# Formulář žádosti

## o stanovisko Hlavního architekta eGovernmentu k plánovanému projektu zahrnujícímu záměr realizovat výdaj související s informačními a komunikačními technologiemi

(dle usnesení vlády ČR č. 86/2020 a/nebo zákona 365/2000 Sb.)

**typ A**

**Odbor Hlavního architekta eGovernmentu MV**

**Praha, leden 2022**
**verze 7.1**

**UPOZORNĚNÍ: Přestože je formulář zveřejněn ve formátu umožňujícím změny, žadatel není oprávněn měnit strukturu vybraných otázek či předepsaných odpovědí. Pokud se tak stane, Odbor Hlavního architekta eGovernmentu vyhodnotí takovou změnu jako porušení pravidel při schvalování a formulář bude vrácen bez vydání stanoviska. Tam, kde je to třeba pro uvedení dalších položek do tabulky, je žadatel oprávněn přidávat řádky pro tyto položky.**

**Metodický pokyn k vyplňování na adrese:** https://archi.gov.cz/uvod_schvalovani#jake

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

# 1. ZÁKLADNÍ INFORMACE O PROJEKTU

## 1.1. Úvodní informace o žadateli o stanovisko k plánovanému projektu

| Tabulka 1: **Úvodní informace o žadateli o stanovisko** | | | | |
|---|---|---|---|---|
| **Organizace žadatele** | Město Znojmo | | Obroková 1/12<br>669 02 Znojmo | 00293881 |
| **Ředitel pro informatiku nebo Statutární zástupce** | Ing. Jakub Malačka | Starosta | jakub.malacka@muznojmo.cz | 515 216 250 |
| **Kontaktní osoba projektu** | Ing. Lubomír Otepka | Vedoucí OINF MěÚ Znojmo | lubomir.otepka@muznojmo.cz | 515 216 314 |
| **Architekt projektu** | Ing. David Janečka | Konzultant, HCM COMPUTERS, s.r.o. | janecka@hcmcomputers.cz | +420 602 545 680 |

| **Verze předkládaných / doplněných žádostí o stanovisko, data jejich předložení a jejich čísla jednací** | | |
|---|---|---|
| **Číslo předkládané verze:** | **Datum předložení:** | **Verze předložena pod Čj,:** |
| **1.0** | **6. 9. 2022** | |
| | | |
| | | |
| | | |

| Tabulka 2: **Žádost o stanovisko dle (důvod žádosti)** | |
|---|---|
| **Usnesení vlády č. 86, ze dne 27. ledna 2020 (U86)** | ***Ne*** |
| **Zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů (ZoISVS)** | ***Ano*** |
| **Výzvy v Integrovaném regionálním operačním programu** (IROP), **vypište číslo výzvy** | *IROP 04 Kybernetická bezpečnost* |
| **Dobrovolná žádost o stanovisko** | ***Ne*** |

## 1.2. Shrnutí charakteristik projektu

| Tabulka 3: **Shrnutí charakteristik projektu** | |
|---|---|
| **Název projektu:** | Bezpečná infrastruktura města Znojma |
| **Specifický cíl / účel projektu:** | Hlavním cílem projektu je zvýšení kybernetické bezpečnosti informačního systému obce na ekonomicky udržitelnou úroveň za pomoci nástrojů:<br>• Vlastní technické řešení<br>  ○ IDM – správa identit<br>  ○ AntiX Ochrana<br>  ○ Zvýšení odolnosti a dostupnosti infrastruktury<br>• Organizační opatření (vlastní prostředky)<br>  ○ Seznámení s riziky a hrozbami v kybernetické bezpečnosti zaměstnanců.<br>  ○ Definice nových procesů souvisejících s bezpečností.<br>• Preventivní opatření<br>  ○ Technická opatření<br>  ○ Zakoupení služeb bezpečnostního dohledu v provozní fázi.<br>  ○ Pravidelné kontroly penetračními testy. |

| Tabulka 3: **Shrnutí charakteristik projektu** | | |
|---|---|---|
| | | Stávající infrastruktura bude využita k běhu méně exponovaných systémů a jako záložní lokalita. |
| **Seznam žádostí, které již byly v souvislosti s celkovými cíli a specifickým cílem / účelem projektu předány OHA:** | | X |
| **Odkazy na agendy VS, kterých se projekt týká:** | | *Projekt je zaměřen na následující agendy VS:*<br>*A1721 Kybernetická bezpečnost* – Obec nespravuje systém kritické infrastruktury ani základní služby. |
| **Seznam služeb veřejné správy a jejich úkonů z katalogu služeb veřejné správy, kterých se projekt týká:** | | *Nerelevantní* |
| **Odkazy na určené IS dle UV 86/2020 a zákona 365/2000 Sb., kterých se projekt týká:** | *Přímo dotčené určené IS, které projekt realizuje nebo mění* | *Žádný z evidovaných agendových informačních systémů nebude měněn z hlediska funkcí. Tyto však budou přesunuty do nového prostředí.*<br>• 8369 Scarabeus<br>• 8297 Portál občana<br>• 7227 Mapserver<br>• 7226 Stavební úřad<br>• 7225 Webové stránky města – www.znojmocity.cz<br>• 7223 Přestupky<br>• 7221 Personalistika<br>• 7138 YAMACO<br>• 4933 MP Manager<br>• 757 FLUXPAM5<br>• 684 Evidence myslivosti – EMY<br>• 683 Evidence správních řízení – ESPI<br>• 682 Ochrana ovzduší<br>• 681 VITA<br>• 613 HeleTax<br>• 612 Evidence odpadů – EVI<br>• 611 Editor vodoprávní evidence – eVPE<br>• 497 GINIS |
| | *Nepřímo dotčené určené IS* | *Informační systémy města budou chráněny technickými opatřeními v kybernetické bezpečnosti a budou sledovány systémem pro detekci kybernetických událostí. KS/IS: Vnitřní síť LAN.* |
| **Názvy a odkazy na projekty v katalogu Digitálního Česka nebo jejich ID a názvy**<br>*Nebo informace, proč není součástí katalogu Digitální Česko. Financování z tohoto programu nehraje roli, jedná se o jednotný katalog všech ICT záměrů veřejné správy.* | | *Nerelevantní* |

| **Termíny:** | | |
|---|---|---|
| **Zahájení realizace projektu:** | **Spuštění první služby do produkčního prostředí:** | **Ukončení provozní smlouvy plánované v tomto projektu:** |
| 01. 05. 2022 | 31. 07. 2024 | 31. 08. 2029 |

