



TechForum 2026

Jak zvládnout kyberzákon i AI s nadhledem



Digitální transformace jednoho města Smart City a kybernetická bezpečnost

Jan Hofman, Metropolnet, a.s. , Statutární město Ústí nad Labem

O nás

Město Ústí nad Labem

- ^ 90 000 obyvatel, Ústecký kraj, Česká republika
- ^ Strategická poloha: soutok Labe a Bíliny
- ^ Vybrán v soutěži "5G pro 5 měst" v roce 2019
- ^ Příjemce dotací EU: NPO, IROP, URBACT
- ^ Pořadatel Fóra pro města 2026 – sdílení dobré praxe



Metropolnet, a.s.

- ^ 100% vlastněná ICT společnost města
- ^ Provozovatel městské privátní optické sítě
- ^ Systémový integrátor 5G smart city projektů
- ^ Certifikace ISO 27001:2022 (kyberbezpečnost)
- ^ Technický dozor, projektový manažer a správce dotací

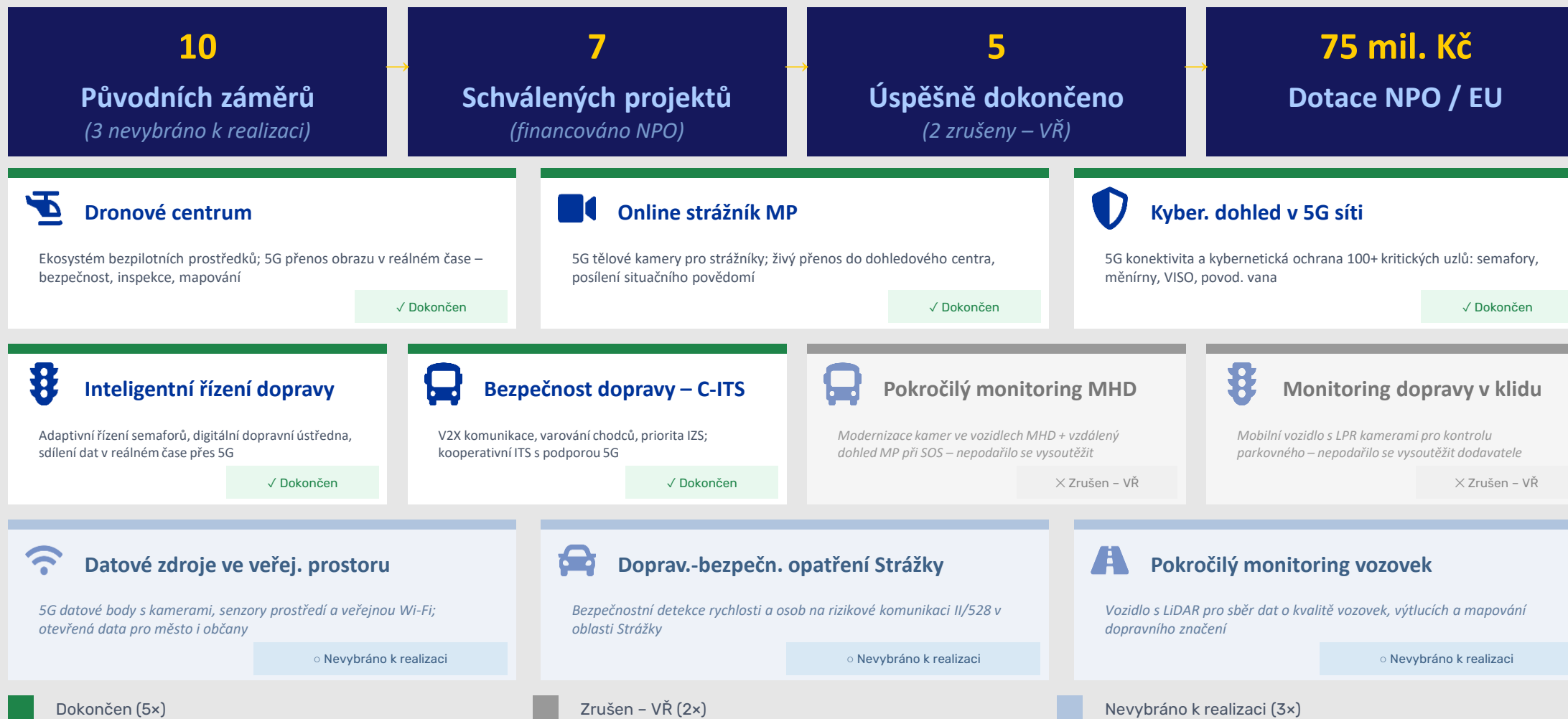


Naše cesta k 5G

od pilotního města k vzoru dobré praxe v 5G



Portfolio 5G projektů



5G projekty v detailu



Dronové centrum Ústí nad Labem

- Flotila UAV pro monitorování akcí, dopravy a majetku města
- 5G umožňuje přenos videa 4K v reálném čase na dispečink
- Podpora krizového řízení, inspekce zeleně a bezpečnosti
- První municipální dronové centrum svého druhu v ČR
- První spolupráce s IZS/HZS 09/26



