MORAVSKOSLEZSKÝ KRAJ
KRAJSKÝ ÚŘAD
28. října 2771/117, 702 00 Ostrava

Váš dopis zn.:
Ze dne: 11. 11. 2025
Čj.: MSK 148485/2025
Sp. zn.: INF/24937/2025/Krp
084.1 S6
Vyřizuje: [redacted]
Odbor: Odbor informatiky
Telefon: [redacted]
Fax: 595 622 126
E-mail: posta@msk.cz
Datum: 25. 11. 2025

[redacted]

Poskytnutí informací dle zákona č. 106/1999 Sb.

Vážená paní doktorko,

na základě Vaší žádosti ze dne 11. 11. 2025 o poskytnutí informací týkajících se **digitalizace krizového řízení u obcí s rozšířenou působností (ORP), u nichž již bylo v rámci celé České republiky provedeno šetření v uvedené oblasti**, a to v návaznosti na cíle a typová opatření vycházející Vládou ČR schválené **„Koncepce Smart Cities – odolnost prostřednictvím SMART řešení pro obce, města a regiony"**, Vám sdělujeme následující:

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?

  Samostatná problematika zaměřená na digitalizaci krizového řízení v návaznosti na moderní technologie a koncept Smart Cities není v současné době zahrnuta v Strategii ICT, protože je řešena jako součást širší koncepce digitalizace celého krajského úřadu. Dalším důvodem je postupná digitalizace krizového řízení ze strany ministerstev a jiných ústředních správních úřadů, kdy krajský úřad v souladu se zákony využívá tyto informační systémy.

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

  Konkrétní cíle pro oblast krizového řízení nejsou ve Strategii ICT uvedeny.

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

  Nelze dohledat plnění těchto cílů, ve Strategii ICT nejsou stanoveny konkrétní úkoly pro oblast krizového řízení.

- 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?

  Jelikož samostatná problematika zaměřená na digitalizaci krizového řízení v návaznosti na moderní technologie a koncept Smart Cities není v současné době zahrnuta v Strategii ICT našeho úřadu, není rovněž stanoveno, jaké moderní technologie jsou pro nás klíčové.

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

  Strategie ICT úřadu obsahuje cíle v oblasti síťové bezpečnosti a kybernetické odolnosti, které mají dopad také na krizové řízení. Pro oblast krizového řízení nejsou samostatně stanoveny další cíle.

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

  Ano, krajský úřad má zpracovanou informační koncepci kraje. Zmiňovaným oblastem se podrobněji věnuje dokument Kapacitní plán.

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

  Financování je převážně zajištěno z rozpočtu kraje, u některých projektů jsou využity investice z dotačních programů. Vyhodnocování probíhá na základě analýzy nákladů a přínosů, ocenění informačních aktiv a analýzy rizik.

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

a) 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?

  Na našem úřadě jsou sledovány trendy v oblasti nových technologií souvisejících s bezpečností ICT infrastruktury a pokud je to možné, jsou využívány účinné, aktuální technologie. Konkrétní používané nebo zvažované technologie jsou citlivou informací.

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

  Ano, tam kde je to možné a vhodné, je využíváno testovací prostředí.

- Mají tyto technologie i souvislost s krizovým řízením?

  Uvedené technologie nemají souvislost s krizovým řízením.

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

  Ano, náš úřad spolupracuje s NÚKIB, komerčními subjekty a vlastní příspěvkovou organizací – Moravskoslezské datové centrum (dále jen „MSDC").

Tel.: 595 622 222 IČ: 70890692
Fax: 595 622 126 DIČ: CZ70890692
ID DS: 8x6bxsd Č. účtu: 1650676349/0800
www.msk.cz

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

  Pravidelně je prováděna analýza rizik, na základě které je stanoven další postup zajištění kybernetické bezpečnosti. Finanční plánování probíhá v rámci rozpočtu kraje.

b) 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?

  Tuto aktivitu úřad neprovádí.

- 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)?

  Plán modernizace síťové infrastruktury je součástí Kapacitního plánu.