| **Výhrady ke zveřejnění formuláře:** | |
|---|---|
| **Formulář obsahuje veřejné informace a předpokládá se jeho zveřejnění. Pokud se zveřejněním nesouhlasíte, uveďte důvod, případně úpravy, které budou nutné, aby bylo zveřejnění možné:** | *Neveřejné jsou informace o tom, zda je žadatel povinnou osobou dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB); dále pak informace obsažené v tabulce č. 34: Dopady narušení bezpečnosti informací v systému. Tyto informace nebudou na základě výjimky dle § 10a ZKB veřejnosti poskytovány* |

| **Výjimky:** | | | |
|---|---|---|---|
| **Žádáte výjimku/y vyplývající z nedodržení architektonických principů eGovernmentu nebo jiných skutečností?** | ***Ne*** | **Počet žádostí o výjimku/y v přílohách:** | **0** |

| Tabulka 3: **Shrnutí charakteristik projektu** | |
|---|---|
| **Určení rolí věcného správce, technického správce, provozovatele a dodavatele** (pokud je předmětem více IS, klasifikujte hlavní a ostatní vysvětlete v tabulce 8)**:** | |
| **Věcný správce**<br>*Subjekt, který je investorem předmětu projektu* | **Město Znojmo – manažer kybernetické bezpečnosti** |
| **Technický správce**<br>*Subjekt, který zajišťuje technickou realizaci požadavků věcného správce k předmětu projektu* | **Město Znojmo ve spolupráci s dodavatelem (případně dodavateli).** |
| **Provozovatel**<br>*Subjekt, který zajišťuje provoz HW a SW předmětu projektu* | **Město Znojmo zastoupené úsekem informatiky** |
| **Dodavatel**<br>*Subjekt, který dodává předmět projektu, pokud je znám v době přípravy projektu* | **Dodavatel bude vybrán z veřejné zakázky** |
| **Bylo provedeno hodnocení ekonomické výhodnosti způsobu provozu určených IS?**<br>*Povinnost dle §5 odst. 2 písm. h) zákona č. 365/2000 Sb.* | ***Ano***<br>*Tato analýza je povinná součást žádosti o podporu.* |
| **Realizační** (implementační) **výdaje v rámci projektu** (součet hodnot ve sloupci ① tabulky 51) **v Kč bez DPH:** | 25 574 151 Kč |
| **Provozní výdaje plánované v rámci projektu** (součet hodnot ve sloupci ② tabulky 51) **v Kč bez DPH:** | 2 250 000 Kč |
| **Pětileté TCO projektu** (součet hodnot ve sloupci ③ tabulky 51) **v Kč bez DPH:** | 27 824 151 Kč |

## 1.3. Popis, potřebnost a výstupy projektu

| Tabulka 4: **Popis projektu** |
|---|
| **Popis výchozí situace projektu** (tzv. As-Is, současný stav)**:** |
| Město Znojmo si jako svůj strategický cíl vytklo budování digitálních služeb pro své občany. Nezbytnou součástí digitalizace služeb je kybernetická bezpečnost. Tato oblast na městě dosud nebyla systematicky řešena, chybí dokumentace, systematizace rolí a zodpovědností. Pokud kybernetický incident nastane, řeší se bez standardizovaného postupu. Prvním krokem v této oblasti byla analýza rizik, která také stanovila obsah tohoto projektu.<br>Přístup do místností se servery je řešen pouze přidělováním klíčů odpovědným osobám a místnosti jsou volně přístupné skrz kanceláře. Budova je střežena výstražným systémem, kamery na sledování k dispozici nejsou. Servery mají ochranu AntiX SW, jsou chráněny před výpadky napájení pomocí UPS.<br>Stanice jsou chráněny zastaralým antivirem, který nemá propojení na aktivní komunikační prvky a nechrání proti moderním nebezpečím, jako jsou ransomware, krádež hesel a účtů, neoprávněná těžba kryptoměn, zcizení citlivých osobních dat a další.<br>Řízení identit není centralizováno, město disponuje mnoha informačními systémy, které vyžadují centrální řízení. Množí se duplicity v účtech, přístupy je nutné spravovat ze stále více a více míst. Uspořádání prvků infrastruktury disponuje slabými místy (SPOF) a není připraveno na provoz ve vysoké dostupnosti zejména v oblasti ochrany dat a zálohování.<br>Na technologické úrovni infrastruktura není optimalizována pro provoz služeb vystavených na internet a s tím související rizika kompromitace informačního systému. Přihlašování do informačního systému je řešeno pomocí Active Directory bez vícefaktorové autentizace.<br>Město disponuje softwarem k zajištění sledování síťového provozu a monitoringu aplikací. K reakci na incidenty nejsou přiřazeni žádní pracovníci. Jakýkoliv bezpečnostní incident tak není včas zachycen a následně vyhodnocen může celé organizaci způsobit značnou újmu, co do správného fungování informačního systému.<br>Datová a komunikační infrastruktura města byla budována průběžně a financována dosud z vlastních prostředků. Bylo vytvořeno datové centrum se základními bezpečnostními prvky. Na zprovozněné infrastruktuře byly implementovány klíčové systémy.<br>Důležitým hybatelem pro investování v oblasti ICT byla také pandemie COVID-19, která ukázala význam digitální komunikace a služeb i z jiného než obvykle chápaného pohledu. V dané situaci nejlépe obstála města s infrastrukturou schopnou bezpečné datové komunikace a vzdáleného výkonu práce. |

Tabulka 4: **Popis projektu**

**Popis cílové situace po dosažení celkového cíle / cílů projektu** (tzv. To-Be, budoucí stav)**:**

Projekt má za cíl vybudovat bezpečné prostředí pro běh agendového informačního systému města disponující pokročilou detekcí malware včetně společné reakce prvků bezpečnostní infrastruktury na kybernetickou hrozbu, centrálním řízením identit a vysokou dostupností včetně pokročilé ochrany záloh před neautorizovanou činností tak, aby odpovídalo nárokům na provoz digitálních služeb a splňovalo alespoň minimální standard daný zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. Město nespadá pod působnost kybernetického zákona. Projekt nebuduje z pohledu zákona kritickou informační infrastrukturu.

S vědomím, že nejvíce útoků mívá původ v koncových stanicích, zabezpečení je budováno pokročilou antiX ochranou s blokováním útoků a heuristickou analýzou. Řízení identit je centralizováno a sjednoceno pro všechny informační systémy včetně doplnění dalšího faktoru pro přihlášení (čipové karty).

