazem na etiku, aby vytvořil bezpečné, otevřené a důvěryhodné městské prostředí, které je vzorem pro další evropská města.



Shrnutí kapitoly:

Příklady z ČR i zahraničí ukazují, že díky VHCN a chytrým bezpečnostním řešením lze nejen zvyšovat ochranu obyvatel a majetku, ale i reálně snižovat náklady na pojištění a zefektivňovat práci složek IZS. Klíčová je vždy kvalitní infrastruktura, propojenost systémů a aktivní spolupráce mezi městem, občany i pojišťovnami.

8. Doporučení a další kroky pro obce

Závěrečná kapitola nabízí soubor praktických doporučení, jak mohou obce postupovat při plánování, zavádění a provozování chytrých bezpečnostních řešení s využitím sítí VHCN. Důraz je kladen na strategii, zapojení veřejnosti, spolupráci s partnery a systematické vyhodnocování přínosů i rizik.

8.1 Strategická doporučení

- **Vytvořit dlouhodobou bezpečnostní strategii obce**

Jasně definujte cíle v oblasti bezpečnosti, zmapujte potřeby území, vytipujte prioritní lokality a určete odpovědné osoby.

- **Plánovat zavádění technologií ve fázích**

Začněte pilotním projektem v nejrizikovější lokalitě, následně rozšiřujte dle vyhodnocených výsledků a zkušeností.

- **Posoudit a pravidelně aktualizovat rizika**

Zahrňte kybernetickou bezpečnost, ochranu dat a legislativní požadavky již od začátku plánování.

- **Zajistit maximální transparentnost postupu**

Průběžně informujte občany o záměru, přínosech i rizicích, vysvětľujte ochranu soukromí a smysl opatření.

8.2 Praktické kroky k zavedení

- **Provedte audit stávající infrastruktury**

Zjistěte úroveň pokrytí VHCN, stav současných kamer, senzorů či rozhlasu.

- **Identifikujte vhodné technologie, které lze nasadit**

Výběr kamerových systémů s AI, IoT senzorů, mobilních aplikací – dle potřeb a finančních možností obce.

- **Naplánujte rozpočet a hledání financí**

Využijte dotační programy, zapojte pojišťovny, popřemýšlejte o PPP nebo participativních projektech.

- **Zajistěte školení pracovníků a zapojte odborníky**

Pravidelně vzdělávejte osoby zodpovědné za provoz systémů včetně základů datové bezpečnosti.

- **Připravte plán komunikace s občany**

Spusťte osvětovou kampaň o přínosech, ochraně dat i možnostech zapojení obyvatel (např. hlášení incidentů).

8.3 Spolupráce a zapojení partnerů

- **Navazujte partnerství s telekomunikačními společnostmi**

Zajistěte stabilní připojení a průběžný rozvoj VHCN infrastruktury.

- **Jednejte s pojišťovnami o zvýhodněném pojistném**

Prokažte reálné dopady na bezpečnost, nabídněte spolupráci při vyhodnocování úspor.

- **Spolupracujte se složkami IZS a dalšími institucemi**

Zapojte do projektu městskou policii, hasiče a zdravotníky – sdílejte data, vytvářejte společné postupy.

- **Nezapomeňte na občany – stakeholders**

Založte pracovní skupiny (např. s dobrovolníky nebo seniory), sbírejte zpětnou vazbu a aktivně dohlížejte na respektování soukromí.

8.4 Sledování a vyhodnocování výsledků

- **Stanovte měřitelné cíle a indikátory úspěchu (KPI)**

Např. snížení počtu krádeží, rychlost zásahu, snížení pojistného, úroveň spokojenosti občanů.

- **Pravidelně vyhodnocujte funkčnost systému**

Sledujte statistiky, analyzujte incidenty a využití technologií.

- **Zajišťujte pravidelnou aktualizaci systémů**

Vyhnete se zastarávání technologií, sledujte nové trendy a reagujte na aktuální bezpečnostní hrozby.

8.5 Shrnutí

Efektivní zavádění chytrých bezpečnostních řešení s využitím sítí VHCN znamená pro obec nejen vyšší úroveň bezpečnosti, ale také dlouhodobé finanční i společenské přínosy. Klíčové je plánovat systematicky, zapojovat občany a partnery, vyhodnocovat dopady a nezanedbávat oblast kybernetické a datové bezpečnosti.

Doporučujeme obcím začít s prvním krokem co nejdříve: vytipovat klíčové cíle a potřeby a navázat kontakty s možnými partnery – cesta k bezpečnější, moderní a otevřeně obci je totiž dlouhodobým, ale užitečným procesem.

9. Závěr

Zavádění chytrých bezpečnostních řešení v obci s využitím sítí VHCN představuje významný posun směrem k modernímu, efektivnímu a proaktivnímu zajištění bezpečnosti občanů i majetku. Tento dokument prokázal, že propojení digitálních technologií s robustní datovou infrastrukturou přináší nejen přímé snížení bezpečnostních rizik, ale také celou škálu provozních, finančních a společenských přínosů.

