Jihočeský kraj
Krajský úřad

Odbor kancelář hejtmana
Úsek vedoucího odboru

KUCBX01JH2R6

Váš dopis zn.:
Ze dne: 9. 11. 2025
Naše č. j.: KUJCK 126670/2025
Sp. Zn.: KHEJ 125527/2025/papo1 SO
Vyřizuje: Pavla Polívková
Telefon: 386720225
E-mail: polivkova@kraj-jihocesky.cz
Datum: 12. 11. 2025

Poskytnutí informací podle § 14 odst. 5 písm. d) zákona č. 106/1999 Sb.

Vážená paní,

Krajský úřad Jihočeského kraje obdržel dne 9. 11. 2025 Vaši žádost o poskytnutí informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, v níž požadujete poskytnutí následující informace:

1. Strategie ICT a digitalizace krizového řízení.
a) Jakou formou je ve Vaší Strategii ICT zahrnuta problematika zaměřená na digitalizaci krizového řízení v návaznosti na moderní technologie a koncepci Smart Cities?
b) Pokud je tato problematika ve Vaší Strategii ICT obsažena, jakým způsobem dochází k plnění těchto cílů?
c) Lze plnění těchto cílů dohledat veřejně např. na webových stránkách nebo specializovaném portále Vašeho úřadu?
d) 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?
e) Obsahuje Strategie ICT Vašeho úřadu také cíle v oblasti síťové bezpečnosti a kybernetické odolnosti, a to v kontextu podpory digitalizace krizového řízení?
f) Má Váš úřad zpracovaný plán rozvoje infrastruktury např. modernizace aktivních prvků, segmentace sítě, modernizace síťové páteře?
g) Jakou formou jsou tyto cíle financovány a vyhodnocovány z hlediska investiční efektivity a udržitelnosti?
2.. Koncepce Smart Cities a rozvoj ICT v oblasti krizového řízení.
Koncepční testování inovativních bezpečnostních technologií
a) 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?
b) Využívá Váš úřad testovací prostředí (sandbox) pro ověřování nových řešení před nasazením do provozu?
c) Mají tyto technologie i souvislost s krizovým řízením?
d) Spolupracuje Váš úřad s NÚKIB, univerzitami či komerčními partnery v oblasti testování bezpečnostních inovativních technologií, pokud ano s jakými ve Vašem kraji?
e) Jakým způsobem IT útvar Vašeho úřadu stanovuje priority a finanční plánování pro testování nových bezpečnostních technologií?

Komplexní rozvoj metropolitních dispečinků jako center situačního a krizového řízení

a) 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?
b) 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)?
c) 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?
d) 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?

Zajištění kompatibility technologických řešení v rámci krizového řízení
a) Jakým způsobem IT útvar Vašeho úřadu zajišťuje interoperabilitu systémů mezi úřadem, městy, složkami IZS a státní správou?
b) Jakým způsobem IT útvar Vašeho úřadu vyhodnocuje bezpečnostní rizika a zajišťuje kompatibilitu síťové architektury s národními systémy?

Zavádění vzdálených přístupů pro PČR do MKDS obcí
a) Koordinuje Váš úřad podporu pro zavádění vzdálených přístupů PČR do městských kamerových systémů, pokud ano, jaký odbor a jakým způsobem?
b) Kdo na Vašem úřadu schvaluje technické parametry a finanční rámec těchto propojení na Vašem úřadu a jaký odbor má za tyto činnosti odpovědnost?

Bezpečné regionální privátní datové sítě
a) Podílí se Váš úřad na rozvoji a rozšiřování bezpečných regionálních datových sítí pro sdílení citlivých dat?
b) Jakým způsobem (formou) IT útvar řeší správu a upgrade aktivních síťových prvků (firewally, switche, routery)?
c) Jakou formou zabezpečení jsou řešena přístupová práva, audit a šifrování datových přenosů?
d) Využívá Váš úřad SIEM pro centralizovanou správu logů a bezpečnostních událostí?
e) Jak jsou tyto sítě financovány a udržovány (interní rozpočet / dotační programy)?
f) Jakým způsobem Váš IT útvar vyhodnocuje návratnost a efektivitu těchto investic?
g) Je součástí těchto procesů také finanční a investiční plánování modernizace sítě na Vašem úřadu?

Metodika zahrnutí bezpečnostního kritéria do činností úřadu
a) 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?
b) Jakou formou je na Vašem úřadu zajištěno projektové řízení IT zahrnující síťovou bezpečnost, řízení rizik a rozpočtové dopady?
c) Jakým způsobem Váš úřad školí pracovníky ICT a vedoucí odborů v oblasti síťové bezpečnosti a krizové komunikace?