Nezbytnou součástí pro digitální služby je také infrastruktura s vysokou dostupností a on-line replikací dat, pro případné přepnutí do nodů v případě poruchy či selhání. Tyto nody jsou na sobě nezávislé a jsou umístěny v různých budovách. Pro záložní lokalitu je využit již existující hardware a nové prvky se organicky zapojí do budovaného datového centra. Data jsou zálohována a replikována tak, aby byla chráněna před neoprávněnou změnou, či pozměněním. Zvláštní pozornost je věnována redundanci prvků pro zvýšenou dostupnost informačního systému i v případě útoku zaměřených na odepření služeb a zálohování dat.

Součástí implementace je penetrační test, který prověří, zda nastavená technická opatření skutečně naplňují očekávání a předpoklady. Jeho výsledky pak budou promítnuty do závěrečných úprav před uvedením opatření do provozu.

Vytvoření dokumentace a zavedení pravidel pak umožní v kombinaci se systémy pro detekci bezpečnostních incidentů a souvisejících služeb včasnou reakci na zjištěné incidenty a jejich řešení bez vážnějších dopadů.

Město po dokončení disponuje infrastrukturu mnohem více odolnou proti kybernetickým hrozbám, zaměstnanci jsou proškoleni a vyhýbají se rizikovému chování. Jsou nastaveny politiky, je zhotovena dokumentace a město je schopno reagovat na kybernetický incident. Je také zaveden systém včasného varování a prevence pomocí služeb bezpečnostního dohledu.

**Popis změn, tzn. výsledků / výstupů projektu nezbytných k dosažení jeho specifického cíle / účelu:**

Zásadní změnou bude vypracování bezpečnostní dokumentace a její udržování v aktuálním stavu. Vypracování dokumentace a její aktualizace bude zajištěna externím subjektem, neboť město nedisponuje dostatečnou znalostí problematiky kybernetické bezpečnosti. Bezpečnostní dokumentace bude obsahovat především pravidla pro uchovávání a vytváření hesel a vydefinované procesy, podle kterých bude nutné postupovat v případě bezpečnostního incidentu.

Dalším krokem je zajištění dostatečných znalostí o kybernetické bezpečnosti u zaměstnanců města prostřednictvím zajišťování pravidelných školení k problematice kybernetické bezpečnosti. Tyto opatření budou také doplňovány pravidelnými penetračními testy.

Dále bude pořízen potřebný software a hardware pro monitorování bezpečnostních rizik a zajištění prevence před možnými bezpečnostními incidenty.

Stávající infrastruktura budu použita pro běh méně exponovaných aplikací (tj. takové, které se používají interně nebo jejich nefunkčnost nemá zásadní dopady na provoz města), další část infrastruktury bude vyčleněna pro redundantní záložní provoz v jiné místnosti (úřad disponuje velkou modernizovanou budovou). Tímto dojde k rozčlenění infrastruktury do různých lokalit, které jsou ve vlastnictví města.

Město dále využije veškeré softwarové licence infrastrukturního SW, zejména licence databází. Stávající dokumentace bude rozšířena o nové prvky, interní směrnice pro kybernetickou bezpečnost budou pravidelně aktualizovány a doplňovány na základě zkušeností.

**Služba bezpečnostního dohledu** – jedná se o provozní službu s cílem zajistit včasnou reakci na incidenty a vykrytí zvýšených personálních nároků. Pracoviště dohledu, které zabezpečí detekci sledované události ve velmi krátké době po její aktivaci. V rozmezí od ihned do maximálně několika minut. Následně předá k řešení odpovědnému správci ICT (aplikace, technologie, apod.). Tomuto správci zajišťuje také podporu, pomoc a metodické vedení pro vyřešení kybernetického incidentu. Tuto službu zajistí dodavatel technických opatření vzešlý z veřejné zakázky. V souvislosti s dodávkou projektu se očekává uzavření nové smlouvy o podpoře s vítězem veřejné zakázky.

Výsledky v seskupení:

Tabulka 4: **Popis projektu**

- Technická (investiční náklady viz tabulka 51, způsob jejich provedení je charakterizován modely):
  - IDM – správa identit
  - AntiX Ochrana
  - Zvýšení odolnosti a dostupnosti infrastruktury
  - Penetrační test pro prověření funkčnosti a správnosti opatření
  - Bezpečnostní dokumentace a plány
- Personální (provozní náklady viz tabulka 51):
  - Současná správa ICT bude navýšena o další kapacity pro správu nově dodaných prvků.
  - Součásti projektu pro kybernetickou bezpečnost je **služba bezpečnostního dohledu**, kterou bude vykonávat dodavatel vzešlý z veřejné zakázky.
  - Vítězný dodavatel také zajistí pravidelnou aktualizaci řešení (bezpečnostní záplaty, update apod.)
  - Vítězný dodavatel také zajistí L2 a L3 podporu pro správu ICT
  - Aktualizace bezpečnostní dokumentace
  - Zajištění kapacit na vyřešení kybernetického incidentu podle potřeby.
- Organizační (běžné režijní náklady)
  - Zajištění a kontrola SLA na obnovu činnosti.
  - Kontrola SLA a způsob reakce na kybernetický incident.
  - Komunikační matice a plán kontinuity činností po havárii.
  - Zajištění nezbytné součinnosti.
  - Zavedení bezpečnostních politik a jejich vynucování.
- Finanční:
  - Město disponuje dostatečným rozpočtem pro zajištění výše zmíněných činností.
  - Do rozpočtu města budou alokovány částky včetně rezerv pro řešení rozsáhlejších havárií při bezpečnostních incidentech.

