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?**

Problematika digitalizace krizového řízení v návaznosti na moderní technologie a koncept Smart Cities není v současné době součástí Strategie ICT našeho úřadu.

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

Problematika digitalizace krizového řízení není v současné době součástí Strategie ICT našeho úřadu, a proto nejsou stanoveny ani konkrétní cíle či mechanismy jejího plnění.

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

Plnění uvedených cílů není možné veřejně dohledat, neboť problematika digitalizace krizového řízení není v současné době součástí Strategie ICT našeho úřadu.

- **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?**

V rámci ICT strategie našeho úřadu nejsou v současné době zahrnuty moderní technologie ani koncepty Smart Cities, jako je využití IoT senzorů, umělé inteligence či cloudových služeb, pro rozvoj krizového řízení.

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

Strategie ICT našeho úřadu v kontextu podpory digitalizace krizového řízení neobsahuje cíle zaměřené na síťovou bezpečnost a kybernetickou odolnost.

- **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?**

Financování z vlastního rozpočtu a z dotačních programů EU. Vyhodnocování probíhá dle konkrétního opatření.

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

- **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?**

Například: nástroje umělé inteligence, monitoring sítě s využitím AI, inteligentní WAF, a podobné.

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

Ano, v omezené míře.

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

Uvedené technologie nejsou v současné době přímo provázány s oblastí krizového řízení.

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

Náš úřad v současné době nespolupracuje s Národním úřadem pro kybernetickou a informační bezpečnost, univerzitami ani komerčními partnery v oblasti testování inovativních bezpečnostních technologií.

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

Způsob je závislý a odvíjí se od architektury informačních technologií krajského úřadu a architektury kybernetické bezpečnosti. Finanční plánování vychází z plánů obnovy a zařazování nových technologií do stávající infrastruktury. Zajištění financí vychází z ročního plánu rozpočtu a otevřených výzev vhodných operačních programů.

- **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?**

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)?**

Nemá.

- **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?**

Nemá.

- **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 ani neprovozuje vlastní informační systém pro krizové řízení, vystupuje pouze v roli uživatele vybraných systémů, jako jsou IS Argis, Krizkom, Krizdata a Povis (Povodňový informační systém). Systém vládního utajovaného spojení Vega D-2G, určený pro příjem utajovaných informací, je provozován Ministerstvem vnitra; Olomoucký kraj je i zde pouze uživatelem. Uvedené informační systémy jsou připraveny k využití vybranými členy Krizového štábu Olomouckého kraje při řešení mimořádných událostí a krizových situací. Provoz jednotlivých systémů zajišťuje Správa státních hmotných rezerv (Argis, Krizkom, Krizdata), externí dodavatel (Povis – digitální povodňový plán) a Ministerstvo vnitra (Vega D-2G).“

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

Nezajišťuje.

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

Dle architektury IT a ve spolupráci s MKB a KKB.

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

Náš úřad v současné době nezajišťuje ani nekoordinuje zavádění vzdálených přístupů Policie České republiky do městských kamerových systémů.

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

Schvalování technických parametrů a finančního rámce uvedených propojení není v působnosti našeho úřadu a není zde určena organizační jednotka, která by tuto činnost vykonávala.

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

Nepodílí.

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

Vlastními silami a smlouvami s dodavateli.

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

Přístupová práva a audit jsou řešena na základě role (RBAC) dle best practice Microsoftu. Šifrování datových přenosů je v souladu se zákonem o kybernetické bezpečnosti, prováděcích vyhlášek a doporučení NÚKIB.

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

Nevyužívá.

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

Vlastní rozpočet a dotační programy.

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

Nevyhodnocuje.

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

Ano.

- **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?**

Náš úřad nemá implementovanou vlastní interní metodiku pro hodnocení bezpečnostních dopadů IT projektů. Při jejich posuzování postupujeme v souladu s platnou legislativou v oblasti kybernetické bezpečnosti České republiky a Evropské unie. Jako metodické vodítko využíváme materiály vydané Národním úřadem pro kybernetickou a informační bezpečnost, které jsou veřejně dostupné na stránkách regulátora.

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

Projektové řízení IT projektů na našem úřadu je realizováno prostřednictvím standardních postupů zahrnujících plánování, alokaci zdrojů, sledování průběhu, řízení rizik a komunikaci se zainteresovanými stranami. V rámci těchto činností jsou zohledňovány podpůrné materiály Národního úřadu pro kybernetickou a informační bezpečnost, zejména metodické průvodce k řízení aktiv a rizik vydané v návaznosti na vyhlášku o kybernetické bezpečnosti.

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

Školení pracovníků ICT a vedoucích odborů v oblasti síťové bezpečnosti a krizové komunikace je na našem úřadu zajišťováno v pravidelných intervalech z vlastních zdrojů. Všichni zaměstnanci jsou průběžně proškolováni s cílem posílit jejich odborné znalosti a praktické dovednosti v uvedených oblastech.

- **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?**

Nezajišťuje.

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

Na základě architektury IT a stavu „as-is“ porovnávaného se stavem „to-be“ z čehož jsou tvořeny jednotlivé projekty na dosažení požadovaného stavu.