Online strážník MP

- 5G přenosné kamery pro všechny strážníky ve službě
- Přímý videostream na operační středisko – nulová latence
- Vzdálená velitelská podpora a digitální záznam důkazů
- Zvýšení bezpečnosti strážníků i důvěry občanů
- OS MP Nivy



Kyber. dohled v 5G síti

- Ochrana koncových bodů 100+ kritických uzlů infrastruktury
- Pokrývá: semaforey, měnirny DPmÚL, povodňovou vanu, VISO
- Kontinuální detekce anomálií přes 5G datový spoj
- Základ NIS2 strategie kybernetické odolnosti města
- Bezpečnostní monitoring



Inteligentní řízení dopravy + C-ITS

- 5G adaptivní řízení semaforů na celé silniční síti města
- C-ITS: komunikace vozidlo–infrastruktura v reálném čase
- Napojení na dopravní ústřednu města Ústí nad Labem
- Zkrácení jízdních dob a snížení emisí CO₂ v dopravě
- Navazující projekt do poloviny roku 2027 (PTK)





**Kybernetický dohled a zabezpečení
datových bodů v 5G síti**

Projekt kybernetického dohledu a zabezpečení datových bodů v 5G síti

Parametry projektu

Žadatel: Statutární město Ústí nad Labem

Program: Národní plán obnovy – 2. výzva 5G

Příprava a realizace: říjen 2023 – prosinec 2025

Rozpočet: 7 537 000 Kč bez DPH

Registrační číslo projektu: CZ.31.6.0/0.0/0.0/23_087/0008729

Partneři realizace: Metropolnet, a.s., Dopravní podnik města Ústí nad Labem (DPMÚL)

5G Ústí nad Labem

Veřejná 5G síť operátora, napojená privátním APN do interní sítě města, prodlužuje, nebo spíše **“virtualizuje”** městskou optiku vzduchem – umožňuje připojit prakticky jakýkoliv bod on-demand, bez pokládky nové optiky i bez vlastní 5G infrastruktury.

Inovace: metropolitní síť „virtualizovaná vzduchem“ nad operátorskou 5G – flexibilní připojení on-demand, nákladově efektivní a přitom zabezpečené na úrovni odpovídající optické páteři.

Ucelené řešení

Růst objemu dat v metropolitní síti zvýšil i její zranitelnost. Ovládání měníren běželo na zastaralém rádiu, chyběl monitoring a vzdálená místa se nesledovala vůbec.

Inovace: jasně pojmenované slabiny se staly základem pro ucelené řešení, ne jen pro dílčí záplaty.

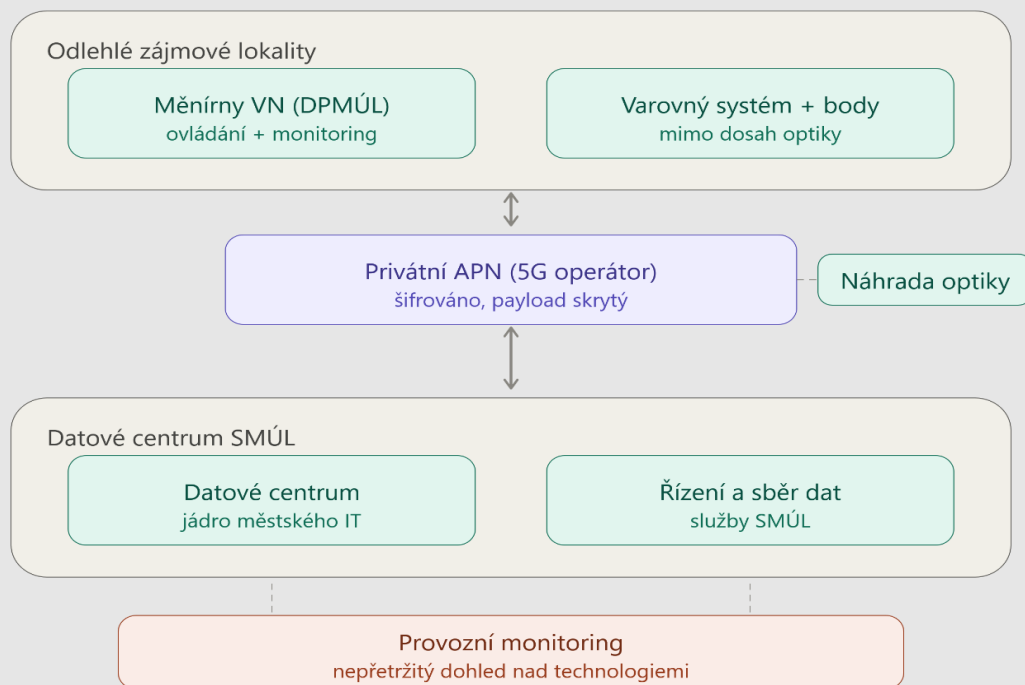
Co je kyber pro občany ?