| **Důvody realizace projektu** (označte všechny relevantní)**:** | | | |
|---|---|---|---|
| Legislativní důvody | ☐ | Konec licencí | ☐ |
| Modernizace, optimalizace řešení (výsledky business analýz) | ☒ | Lepší nabídka trhu | ☐ |
| Požadavky zaměstnanců, uživatelů | ☒ | Konec podpory od dodavatele | ☐ |
| Konec podpory produktu, vynucené modernizace nižších vrstev | ☐ | Jiné (vysvětlete v tabulce 8) | ☒ |
| Hospodárnost | ☒ | | |

| Tabulka 4: **Popis projektu** |
|---|
| **Přehled zvažovaných alternativ řešení rozdílných od „Popisu projektu“** (tzv. To-Be) **specifikovaného výše:** |
| Nulová varianta, tj. ponechání v současném stavu – nevyhovující. Pod pojmem nulová varianta se rozumí nepřistoupení k realizaci projektu za daných podmínek. Město, aby se vyhnulo škodám vyplývajících z kybernetických hrozeb, tak nebude budovat žádné služby v portálu občana. Škody z napadení vnitřího informačního systému bude mnohem více pravděpodobná. Náklady na hrazení škod jsou nepoměrně vyšší než náklady na zabezpečení. V případě bezpečnostního incidentu tak bude ORP vystavena velkému nebezpečí odcizení dat, případně poškození důležitých aplikací informačního systému.<br><br>Minimální varianta – Tato varianta řešení počítá pouze s využitím pouze stávajících kapacit ICT bez rozšíření a konsolidace z výzvy a jejich realizací pouze pomocí vlastních prostředků města. Klíčovým rozdílem mezi nulovou variantou a touto variantou je to, že projekt bude realizován, na rozdíl od nulové, ale nebude využita výzva IROP 03, tudíž bude realizován v minimálním rozsahu v dlouhém čase.<br><br>Nájem nebo outsourcing – na řešení v této variantě nelze získat dotaci dle výzvy IROP 03, a proto je v konečném důsledku nevýhodná a v podstatě shodná s variantou budování vlastními prostředky. Pouze se liší způsobem profinancování a provozování.<br><br>Další variantou by mohlo být využití Government Cloudu (Gcloud). Vzhledem k opakovaným odkladům a aktuální neznalosti závazného termínu spuštění provozu není tato varianta využitelná. S rozvojem GCloudu souvisí úvaha nabízení služeb dalším městům – v této chvíli zkušenosti z kybernetických incidentů a jejich zvládání. V dalších částech projektu můžeme nabídnout provozování automatizovaných procesů pro výběr místních poplatků obcím ve svém správním obvodu, ale to je otázkou politického rozhodnutí. Toto rozhodnutí bude provedeno po vyhodnocení zkušeností z provozování automatizovaných procesů a zvládání kybernetických incidentů.<br><br>Cloudové řešení – s ohledem na záměr provozovat na tomto prostředí klíčové digitální služby městské korporace a znalostem interního týmu ICT. Nutností čelit riziku úpadku nebo jinému důvodu odepření služeb cloudu se snižuje výhodnost nákladových úspor, protože interní tým musí zálohovat prostředí. Dále také s ohledem na finanční model výzev je s ohledem na péči řádného hospodáře efektivnější vlastní provoz.<br><br>Vlastní vývoj aplikací je zjevně nehospodárný.<br><br>Rozvojová varianta – realizací dojde k odstranění problémů kybernetické bezpečnosti města. Cílový stav počítá s kvalitně zpracovanými bezpečnostními politikami, nastavenými procesy a pravidly, která budou uplatňována v praxi a přispějí k větší bezpečnosti informačního systému a jednotlivých aplikací a snížení rizika výskytu bezpečnostních incidentů. Díky realizaci projektu bude značně sníženo riziko poškození informačních systému, případně odcizení dat.<br><br>**Město se rozhodlo pro rozvojovou variantu** |

| Tabulka 5: **Přehled výstupů projektu – Ceny bez DPH** | | | | |
|---|---|---|---|---|
| **Označení výstupu** | **Množství a jednotka** | **Celková cena výstupu** [Kč] | **Plánovaná životnost výstupu [rok]** | **Vysvětlení výstupu** |
| Bezpečnostní dokumentace | 1 ks | 110 000 Kč (V rozpočtu projektu je zahrnuta do puašálních výdajů na provoz, je tedy zahrnuta v celkové částce) | 5 let a více | Kvalitní bezpečnostní dokumentace je nezbytným nástrojem k dosažení cíle tohoto projektu. Díky bezpečnostní dokumentaci budou jasně definovaná pravidla i procesy, jak bojovat s bezpečnostními incidenty, jakož i další pravidla, která zajistí prevenci před takovými incidenty.<br>Dokumentace bude pravidelně aktualizována, ať už bude projekt realizován nebo ne. |
| Příprava projektu | 1 ks | 410 000 Kč | Příprava projektu | Nutná součást projektové dokumentace a příprava projektu. |

| Tabulka 5: **Přehled výstupů projektu – Ceny bez DPH** | | | | |
|---|---|---|---|---|
| **Označení výstupu** | **Množství a jednotka** | **Celková cena výstupu** [Kč] | **Plánovaná životnost výstupu [rok]** | **Vysvětlení výstupu** |
| IDM – správa identit | 1 ks | 5 028 940 Kč | IDM – správa identit | Nástroj pro ověřování identity uživatelů a administrátorů zajišťuje ověření identity uživatelů a administrátorů před zahájením jejich aktivit v informačním systému. |
| AntiX Ochrana | 1 celek | 2 906 525 Kč | AntiX Ochrana | Jedná se o vícevrstvou ochranu, která umožňuje bojovat proti celé řadě škodlivých činností. Zejména proti krádeži hesel a účtů, neoprávněné těžbě kryptoměn, zašifrování souborů pomocí ransomwaru, získání citlivých osobních údajů, spamu, podvodům a dalším formám kybernetických útoků. |
| Zvýšení odolnosti a dostupnosti infrastruktury | 1 celek | 15 865 611 Kč | Zvýšení odolnosti a dostupnosti infrastruktury | Jedná se o prostředí podporující virtualizaci a plynulý chod informačních systémů. Dále se jedná zajištění redundance a o vyloučení úzkých míst, aby služby infrastruktury byly stále dostupné. |
| Penetrační test | 1 celek | 100 000 Kč | Penetrační test | Provedení penetračních testů a následně jejich pravidelné opakování |
| Dozor nad implementací opatření | 1 celek | 100 000 Kč | Dozor nad implementací opatření | Konzultace a technická pomoc při implementaci projektu a jeho bezpečnostních opatření.<br>S ohledem na šíři problematiky může být daná aktivita vhodně rozdělena podle potřeby na části. |
| Příprava a organizace veřejné zakázky, právní služby | 1 ks | 250 000 Kč | Příprava a organizace veřejné zakázky, právní služby | Realizace veřejné zakázky v souladu se zákonem o ZVZ. |
| Administrace projektu, management dotace | 1 ks | 150 000 Kč | Administrace projektu, management dotace | Vedení dokumentace k prokazování vůči poskytovateli dotace |
| Publicita stálá pamětní deska | 1 ks | 4 000 Kč | Publicita stálá pamětní deska | Publicita v rozsahu daného projektem vyplývající z podmínek výzvy |
| Ostatní náklady spojené s řízením a realizací projektu | 1 ks | 759 075 Kč | Ostatní náklady spojené s řízením a realizací projektu | Činnosti nutné k realizaci projektu a s ním související nespecifikované. |
| Školení pro zaměstnance | 1 ks | 0 Kč (financuje jiný projekt) | Jedná se o školení | Slouží k omezení rizikového chování zaměstnanců a pro pochopení rizik. |