Kompatibilita inovativních technologických řešení

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

K výše uvedené žádosti Vám sdělujeme následující:

Ad 1)

a) Strategie Krajského úřadu Jihočeského kraje 2023–2025 Strategie Krajského úřadu Jihočeského kraje 2023-2025.pdf. V rámci naplňování Strategie KÚ JK došlo k založení Jihočeského centra kybernetické bezpečnosti, s.r.o. jako servisní organizace, jejímž smyslem je pomoc při zajištění bezpečnosti a bezpečnosti informací pro zřizované organizace kraje a Krajského úřadu Jihočeského kraje (KÚ JK). Oblast krizového řízení je jednou z agend, kterou KÚ JK zajišťuje v rámci své činnosti. Obecně lze konstatovat, že KÚ JK klade velký důraz na digitalizaci a bezpečnost vykonávaných agend. V rámci naplňování strategie Digitální Česko a Strategie KÚ JK je mimo jiné realizován projekt Portál krizového řízení Jihočeského kraje (IROP 21+, Evropské projekty kraje | www.kraj-jihocesky.cz) coby informační systém digitalizující jak plánovací část činností, tak samotnou operativu při řešení vzniklých situací. Koncepce Smart Cities není s tímto projektem v průniku.
b) Viz předchozí odpověď.
c) Projekty, na které se odkazujeme ve svých odpovědích jsou aktuálně ve stádiu realizace, tj. lze odkázat pouze na informace na shora uvedených odkazech.
d) 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 a SÚJB).
e) Otázka bezpečnosti a kybernetické bezpečnosti je standardní součástí plánování/řízení.
f) KÚ JK plánuje rozvoj infrastruktury s ohledem na síťovou bezpečnost a kybernetickou odolnost, za tímto účelem aktuálně realizuje projekt „Zvýšení kybernetické bezpečnosti v Jihočeském kraji“ (NPO, Zvýšení kybernetické bezpečnosti v Jihočeském kraji | www.kraj-jihocesky.cz).
g) Obecně se kraj/krajský úřad snaží zjistit pro realizaci uvedených projektů vícezdrojové financování ze zdrojů Jihočeského kraje, státního rozpočtu a prostředků evropských fondů (IROP, NPO). V rámci přípravy projektů obecně KÚ JK realizuje zpracování studií proveditelnosti vč. průzkumů trhu, realizace procesů probíhá na základě realizace veřejných zakázek, které jsou konzultovány/kontrolovány poskytovatelem dotace.

Ad 2)

Koncepční testování inovativních bezpečnostních technologií

a) V rámci sítě KÚ JK je nasazena technologie endpoint detection a sledování síťových toků
b) Nevyužívá
c) Jsou implementovány v síti KÚ JK
d) Nespolupracuje, ve spolupráci s NÚKIB bylo realizováno penetrační testování některých služeb, které KÚ JK provozuje
e) BestPractises, oborové standardy, doporučení relevantních institucí (např. NUKI)

Komplexní rozvoj metropolitních dispečinků jako center situačního a krizového řízení

a) Není nám znám provoz metropolitních dispečinků na území Jihočeského kraje.

b) Propojení informačního systému Portál krizového řízení kraje není realizováno do vlastních informačních systémů složek IZS ale udělením přístupů operátorům do našeho informačního systému přes webové rozhraní v síti internet.
c) SOC ne, log management pro systémy KÚ JK.
d) V rámci zajištění činnosti krizového štábu kraje dle zákona č. 412/2005 Sb., je využíván systém vládního utajovaného spojení a certifikovaný informační systém JK pro zpracování utajovaných informací.
Provoz je zajišťován vlastními zaměstnanci KÚ JK.

Zajištění kompatibility technologických řešení v rámci krizového řízení

a) Interoperabilita není přímo zajišťována ze strany KÚ JK. Pro užívání informačního systému Portálu krizového řízení kraje je spolupráce zajišťována udělením přístupů do systému pracovníkům kraje, obcí a měst, základních složek IZS a dalších subjektů podílejících se na řešení nebo plánování v oblasti krizového řízení.
b) Bezpečnostní rizika jsou hodnocena v rámci procesu analýzy aktiv a rizik, jejíž aktualizace je realizována na každoroční bázi, či dle potřeby, soulad s kompatibilitou s národními systémy je realizován na základě doporučení a metodik viz archi.gov.cz a oborových standardů.

Zavádění vzdálených přístupů pro PČR do MKDS obcí

a) Tato problematika není v kompetenci KÚ JK.
b) Nerelevantní, viz předchozí odpověď.

Bezpečné regionální privátní datové sítě

a) Jihočeský kraj nemá vybudovanou ani neprovozuje vlastní regionální datovou síť. Jihočeský kraj poskytuje služby krajského konektoru v rámci KIVS pro přístup definovaných subjektů k centrálním službám státu.
b) - g) Nerelevantní, viz předchozí odpověď.

Metodika zahrnutí bezpečnostního kritéria do činností úřadu

a) KÚ JK postupuje v souladu s platnou legislativou (zejména zákon o kybernetické bezpečnosti a navazující vyhlášky, případně v souladu s požadavky poskytovatelů dotačních prostředků. Zejména se jedná o hodnocení dodavatelů v souladu se zákonem o kybernetické bezpečnosti.
b) zajištěno vlastními zaměstnanci KÚ JK případně ve spolupráci s pracovníky svěřené správy a pracovníky dodavatelů
c) Obecně jsou pracovníci KÚ JK, tedy i ICT školení v oblasti kybernetické bezpečnosti, a to jak pomocí interních kapacit či kapacit externích, ICT si dále zajišťuje svá specifická školení dle potřeby. Školení krizové komunikace...

Kompatibilita inovativních technologických řešení

a) KÚ JK se snaží v maximální možné míře dodržovat standardy v dané oblasti.
b) Využíváme prostředků dotačních titulů a vlastních zdrojů, provádíme pravidelnou obnovu síťové infrastruktury a ICT vybavení

S pozdravem

Mgr. Petr Podhola
vedoucí odboru KHEJ