Hlavní poznatky z předchozích kapitol lze shrnout takto:

- **Bezpečnost v obci je komplexní téma**, které vyžaduje propojení tradičních metod s nejmodernějšími digitálními nástroji a datovou infrastrukturou.
- **Sítě VHCN jsou klíčovým předpokladem** pro úspěšné zavádění pokročilých bezpečnostních technologií, umožňujících rychlý přenos dat, analytiku v reálném čase a propojení různých systémů.
- **Chytrá řešení výrazně zvyšují efektivitu, transparentnost a preventivní působení** – obce mohou lépe reagovat na mimořádné události, oslovit občany i optimalizovat provoz.
- **Financování těchto projektů je možné kombinovat z více zdrojů**, přičemž důležitou roli hrají nejen dotace a veřejné rozpočty, ale také pojišťovny, PPP projekty či participace občanů.
- **Zkušenosti z praxe v Česku i zahraničí ukazují, že investice do bezpečnosti se vrací**, ať už v podobě nižší kriminality, spokojenějších obyvatel nebo úspor na pojistném i provozu.
- **Společenská poptávka po řešení takovéto VAS** – musí vzniknout na základě informovaného konsenzu občanů obce (tedy včetně všech dalších, např. ekonomických entit v obci)

Je však nutné nezanedbat možná rizika a bariéry, zejména v oblasti ochrany soukromí, kybernetické bezpečnosti, nutnosti průběžné aktualizace systémů a pečlivého plánování financování i provozu. Klíčovým faktorem je zapojení všech relevantních aktérů – od vedení obce přes složky IZS až po samotné občany, jejichž důvěra a spolupráce jsou nepostradatelné.

A ještě jedno doporučení – jakýkoliv externí dodavatel, poradce pro zavedení jakékoliv Služby s přidanou hodnotou (VAS) je sice v daném okamžiku zdánlivě rychlým a proveditelným řešením

Závěrem lze konstatovat, že cesta k bezpečnější a modernější obci začíná kvalitní analýzou potřeb, otevřenou komunikací a postupným, systematickým rozvojem digitální infrastruktury i bezpečnostní kultury. Proaktivní přístup k implementaci chytrých řešení je nejen odpovědností vůči občanům, ale také strategickou investicí do budoucnosti celé komunity.

Leták

Chytrá bezpečnost v obcích s využitím VHCN

Bezpečnost patří mezi klíčové faktory kvality života v obcích. Moderní bezpečnostní řešení již překračují rámec tradiční městské policie či základních kamerových systémů a stále více se opírají o digitalizaci a vysokorychlostní datové sítě nové generace (VHCN). Tyto sítě umožňují nejen efektivní přenos dat z kamer a senzorů v reálném čase, ale také integraci různých bezpečnostních technologií a rychlou komunikaci mezi obecními složkami, složkami IZS i občany.

Přínosy chytrých bezpečnostních řešení

Implementace digitálních technologií (chytré kamerové systémy s AI, IoT senzory, mobilní aplikace pro varování občanů, elektronické sirény aj.) přináší obcím řadu výhod:

- Rychlejší a přesnější reakce na incidenty, snížení škod a optimalizace práce bezpečnostních složek.
- Možnost snížení pojistného díky prokazatelně nižšímu riziku.
- Zvýšení atraktivity obce pro obyvatele i podnikatele, vyšší transparentnost a důvěra občanů.
- Efektivnější komunikace s občany a lepší ochrana zranitelných skupin.

Rizika a omezení

Zavádění těchto systémů je spojeno s vysokými počátečními investicemi, nároky na údržbu a odborný personál, provozními a technologickými riziky (výpadky, kybernetické hrozby, neúplná integrace). Významnou výzvou je také ochrana osobních údajů, legislativní nejistota a odpor části veřejnosti z obav o soukromí. Důležitým faktorem úspěchu je proto transparentní komunikace, zapojení občanů a pečlivé plánování.



Příklady z praxe

Města jako Písek či Amsterdam ukazují, že chytrá bezpečnostní řešení propojená s VHCN vedou k efektivnějším zásahům, lepší prevenci kriminality a vyšší spokojenosti obyvatel. Zároveň však potvrzují potřebu důsledné ochrany dat a etického přístupu k monitoringu veřejného prostoru.

Závěr

Chytrá bezpečnostní řešení s využitím VHCN představují strategickou investici do budoucnosti obce. Přinášejí vyšší bezpečnost, efektivitu a důvěru, ale vyžadují systematický přístup, otevřenou komunikaci a důsledné řízení rizik.

10. Literatura a zdroje

A. Základní a odborná literatura

Ministerstvo vnitra ČR.

Prevence kriminality na regionální a lokální úrovni

[Prevence kriminality na regionální a lokální úrovni - Ministerstvo vnitra České republiky](#)

Ministerstvo vnitra ČR.

Koncepce prevence kriminality na léta 2022 až 2027. Praha: MVČR, 2022.

Dostupné z:

<https://www.mvcr.cz/soubor/koncepce-prevence-kriminality-2022-2027-pdf.aspx>

Zákon č. 128/2000 Sb., o obcích (obecní zřízení).

