Digitalizace krizového řízení, strategie a rozvoj ICT v oblasti krizového řízení, koncepce Smart Cities

20. 11. 2025 09:45

Předmět žádosti: žadatel požaduje odpovědi na dotazy týkající se Strategie a rozvoje ICT v oblasti krizového řízení, digitalizace krizového řízení, koncepce Smart Cities apod. V žádosti uvedl, že poskytnuté informace budou využity pro zpracování habilitační práce a pro řešení výzkumného úkolu zaměřeného na digitalizaci krizového řízení u obcí s rozšířenou působností (ORP).

K požadavkům žadatele KÚ LK uvedl, že z krajské úrovně nelze odpovědět na rozsah řešení problematiky digitalizace krizového řízení u ORP. Níže zaslané doplněné dílčí odpovědi jsou uváděny z pohledu Libereckého kraje, nikoliv ORP a obce. ORP i obce jsou samostatné subjekty, a tudíž si případné technologie zabezpečují samostatně. Dotazy je potřeba adresovat přímo na ně.

1. Strategie ICT a digitalizace krizového řízení.

- **Jakou formou je ve Vaší Strategii ICT zahrnuta problematika zaměřená na digitalizaci krizového řízení v návaznosti na moderní technologie a koncepci Smart Cities?**

Odpověď:

Oddělení krizového řízení KÚ LK nezpracovává žádnou strategii ICT. Digitalizace krizového řízení není u KÚ LK řešena.

U KÚ LK je v rámci krizového řízení využíván informační systém tzv. Portál krizového řízení Libereckého kraje (dále jen „PKŘ LK“) dostupný na internetu ***https://pkr.kraj-lbc.cz/portal/***.

PKŘ LK se skládá ze dvou částí:

a. Veřejná část PKŘ LK:

- Je určena pro občany.
- Informace o mimořádné – krizové situaci, aktuální situace.
- Zásady, jak se chovat při mimořádné události krizovém stavu.

a. Neveřejná část PKŘ LK:

- Je určena pro krizové štáby LK a ORP, pro starosty obcí LK, pro složky IZS
- Kontakty – spojení.
- Krizový plán, Havarijní plán.
- Systém řízení KŠ kraje (deník činnosti – evidence plněných úkolů napříč skupinami KŠ) atd.

Dle informací tajemníků bezpečnostních rad je připravován celorepublikový informační systém krizového řízení (dále jen „ISKŘ“), který je v kompetenci Ministerstva vnitra-Generálního ředitelství Hasičského záchranného sboru ČR (dále jen „GŘ HZS“). Nyní je tento ISKŘ ve stavu přípravy a nemáme k němu žádné bližší informace. Je nutné směřovat otázku ISKŘ pro všechny krajské úřady na GŘ HZS.

- **Pokud je tato problematika ve Vaší Strategii ICT obsažena, jakým způsobem dochází k plnění těchto cílů?**

Odpověď:

Není obsažena.

- **Lze plnění těchto cílů dohledat veřejně např. na webových stránkách nebo specializovaném portále Vašeho úřadu?**

Odpověď:

Oddělení krizového řízení tuto problematiku neřeší ani na webových stránkách.

- **Jaké moderní technologie nebo koncepty Smart Cities považuje Váš úřad za klíčové pro rozvoj krizového řízení např. prostřednictvím IoT senzorů, umělé inteligence nebo cloudových služeb?**

Odpověď:

Krizové řízení v daný okamžik nevyužívá žádné moderní technologie umělé inteligence. Určité senzorické vstupy má informační systém Portál krizového řízení integrovány. Nejedná se o běžné senzory IoT, ale o data z těchto senzorů předávaná webovou službou původce dat (např. ČHMÚ).

- **Obsahuje Strategie ICT Vašeho úřadu také cíle v oblasti síťové bezpečnosti a kybernetické odolnosti, a to v kontextu podpory digitalizace krizového řízení?**

Odpověď:

Ne.

- **Má Váš úřad zpracovaný plán rozvoje infrastruktury např. modernizace aktivních prvků, segmentace sítě, modernizace síťové páteře?**

Odpověď:

Ne.