- 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, je využíván SOC zajištěný externí organizací, součástí této služby není dohled bezpečnostních událostí ze systémů měst a dispečinků krizového řízení.

- 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?

  Krajský úřad nezajišťuje provoz, ani neprovozuje vlastní informační systém pro krizové řízení. V současnosti využívá informační systémy ministerstev a jiných správních úřadů jako uživatel. V oblasti utajovaných informací využívá úřad vládní utajované spojení Vega D-2G provozované Ministerstvem vnitra ČR, kraj pouze spravuje tento systém na své úrovni. Systém Vega D-2G není součástí technického zázemí krizového štábu.

c) 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?

  Krajský úřad nezajišťuje interoperabilitu systémů krizového řízení.

Tel.: 595 622 222 IČ: 70890692
Fax: 595 622 126 DIČ: CZ70890692
ID DS: 8x6bxsd Č. účtu: 1650676349/0800
www.msk.cz

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

  V případě technologických řešení jsou prováděny analýzy rizik (identifikace aktiv, hrozeb a zranitelností). Kompatibilita síťové infrastruktury je zajišťována dodržováním standardů DIA, NAKIT.

d) 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?

  Krajský úřad nekoordinuje ani neřídí vzdálený přístup PČR ke kamerovým systémům.

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

  Tyto činnosti úřad nerealizuje, viz výše.

e) Bezpečné regionální privátní datové sítě

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

  Ano, kraj provozuje neveřejnou vysokorychlostní datovou síť (dále jen „VDS"). Její provoz je zajištěn prostřednictvím příspěvkové organizace Moravskoslezské datové centrum. Rozvoj této sítě je aktuálně pozastaven.

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

  Správa síťové infrastruktury VDS je zajištěna interními zaměstnanci odboru informatiky, zaměstnanci MSDC a externími dodavateli.

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

  VDS je provozována jako přenosové médium, přístupová oprávnění a šifrování jsou v kompetenci klientů využívajících toto médium.

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

  Ano, využívá.

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

  Financování VDS je řešeno z rozpočtu kraje.

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

  Aktuálně se přehodnocuje záměr a koncepce VDS, v rámci tohoto přehodnocení se bude zpracovávat také analýza nákladů a dopadů.

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

  Ne, rozvoj interní sítě krajského úřadu je oddělen od plánů provozu a rozvoje VDS.

Tel.: 595 622 222 IČ: 70890692
Fax: 595 622 126 DIČ: CZ70890692
ID DS: 8x6bxsd Č. účtu: 1650676349/0800

f) 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, interní metodika je implementována. S vydáním nového zákona o kybernetické bezpečnosti a jeho vyhlášek bude aktualizována.

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

  Krajský úřad má definované procesy posuzování a schvalování záměrů rozvoje ICT technologií a kybernetické bezpečnosti. Samotná forma projektového řízení je volena podle velikosti a náročnosti konkrétního projektu.

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

  Krajský úřad pro zaměstnance kraje a jeho příspěvkových organizací provozuje vlastní e-learningový nástroj, v rámci kterého jsou řešeny také oblasti kybernetické bezpečnosti. Pro ICT pracovníky jsou také využívána odborná externí školení.

g) 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?

  Při rozvoji ICT a síťové infrastruktury kraj nevychází z koncepce Smart Cities.

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

  Rozvoj a provoz ICT a síťové infrastruktury je kontinuální činnost kraje, která vychází z koncepčních záměrů.

S pozdravem

Elektronický podpis: 25.11.2025
Certifikát autora podpisu:
Jméno: Ing. Jiří Hošek
Vydal: PostSignum Qualified CA 4
Platnost do: 21.10.2028 08:43 +02:00

Ing. Jiří Hošek
pověřený zastupováním funkce vedoucího odboru informatiky

Tel.: 595 622 222 IČ: 70890692
Fax: 595 622 126 DIČ: CZ70890692
ID DS: 8x6bxsd Č. účtu: 1650676349/0800