## 1.4. Právní klasifikace specifického cíle / účelu projektu

| Tabulka 6: **Klasifikace specifického cíle / účelu projektu dle legislativy eGovernmentu (pokud je v rámci projektu realizováno více IS, klasifikujte hlavní a ostatní vysvětlete)** | | |
|---|---|---|
| **Klasifikace** | **Vyberte** | |
| **Druh informačního systému dle klasifikace zák. č. 365/2000 Sb., o informačních systémech VS** | **Provozní informační systém nepodléhající zák. 365/2000 Sb.** | |
| **Je projektem dotčen (tj. realizován nebo na úrovni jeho procesní a aplikační architektonické vrstvy měněn) určený informační systém dle zák. č. 365/2000 Sb., o informačních systémech VS?** | **Ano - VYPLŇTE DLE JAKÉHO KRITÉRIA** | ☑ 1. Využívá služby referenčního rozhraní nebo poskytuje služby referenčnímu rozhraní<br>☑ 2. Má vazbu na systém dle bodu 1<br>☐ 3. Je určený k poskytování služby fyzickým nebo právnickým osobám s předpokládaným počtem uživatelů, kteří využívají přístup se zaručenou identitou, alespoň 5000 ročně |
| **Je projektem dotčen agendový informační systém dle zákona č. 111/2009 Sb., o základních registrech?** | **Ano** | |
| **Budou informačním systémem, který je projektem dotčen, přijímány a odesílány datové zprávy dle zák. č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů?** | **Ano** | |
| **Druh informačního / komunikačního systému dle klasifikace stanovené zákonem č. 181/2014 Sb., o kybernetické bezpečnosti** | **Nespadá pod definici dle ZoKB** | |
| **Bezpečnostní úroveň informačního systému dle vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci** | **Bezpečnostní úroveň nízká** | |

## 1.5. Přínosy (celkový cíl / cíle) projektu

Tabulka 7: **Strukturovaný přehled přínosů (celkového cíle / cílů) projektu včetně uvedení objektivně ověřitelných ukazatelů jejich dosažení a zdrojů a prostředků jejich ověření**

**Přínosy na straně uživatelů** (např. snížená časová nebo administrativní náročnost oproti vyřízení aktivity dosavadním způsobem, vyšší ochrana osobních dat aj.)**:**

Vytvořením pravidel bude zajištěno, že každý zaměstnanec bude znát své povinnosti, rizika a odpovědnosti v případě bezpečnostních incidentů. Při práci s informačními systémy budou mít zaměstnanci jistotu zabezpečení před odcizením citlivých dat a údajů. Nastavená pravidla umožní pružnou reakci na potencionální bezpečnostní incidenty tak, aby nebylo ohroženo poskytování služeb.

Ve stručnosti – uživatelé:

- využívají bezpečnou službu,
- zmenšení obav z úniků důvěrných dat,
- vznik infrastruktury pro elektronické služby,
- snížení škod plynoucích z kybernetické kriminality,
- kontrola stanice před nákazou malwarem,
- vyšší ochrana osobních dat.

**Měřitelná kritéria pak definuje Tabulka č. 14.**

**Přínosy na straně věcného správce** (zvýšení kvality jeho výstupů, snížení pracnosti na straně jeho úředníků aj.)**:**

Díky zvýšení kybernetické bezpečnosti bude značně omezeno riziko odcizení citlivých dat a údajů. Věcný správce dále získá nové nástroje (bezpečnostní dokumentace, technické nástroje a proškolené zaměstnance), díky kterým bude moci předcházet bezpečnostním incidentům a efektivně je řešit v případě že nastanou.

Ve stručnosti – věcný správce získá:

- zajištění bezpečnosti prostředí pro výkon agend,
- omezení rizik kybernetické kriminality,
- rychlejší detekce bezpečnostních událostí,
- zvýšení schopnosti práce s elektronickými dokumenty,
- zvýšení efektivity práce,
- uživatel se dostane pouze ke službám a datům, na která má oprávnění (autorizaci),
- zvýšení hospodárnosti a nákladů na výkon veřejné správy,
- lepší možnosti pro budování samoobslužných služeb,
- omezení pravděpodobnosti škody z kybernetického incidentu příjmem zpráv pouze přes kontrolované brány.

**Měřitelná kritéria pak definuje Tabulka č. 14.**

**Přínosy pro technického správce a provozovatele služby** (snížení energetické náročnosti, zjednodušení a úspora pracnosti správy systému, snížení výdajů na provoz aj.)**:**

Předcházení bezpečnostním incidentům a jejich efektivní řešení v první řadě přispěje k větší spolehlivosti provozovaného softwaru a infrastruktury.

- získání nových nástrojů na ochranu infrastruktury,
- centralizace správy identit,
- snížené náklady na řešení následků kybernetického útoku,
- včasné zachycení bezpečnostních hrozeb,
- zlepšení provozních charakteristik,
- omezení prostoru pro průnik útočníka a z toho vyplývajících škod,
- významně vyšší spolehlivost provozu služeb,
- prevence škod vyplývajících z kybernetické kriminality,
- značné snížení nákladů na správu spočívající v nápravě škod po kybernetickém incidentu.

**Měřitelná kritéria pak definuje Tabulka č. 14.**

Tabulka 8: **Vysvětlení k základním podmínkám dosažení přínosů (nutným předpokladům a rizikům dosažení celkového cíle / cílů) projektu**

V rámci projektu byly nalezeny a vymezeny základní rizikové faktory, které jsou příčinou či zdrojem rizika, které je neoddělitelnou součástí řízení projektů. Tyto faktory se objevují zejména v předpokládaných veličinách, které jsou pro výsledky projektu, jeho realizovatelnost a smysluplnost, významné. Jejich hodnoty a průběh je nutné předem co nejlépe odhadnout a zvažovat následky, které může omyl v tomto odhadu mít. Dalším logickým krokem je snaha o vymezení nástrojů a procesů, kterými lze tyto důsledky snížit – definice tzv. eliminačních opatření.