Kybernetická bezpečnost se promítá do každodenního života – spolehlivější MHD, ochrana osobních údajů obyvatel a pružnější úřad.

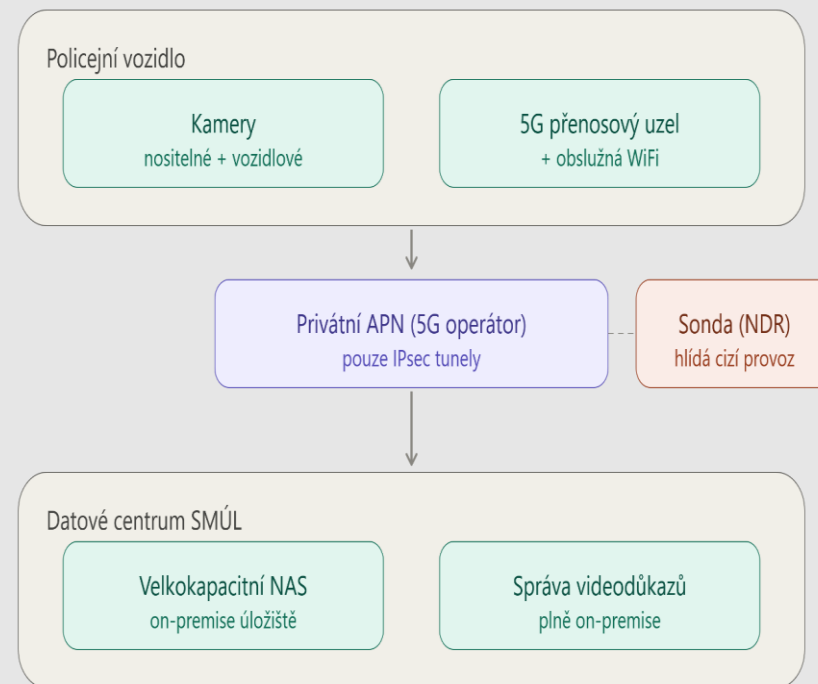
Inovace: abstraktní téma převedené do konkrétních a viditelných přínosů pro občany.



Provozní monitorovací systém, ohlíží na všechny nasazené technologie a provozní parametry



On-line strážník





Kybernetická bezpečnost

Projekt zvýšení kybernetické bezpečnosti statutárního města Ústí nad Labem



Parametry projektu

Žadatel: Statutární město Ústí nad Labem

Program: Národní plán obnovy – Výzva č. 41, Kyber. bezpečnost – obce

Dotace: 49 700 000 Kč bez DPH

Registrační číslo projektu: CZ.31.2.0/0.0/0.0/23_093/0008359

Výstup

Výstup: Nezávislý audit kyberbezpečnosti • Certifikovaný soulad se ZoKB / NIS2 • Sdílené služby pro PO města

Pokročilá síťová segmentace

Zero-trust architektura; oddělení kritických systémů od obecné IT sítě

Monitoring bezpečnostních událostí

Sběr logů a detekce anomálií 24/7 v celé IT infrastruktuře města

Ochrana koncových bodů

Nasazení na všech zařízeních

Sekundární datové centrum

Redundantní cluster pro kontinuitu provozu a obnovu po havárii

Procesní rámec NIS2

Bezpečnostní politiky, řízení přístupů, zvládání incidentů – soulad s NIS2

Souvislost a návaznost s 5G projekty

Kyberbezpečnost přenosové sítě (5G), centrální monitoring



Kybernetická bezpečnost - struktura

★ Veškerá opatření jsou realizována v souladu s EU směrnicí NIS2 (2022/2555) • Zákon č. 264/2025 Sb. ★