- **Jakou formou jsou tyto cíle financovány a vyhodnocovány z hlediska investiční efektivity a udržitelnosti?**

Odpověď:

Využíváme prostředky z evropských fondů s podílem vlastních finančních zdrojů. Efektivita a udržitelnost je hodnocena již při realizaci veřejných zakázek.

2. Koncepce Smart Cities a rozvoj ICT v oblasti krizového řízení.

Koncepční testování inovativních bezpečnostních technologií

- **Jaké nové technologie v oblasti bezpečnosti ICT infrastruktury Váš úřad testuje nebo jaké jsou na Vašem úřadu implementovány přístupy např. Zero Trust, behaviorální monitoring, endpoint detection?**

Odpověď:

V oblasti KŘ se žádné bezpečnostní technologie netestují.

- **Využívá Váš úřad testovací prostředí (sandbox) pro ověřování nových řešení před nasazením do provozu?**

Odpověď:

Ne.

- **Mají tyto technologie i souvislost s krizovým řízením?**

Odpověď:

Ne.

- **Spolupracuje Váš úřad s NÚKIB, univerzitami či komerčními partnery v oblasti testování bezpečnostních inovativních technologií, pokud ano s jakými ve Vašem kraji?**

Odpověď:

Ne.

- **Jakým způsobem IT útvar Vašeho úřadu stanovuje priority a finanční plánování pro testování nových bezpečnostních technologií?**

Odpověď:

Pro oblast KŘ odbor IT nestanovuje. KŘ se řídí zákonem č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) (dále jen „krizový zákon“) a zákonem č. 241/2000 Sb., o hospodářských opatření pro krizové stavy a o změně některých souvisejících zákonů.

Komplexní rozvoj metropolitních dispečinků jako center situačního a krizového řízení

- **Jakým způsobem IT útvar Vašeho úřadu technicky nebo bezpečnostně podporuje městské či regionální dispečerské systémy např. formou metodické podpory, sdílení infrastruktury, zajištění konektivity, šifrovaného přenosu dat nebo zálohovacích služeb?**

Odpověď:

Nepodporuje.

- **Má Váš úřad zpracovaný plán modernizace síťové infrastruktury např. aktivních prvků, serverů, datových linek, které jsou využívány také pro datové propojení a komunikaci s dispečerskými systémy měst a složek Integrovaného záchranného systému (IZS)?**

Odpověď:

Ne.

- **Má Váš úřad zřízen centrální bezpečnostní dohled např. SOC nebo SIEM, a pokud ano, zahrnuje tento dohled i monitoring nebo koordinaci bezpečnostních událostí z informačních systémů, které využívají města nebo dispečinky v rámci krizového řízení?**

Odpověď:

SIEM je využíván pouze pro potřeby KÚ LK.

- **V rámci zajištění technologické infrastruktury a informačních toků pro krizové řízení krajské úřady spravují také účelové informační systémy pro krizové řízení, včetně systémů v režimu utajovaných informací. Krajské úřady tedy zajišťují provoz, bezpečnost a správu informačního systému krizového řízení, včetně částí fungujících v režimu utajovaných informací podle zákona č. 412/2005 Sb. Je tento systém součástí technického zázemí krajského dispečinku nebo krizového štábu? Zajišťuje provoz tohoto systému přímo Váš úřad IT útvarem nebo prostřednictvím externího dodavatele např. na základě servisní smlouvy?**

Odpověď:

Součástí technického zázemí oddělení krizového řízení je informační systém ministerstva vnitra: Vega D-2 T. Provoz IS Vega D-2T zajištuje oddělení krizového řízení ve spolupráci s odborem IT. Na pult ostrahy budovy úřadu je napojeno zabezpečení místnosti.

Zajištění kompatibility technologických řešení v rámci krizového řízení

- **Jakým způsobem IT útvar Vašeho úřadu zajišťuje interoperabilitu systémů mezi úřadem, městy, složkami IZS a státní správou?**

Odpověď:

Složky IZS komunikují na základě vlastních předpisů a postupů. Oddělení krizového řízení je dle krizového zákona metodickým odborným orgánem pracovníků krizového řízení ORP.