Tabulka 8: **Vysvětlení k základním podmínkám dosažení přínosů (nutným předpokladům a rizikům dosažení celkového cíle / cílů) projektu**

Základní oblasti, které je nutno řešit jsou:

- Motivace:
  - Rozhodující skupiny musí být přesvědčeny o tom, že tento projekt pro organizaci nebo její okolí znamená přínos.
  - Tým podílející se na zvládání incidentů bude motivován odměnami.
- Právní podmínky – v průběhu projektu existuje riziko změn podmínek.
  - Změny jsou řešeny pomocí smlouvy o podpoře, která obsahuje legislativní upgrade a update.
  - Problémy se zajištěním záruk a servisních služeb – jsou řešeny pomocí smluvních sankcí.
  - Nevyřešené vlastnické vztahy – toto riziko nehrozí, protože všechny prostředky jsou vlastněny městem.
  - Problémy se zajištěním součinnosti partnerů – řešeno jasnými a přesnými vyjádřeními smluvních kompetencí.
  - Nedodržení podmínek IROP – projektovým řízením a administrací budou pověřeni zkušení pracovníci, případně bude využita externí odborná podpora.
- Organizační rizika
  - Zajištění součinnosti ze strany města – management úřadu stanoví prioritu projektu a podle toho budou alokovány nutné zdroje.
  - Nedodržení termínu realizace – důsledné definování harmonogramu všemi zúčastněnými stranami a zajištění dodržení všech kvalitativních ukazatelů ve smlouvách, sankce za zpožďování a neplnění dodávky.
  - Zpoždění veřejné zakázky – zahájení přípravy výběrového řízení na dodavatele ještě v přípravné etapě projektu před schválením rozhodnutí o poskytnutí dotace.
  - Nedostatečná koordinace prací – projektové vedení se bude pravidelně scházet a koordinovat postup prací dle vypracovaných plánů.
- Technická rizika
  - Nedostatky v projektové dokumentaci – důsledné plánování přípravy a schvalování projektové dokumentace. Zajištění zkušeného týmu pro precizaci zadání.
  - Dojde ke kompromitaci dat – důsledná ochrana dat šifrováním, sestavení plánu obnovy a reakce na incidenty.
  - Dojde k využití bezpečnostní chyby a instalaci malware – pravidelná aktualizace a záplatování produktů v infrastruktuře. Detekce podezřelého chování v rámci vnitřní a vnější sítě pomocí služby bezpečnostního dohledu.
  - DDos útok – ochrana pomocí technických prvků.
- Finanční rizika:
  - Neobdržení dotace – zpomalení projektu a jeho realizace z rozpočtu města postupnými kroky.
  - Zvýšení cen vstupů – technická podpora a další související služby bude také soutěžená zároveň a bude zaručena její cena.
  - Zvýšení DPH – znamená nárůst plateb dodavatelům v provozní fázi. Je nutno alokovat rezervy pro pokrytí tohoto nárůstu.
  - Náhlé výdaje v souvislosti s incidentem nebo havárií – alokace peněz v rozpočtu města i na havárie tohoto typu.
  - Omezené zdroje města – vždy bude potřeba pečlivě zvažovat efektivitu opatření a náklady na něj.
- Provozní rizika:
  - Neplnění dodavatelských smluv – důsledné vymáhání dohodnutých SLA a pečlivé smluvní ošetření sankčních ujednání za jejich neplnění.
  - Zahlcení helpdesku nepodstatnými chybami – pečlivé prověření incidentů a jejich priority s oboustranným odsouhlasením.
  - Dlouhá reakce na požadavek – ošetření reakčních dob v servisní smlouvě.
  - Úpadek dodavatele – důsledná dokumentace řešení a dodržení Exit strategie.
- Personální rizika:
  - Navýšení personálních kapacit – projekt počítá s navýšením personálních kapacit na provozní správu dalších prvků. Dále také počítá s využitím služeb bezpečnostního dohledu na pokrytí potřeb odborných sil nutných ke zvládnutí bezpečnostního incidentu.
  - Nedostatek kapacit na trhu – smluvní ujednání zajišťující alokaci kapacit po celou dobu trvání projektu.

# 2. ARCHITEKTONICKÉ INFORMACE O PROJEKTU

## 2.1. Dodržení architektonických principů NA VS ČR

| Tabulka 9: **Dodržení architektonických principů Národní architektury veřejné správy ČR** | | | |
|---|---|---|---|
| **Klasifikace** | **Vyberte** | **Č. žádosti o výjimku** | **Vysvětlete** |
| Standardně digitalizované | **Nerelevantní** | | |
| Zásada „pouze jednou“ | **Nerelevantní** | | |
| Podpora začlenění a přístupnost | **Nerelevantní** | | |
| Otevřenost a transparentnost | **Nerelevantní** | | |
| Přeshraniční přístup jako standard | **Nerelevantní** | | |
| Interoperabilita jako standard | **Nerelevantní** | | |
| Důvěryhodnost a bezpečnost | **Ano** | | Projekt je zaměřen na posílení důvěryhodnosti a bezpečnosti digitálních služeb. |
| Jeden stát | **Nerelevantní** | | |
| Sdílené služby veřejné správy | **Nerelevantní** | | |
| Připravenost na změny | **Ano** | | Součástí projektu je také update i upgrade včetně legislativního. |
| eGovernment jako platforma | **Nerelevantní** | | |
| Vnitřně pouze digitální | **Nerelevantní** | | |
| Otevřená data jako standard | **Ano** | | Město plánuje publikaci otevřených dat a to počet kritických incidentů a útoků na infrastrukturu. |
| Technologická neutralita | **Nerelevantní** | | |
| Uživatelská přívětivost | **Nerelevantní** | | |
| Konsolidace a propojování | **Nerelevantní** | | |
| Omezení budování monolitických systémů | **Nerelevantní** | | |

## 2.2. Enterprise architektura projektu a její kontext

| Tabulka 10: **Architektonický model** | |
|---|---|
| **V rámci Enterprise Architektury projektu přiložte jako přílohu model exportovaný ve standardizovaném výměnném formátu The Open Group ArchiMate Model Exchange File Format** | Ano, model je přiložen jako příloha ve standardizovaném formátu |
| **Případně vysvětlete, proč není model přiložen ve standardizovaném formátu či není přiložen vůbec.** | Model ve formátu archimate, který je ve veřejné správě doporučen k použití, zašleme na vyžádání. Tento formát neakceptuje datová schránka. Adresa pro vyžádání je janecka@hcmcomputers.cz |