Bezpečnostní politika

Cíle, zásady a odpovědnosti v kybernetické bezpečnosti



Řízení aktiv

Inventarizace a klasifikace HW, SW a datových aktiv



Řízení přístupů

MFA, správa privilegovaných účtů, princip min. oprávnění



Bezpečnost lid. zdrojů

Školení, проверки, smluvní odpovědnosti



Provozní bezpečnost

Monitoring, antivirus, zálohy, správa zranitelností



Fyzická bezpečnost

Serverovny, řízený přístup, kamerové systémy



Bezpečnost komunikací

Síťová segmentace, NGFW, šifrování, ochrana perimetru



Bezpečnost dodavatelů

Hodnocení supply chain, smluvní záruky bezpečnosti



Zvládání incidentů

Detekce, klasifikace, hlášení NÚKIB do 24 h



Kontinuita činností

DRP, BCP, testování zálohovacích scénářů

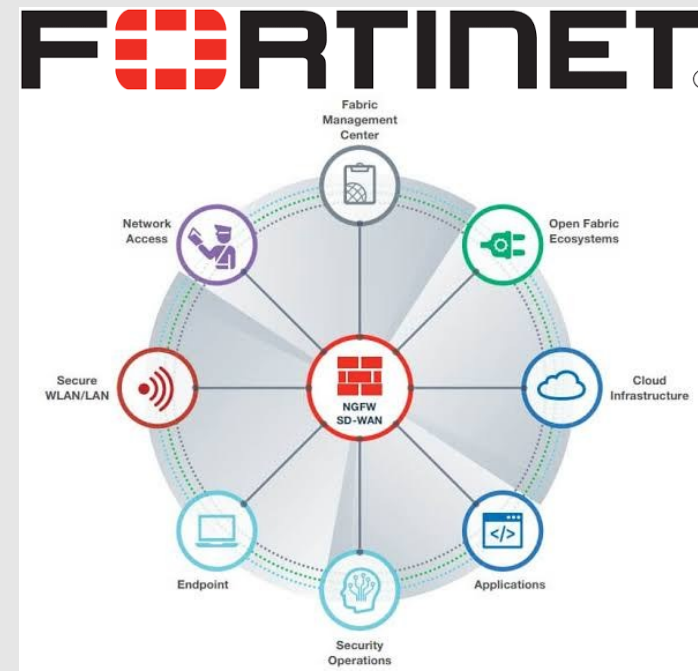


Audit kybernetické bezpečnosti

Nezávislý audit • plný soulad ZoKB • realizuje Metropolnet • 06/2026

Technologie v projektu

- ^ Fortinet FortiGate (v režimu HA)
 - ^ Fortinet FortiEDR
 - ^ Fortinet FortiDeceptor
 - ^ Fortinet FortiZTNA
 - ^ Fortinet FortiPAM
-
- ^ Aricoma IDM
 - ^ Hierarchická PKI infrastruktura
 - ^ Monet (Card Management System)



Projekt rozšíření neveřejné sítě veřejné správy

Parametry projektu

Žadatel: Statutární město Ústí nad Labem

Program: IROP (Integrovaný regionální operační program) • MMR

Rozpočet: 74 400 000 Kč bez DPH



Popis projektu

Připojení 52 městských objektů k neveřejné optické síti

Síť spravovaná MNETem – integrace do CMS2 (MVČR, centrální systém eGovernmentu)

Bezpečná, nekomerční, vysokorychlostní konektivita,

Zahrnuje: školy, komunitní centra, záchranné složky, sociální zařízení

Parametry dle stanovených podmínek IROP / MMR

Umožňuje centralizované ICT a CMS 2.0 služby



Kybernetická bezpečnost města

Město s Metropolnetem (garant kyberbezpečnosti) završuje komplexní zabezpečení informačních systémů, spolufinancované z NPO.



Technická opatření: segmentace, monitoring událostí, ochrana koncových bodů.



Procesní opatření: politiky, řízení přístupů, incidenty, kontinuita.



Audit → soulad se ZoKB, ISO 27001, GDPR.



Data města: šifrováno, odděleno od internetu, žádný cloud.



Report kyberbezpečnosti — provozní statistiky ochrany (2025)



Technologický ekosystém města – vše naráz

Chytré a propojené město

- › Řídicí platforma a dohledové centrum
- › Dopravní ústředna a řízení křižovatek
- › C-ITS — kooperativní doprava
- › Metropolitní optická síť (MOS)
- › Data, analytika a reporting

Bezpečnost občanů

- ★ **Dronové centrum**
- › Městský kamerový systém (MKDS)
- › Online strážník MP (5G)
- › Operační středisko Na Nivách
- › Integrace HZS, IZS, MP · varování

Jednotné městské ICT

- › Kybernetická bezpečnost (ZoKB)
- › Neveřejná síť veřejné správy (CMS2)
- › Centrální ICT a datové centrum
- › Rozvoj informačních systémů
- › Regulace: NIS2, ISO 27001, GDPR

Technologické kompetenční centrum – Metropolnet, a.s.

2022 – 2026: 9+ investičních 5G projektů projektů z NPO

2026 – 2030: 3 rozvojové cíle města



Děkuji za pozornost

TechForum 2026

Jan Hofman

Metropolnet, a.s. / Statutární město Ústí nad Labem

sekretariat@metropolnet.cz / www.metropolnet.cz / Mírové náměstí 3097/37, Ústí nad Labem





TechForum 2026

Jak zvládnout kyberzákon i AI s nadhledem