Zákony pro lidi.

Dostupné z:

<https://www.zakonyprolidi.cz/cs/2000-128>

B. Oficiální metodiky, doporučení a právní normy

Ministerstvo vnitra ČR.

Metodika tvorby a realizace místních koncepcí prevence kriminality. Praha: MVČR, 2021.

Dostupné z:

<https://www.mvcr.cz/clanek/metodiky-a-prirucky-z-oblasti-prevence-kriminality.aspx>

Úřad vlády ČR

Strategie bezpečnosti ČR 2023–2030. Praha: Úřad vlády, 2023.

Dostupné z:

<https://www.vlada.cz/assets/media-centrum/aktualne/Strategie-bezpecnosti-2023-2030.pdf>

C. Příklady a případové studie

Oficiální stránky města Písek – Smart Písek

Město Písek. Smart Písek – Město Písek. Dostupné z:

<https://www.mesto-pisek.cz/smart-pisek/ds-15031>

Strategický dokument „Modrožlutá kniha Smart Písek“ (PDF)

Město Písek. Modrožlutá kniha Smart Písek. Dostupné z:

https://www.mesto-pisek.cz/assets/File.ashx?id_org=12075&id_dokumenty=53122

RISJK – Písek má ambici i potenciál stát se nejchytřejším městem v ČR

RISJK. Písek má ambici i potenciál stát se nejchytřejším městem v ČR. Dostupné z:

<https://www.risjk.cz/aktuality/pisek-ma-ambici-i-potencial-stat-se-nejchytrejsim-mestem-v-cr.html3>

Hospodářské noviny – Město Písek rozvíjí chytrá řešení, nově se spojilo s ČD Telematikou a Technologickým centrem Písek

Hospodářské noviny. Město Písek rozvíjí chytrá řešení, nově se spojilo s ČD. Dostupné z:

<https://hn.cz/c1-65892740-mesto-pisek-rozviji-chytra-reseni-nove-se-spojilo-s-cd-telematikou-a-technologickym-centrem-pisek4>

Oficiální web Smart Písek – O Smart City

Smart Písek. O Smart City – Smart Písek. Dostupné z:

<https://smart.pisek.eu/scp/o-projektu.html5>

Přehled činností Smart Písek (PDF)

Město Písek. Přehled činností Smart Písek. Dostupné z:

https://www.mupisek.cz/assets/File.ashx?id_org=12075&id_dokumenty=368799

Písecký svět – Smart City: Naše radostná budoucnost? (kritický pohled na bezpečnost a ochranu soukromí)

Písecký svět. Smart City – Naše radostná budoucnost? Dostupné z:

<http://www.piseckysvet.cz/pisecky-hydepark/nase-radostna-budoucnost>

Tienkamp, R. (2021). Following the crowd: Amsterdam's smart city solution. Euronews.

Popisuje projekt Public Eye, který využívá kamery, senzory a AI pro monitoring davů v reálném čase a řízení bezpečnosti na veřejných prostranstvích. Důraz je kladen na ochranu soukromí a transparentní zpracování dat.

Dostupné z:

<https://www.euronews.com/business/2021/08/27/following-the-crowd-amsterdam-s-smart-city-solution 5>

van Zoonen, L. (2019). People's strategies for perceived surveillance in Amsterdam Smart City. Urban Geography, 40(9), 1290–1308.

Analýza vnímání dohledu a bezpečnostních opatření v rámci chytrého města Amsterdam z pohledu občanů.

Dostupné z:

<https://www.tandfonline.com/doi/full/10.1080/02723638.2019.1614369 1>

Boenink, M., & Kudina, O. (2023). When 'doing ethics' meets public procurement of smart city technology. IASDR 2023 Conference Proceedings.

Studie etických aspektů a ochrany soukromí při zavádění kamerových a senzorových systémů v Amsterdamu, včetně participace občanů na rozhodování o bezpečnostních technologiích.

Dostupné z:

<https://dl.designresearchsociety.org/cgi/viewcontent.cgi?article=1221&context=iasdr 2>

Bee Smart City (2022). Amsterdam Smart City: A World Leader in Smart City Development.

Přehled chytrých řešení v Amsterdamu včetně bezpečnostních iniciativ a zapojení

občanů do tvorby bezpečnějšího městského prostředí.

Dostupné z:

<https://www.beesmart.city/en/smart-city-blog/smart-city-portrait-amsterdam-3>

CITEGO (2017). Amsterdam Smart City: the creation of new partnerships for a smart city.

Popisuje vznik a rozvoj platformy Amsterdam Smart City, včetně pilotních projektů zaměřených na bezpečnost a spolupráci různých aktérů města.

Dostupné z:

https://www.citego.org/bdf_fiche-document-883_en.html

D. Další zdroje a inspirace

Ministerstvo vnitra ČR

Mapy kriminality: Online nástroj pro veřejnost.

Dostupné z:

<https://kriminalita.policie.cz>

Czech Smart City Cluster.

Přehled chytrých řešení v oblasti bezpečnosti.

Dostupné z:

<https://www.czechsmartcitycluster.cz/bezpecnost/>