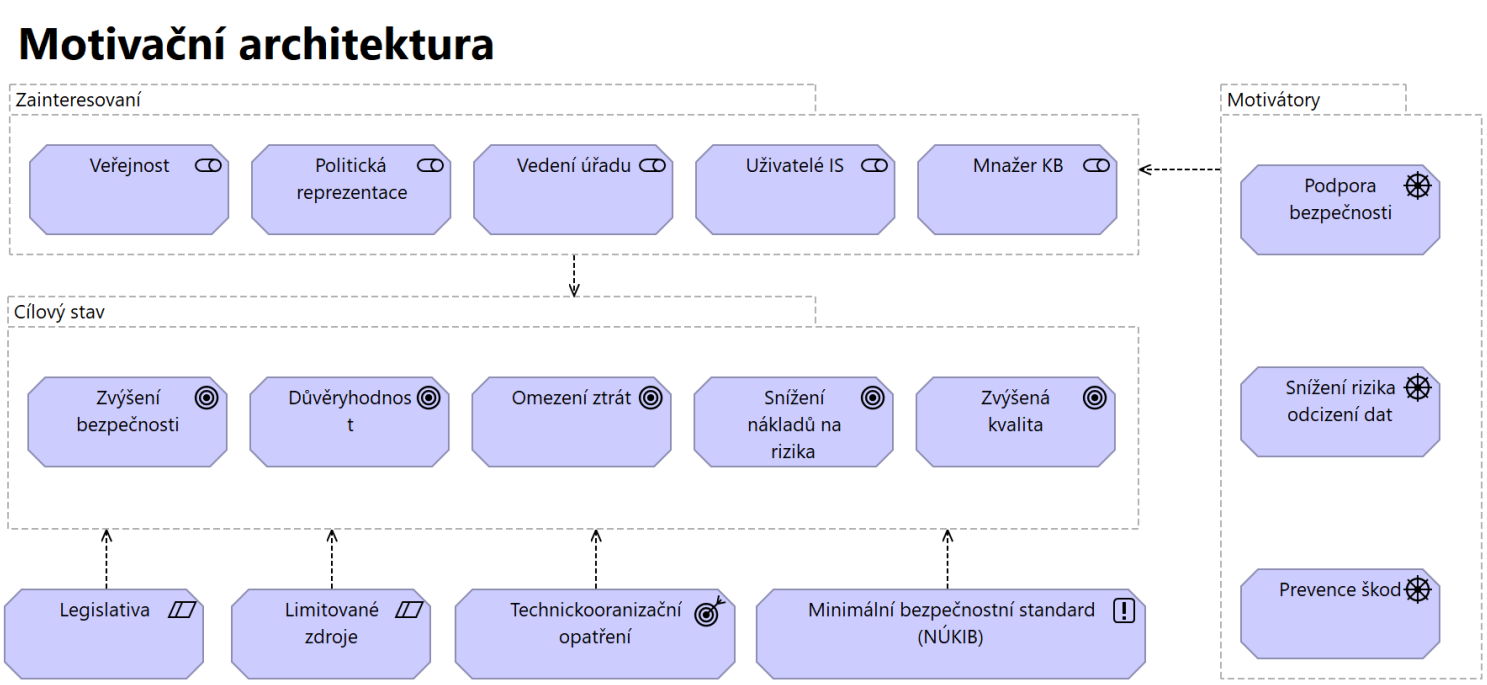
### 2.2.1. Motivační architektura – strategie a směrování

| Tabulka 11: **Vysvětlete, proč projekt realizujete v této podobě a čeho jím chcete dosáhnout.** Pro vysvětlení motivace použijte zejména pojmy z odpovídajícího modelu motivační architektury (motivátory, zainteresované osoby, cíle, principy, podmínky, architektonické požadavky)**:** |
|---|
| Projektem chceme dosáhnout především možnosti provozovat digitální a infrastrukturní služby města, jak máme definováno v našich strategických dokumentech. Cílem je zlepšení kvality služeb, zvýšení zastupitelnosti, snížení administrativní zátěže a poskytnutí služeb města včetně jeho organizací.<br>Strategický plán rozvoje ICT města Znojmo definuje vizi „7.4 Vize rozvoje ICT v oblasti bezpečnosti“, kde uvádí potřebu města digitalizovat služby, zajistit spolehlivost a bezpečnost informačního systému města. |

| Tabulka 11: **Vysvětlete, proč projekt realizujete v této podobě a čeho jím chcete dosáhnout.** Pro vysvětlení motivace použijte zejména pojmy z odpovídajícího modelu motivační architektury (motivátory, zainteresované osoby, cíle, principy, podmínky, architektonické požadavky)**:** |
|---|
| Další motivační prvky vyplývají z podstaty kybernetické bezpečnosti. Město nespadá pod mezi povinné subjekty podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti, ale pro své potřeby chce využívat jako standard materiál NUKIB „Minimální bezpečnostní standard“.<br>Jedním z důvodů pro realizaci projektu je získat návod (proces), jak reagovat na bezpečnostní incident, když nastane a jak poznat, že nastal.<br>Další motivací je obrana proti odcizení dat nebo jejich zničení. Hodnota dat je vyčíslitelná prací vloženou do jejich pořízení, tedy za dobu fungování města jde řádově o stamiliony korun. Proto město hodlá pořídit detekční mechanismy, zálohování a spisové služby pro organizace pro řízení oběhu (přístupu) dokumentům.<br>Omezení financemi chce město řešit podporou projektu z výzvy IROP, omezení personálními kapacitami je město připraveno řešit nákupem kapacit a to jak pro správu, tak pro bezpečnostní dohled. |

| **Tabulka 12: Katalog prvků motivační architektury** | | | |
|---|---|---|---|
| **ID** | **Typ prvku** | **Jméno prvku** | **Popis prvku** |
| | | | |

