Zlínský Krajský úřad kraj

Odbor právní a Krajský živnostenský úřad
Oddělení státního občanství a přestupků

Poskytnutí informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím

Dne 11. listopadu 2025 obdržel Krajský úřad Zlínského kraje (dále jen „krajský úřad“) jako povinný subjekt Vaši žádost podanou ve smyslu zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, kterou jste požádala o informace (doslovný přepis) týkající se digitalizace krizového řízení.

Na základě podkladů poskytnutých Odborem Kancelář hejtmana, Odborem informačních a komunikačních technologií a Odborem strategického rozvoje kraje Vám informace poskytujeme formou dopsání sdělení k Vámi položeným dotazům:

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?*

Tato oblast není nijak speciálně řešena.

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

Viz předchozí odpověď.

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

Viz první odpověď.

• *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?*

Důležitá je bezpečnost a provoz v on-prem prostředí.

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

Obecně se zaměřujeme na bezpečný síťový provoz a kybernetickou bezpečnost v souladu se zákonem o kybernetické bezpečnosti.

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

Ano

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

Cíle jsou financovány z rozpočtu Odboru ICT, případně dotačních programů. Projekty jsou plánovány v 3letém výhledu rozpočtu dle bezpečnostních požadavků (ZKB) v návaznosti na služby a kapacitní a výkonové limity.

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

Zlínský kraj nemá zpracovánu koncepci s názvem „Koncepce Smart Cities“, nicméně má schválen koncepční dokument s názvem Chytrý kraj – Strategie rozvoje chytrého regionu Zlínského kraje 2030 (dále také Strategie). Dokument schválila Rada Zlínského kraje 22. února 2021, č. usnesení 0130/R07/21, odkaz na dokument zde: https://zlinskykraj.cz/chytry-kraj-strategie-rozvoje-chytreho-regionu-zlinskeho-kraje-2030 (např. 8.1 Chytrá veřejná správa – jako součást širší situační analýzy, 13.5 Specifický cíl 3.1 Kvalitní ICT a vybudovaná e-governance).

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?*

Z hlediska přístupů a principů kybernetické bezpečnosti podléhá oblast krizového řízení bez výjimek obecným zásadám a nastavením zajišťovaným odborem ICT. Ten sleduje aktuální trendy a požadavky dle ZKB, na základě kterých implementuje jednotlivé oblasti bezpečnosti ICT infrastruktury.

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

Využíváme testovací prostředí.

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

Pravidla platí pro všechny provozované systémy.

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

Ne

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

Úřad nemá útvar pro vývoj a výzkum. Technologie u nás netestujeme a neprovádíme testování ve spolupráci s dalšími subjekty.

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?*

Pracoviště je propojeno zabezpečenou komunikační infrastrukturou pomocí optických vláken (NET21Net – krajská neveřejná síť) se všemi 13 pracovišti krizového řízení obcí s rozšířenou působností a jejich povodňovými a krizovými štáby.

• *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)?*

Ano

• *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?*

Ano, máme centrální bezpečnostní dohled. Nezahrnuje monitoring nebo koordinaci bezpečnostních událostí z IS, které využívají města nebo dispečinky.

• *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?

Systém vládního utajovaného spojení Vega D-2G, určený pro příjem utajovaných informací, je provozován Ministerstvem vnitra ČR.

Informace dle zákona č. 412/2005 Sb. jsou vyjmuty z rozsah systému řízení bezpečnosti informací. Provoz je zajištěn IT útvarem.

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?

Sdílením informací, standardizovanými rozhraními.

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

Analýzou rizik a stanovením standardů do zadávací dokumentace.

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?

Nekoordinuje.

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

Není relevantní.

Bezpečné regionální privátní datové sítě

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

Ano

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

Vlastními silami, podporou výrobce jednotlivých technologií a servisními partnery.

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

Dle zákona o kybernetické bezpečnosti.

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

Ano

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

Interní rozpočet, dotační programy.

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

Investice jsou plánovány v 3letém výhledu rozpočtu dle bezpečnostních požadavků (ZKB) v návaznosti na služby a kapacitní a výkonové limity.

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

Ano

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?*

Ano

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

Standardizovanými postupy řešenými v rámci vnitřních norem.

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

Využíváme více forem vzdělávání v oblasti bezpečnosti informačních systémů.

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?*

Dle interních pokynů odboru ICT.

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

Na základě plánu rozvoje ICT.