- **Jakým způsobem IT útvar Vašeho úřadu vyhodnocuje bezpečnostní rizika a zajišťuje kompatibilitu síťové architektury s národními systémy?**

Odpověď:

IT uvedenou oblast nezajišťuje.

Zavádění vzdálených přístupů pro PČR do MKDS obcí

- **Koordinuje Váš úřad podporu pro zavádění vzdálených přístupů PČR do městských kamerových systémů, pokud ano, jaký odbor a jakým způsobem?**

Odpověď:

IT ani KŘ takovou podporu nekoordinuje. Toto je otázka na PČR. V případě požadavku PČR je možné na zavedení nových kamerových systémů poskytnout dotaci.

- **Kdo na Vašem úřadu schvaluje technické parametry a finanční rámec těchto propojení na Vašem úřadu a jaký odbor má za tyto činnosti odpovědnost?**

Odpověď:

Oddělení KŘ ani IT toto neřeší.

Bezpečné regionální privátní datové sítě

- **Podílí se Váš úřad na rozvoji a rozšiřování bezpečných regionálních datových sítí pro sdílení citlivých dat?**

Odpověď:

Liberecký kraj neprovozuje a ani se nepodílí na provozu privátních regionálních sítí.

- **Jakým způsobem (formou) IT útvar řeší správu a upgrade aktivních síťových prvků (firewally, switche, routery)?**

Odpověď:

IT neřeší správu regionálních datových sítí.

- **Jakou formou zabezpečení jsou řešena přístupová práva, audit a šifrování datových přenosů?**

Odpověď:

Odpověď není relevantní – viz. výše.

- **Využívá Váš úřad SIEM pro centralizovanou správu logů a bezpečnostních událostí?**

Odpověď:

Odpověď není relevantní – viz. výše.

- **Jak jsou tyto sítě financovány a udržovány (interní rozpočet / dotační programy)?**

Odpověď:

Odpověď není relevantní – viz. výše.

- **Jakým způsobem Váš IT útvar vyhodnocuje návratnost a efektivitu těchto investic?**

Odpověď:

Odpověď není relevantní – viz. výše.

- **Je součástí těchto procesů také finanční a investiční plánování modernizace sítě na Vašem úřadu?**

Odpověď:

Odpověď není relevantní – viz. výše.

Metodika zahrnutí bezpečnostního kritéria do činností úřadu

- Má Váš úřad implementovanou interní metodiku pro hodnocení bezpečnostních dopadů IT projektů v souladu s platnou legislativou v oblasti kybernetické bezpečnosti v ČR a EU?

Odpověď:

Ano.

- **Jakou formou je na Vašem úřadu zajištěno projektové řízení IT zahrnující síťovou bezpečnost, řízení rizik a rozpočtové dopady?**

Odpověď:

Řídí se interní směrnicí.

- **Jakým způsobem Váš úřad školí pracovníky ICT a vedoucí odborů v oblasti síťové bezpečnosti a krizové komunikace?**

Odpověď:

Odbor informatiky zajišťuje školení pro své pracovníky. Manažer kybernetické bezpečnosti zajišťuje školení všech zaměstnanců v oblasti kybernetické bezpečnosti.

Kompatibilita inovativních technologických řešení

- **Jakým způsobem IT útvar Vašeho úřadu zajišťuje technickou a bezpečnostní kompatibilitu nových řešení vycházejících z koncepce Smart Cities a digitalizace krizového řízení se stávající síťovou infrastrukturou úřadu?**

Odpověď:

Dle informací tajemníků bezpečnostních rad je připravován celorepublikový informační systém krizového řízení (dále jen „ISKŘ“), který je v kompetenci Ministerstva vnitra-Generálního ředitelství Hasičského záchranného sboru ČR (dále jen „GŘ HZS“). Nyní je tento ISKŘ ve stavu přípravy a nemáme k němu žádné bližší informace. Je nutné směřovat otázku ISKŘ pro všechny krajské úřady na GŘ HZS.

- **Jakým způsobem IT útvar plánuje modernizaci a financování síťové infrastruktury v souvislosti s digitální transformací?**

Odpověď:

Dle potřeb, finančních možností a požadavků doby.