**Diagram motivační architektury**

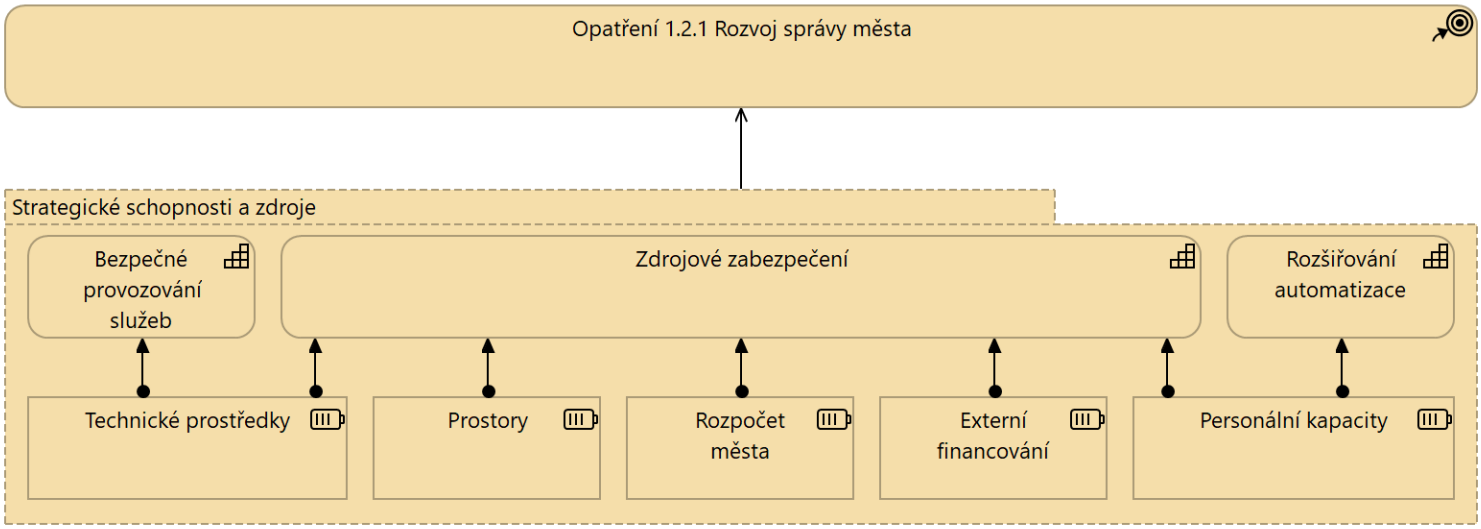



| Prvek | Popis |
|---|---|
| **Grouping** | |
| Zainteresovaní | Seskupení zájmových skupin pro zjednodušení modelu. |
| Cílový stav | Skupina cílů, kterou je nutné dosáhnout. |
| Motivátory | Skupina motivátorů (hnacích prvků) pro zainteresované. |
| **Zájmové skupiny (zainteresovaní)** | |
| Veřejnost | Občanská veřejnost využívající služby nebo budované portály. |
| Politická reprezentace | Zástupci veřejnosti, kteří prosazují svůj politický program. |
| Vedení úřadu | Vedení úřadu města Slavičín, které realizuje politický program samosprávy nebo vykonává přenesenou působnost. |
| Uživatelé IS | Uživatelé informačního systému města. |

| | |
|---|---|
| Manažer KB | Manažer kybernetické bezpečnosti – ať už jde nakoupenou službu nebo interního člena týmu. |
| **Omezující podmínky** | |
| Legislativa | Právní prostředí pro výkon veřejné správy. |
| Limitované zdroje | Limitované zdroje alokované do rozpočtu města vynucující zásadu – udržení poměru cena výkon. |
| **Motivátor** | |
| Podpora bezpečnosti | Podpora bezpečnosti procesu zpracování dat v rámci práce úřadu je klíčová s ohledem na rizika vyplývající z kybernetické kriminality nebo obecně z rizik zneužití agendových informačních systémů. |
| Snížení rizika odcizení dat | Snížení rizika odcizení dat a z toho plynoucích následků. |
| Prevence škod | Prevence škod vzniklých kybernetickou kriminalitou. |
| **Cíl** | |
| Zvýšení bezpečnosti | Vnitřní prostředí pro práci informačního systému je bezpečné, rizika jsou v rozumné míře omezena a lze omezit známá rizika. |
| Důvěryhodnost | Důvěryhodnost znamená, že se veřejnost nemusí obávat svěřit veřejné správě svá data, obavy z jejich zneužití jsou tak menší. |
| Omezení ztrát | Omezení ztrát vyplývajících z možných poškození vnitřní infrastruktury vyplývající z napadení nebo realizace nežádoucích aktivit ve vnitřní síti. |
| Snížení nákladů na rizika | Díky bezpečnostním opatřením je možné eliminovat rizika, která jsou momentálně eliminována s vyššími náklady. Lze tedy tuto činnost vykonávat ve vyšší kvalitě za nižší náklady. |
| Zvýšená kvalita | Zvýšená kvalita fungování informačního systému. |
| **Výstup** | |
| Technickooranizační opatření | Technickooranizační opatření v rámci výstupů vykonávaného projektu, ať už jde o bezpečnostní dokumentaci, změnu procesů, školení zaměstnanců, či technické prvky nakupované pro zvýšení kybernetické bezpečnosti. |
| **Princip** | |
| Minimální bezpečnostní standard (NÚKIB) | Obec s rozšířenou působností nebude zpravidla povinným subjektem podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti. Z toho důvodu byl Národním úřadem pro kybernetickou a informační bezpečnost vydán dokument, který alespoň rámcově vymezuje pravidla kybernetické bezpečnosti pro subjekty, které pod uvedený zákon nespadají. |

Strategické cíle jsou popsány v příslušných koncepčních dokumentech

# Strategické cíle města




| Prvek | Popis |
|---|---|
| **Zdroje** | |
| Prostory | Prostor pro umístění prostředků (servery, síťové prvky, stanice apod.). |

| | |
|---|---|
| Technické prostředky | Technické prostředky zajišťující chod služeb. Tyto prostředky umožňují provádět realizaci takových procesů – jedná se o technologické centrum a další prvky technologické vrstvy. |
| Rozpočet města | Prostředky obce zajišťující chod nebo malý rozvoj automatizovaných procesů. |
| Externí financování | Investiční prostředky pro rozvoj a nákup technologií potřebných pro automatizaci. Externími prostředky se míní podaný a schválený projekt pro obec jako žadatele. |
| Personální kapacity | Personální kapacity zajišťující rozvoj nebo provoz a obsluhu služeb. Samotný výkon je prováděn strojovými prostředky. |
| **Schopnost** | |
| Bezpečné provozování služeb | Bezpečné provozování služeb podporující procesy organizace je základní schopnost pro jeho výkon. Služby musí být natolik bezpečné, aby nebyla odmítána klienty / interními pracovníky pro její nedůvěryhodnost nebo nuceně zastavena, protože je snadno napadnutelná. |
| Zdrojové zabezpečení automatizace | Schopnost poskytnout potřebné zdroje k běhu automatického procesu. |
| Rozšiřování automatizace | Schopnost organizace neustrnout na místě a pokračovat v rozvoji nebo zlepšování procesů směrem k automatizaci nebo reagovat na měnící se poptávku. |

### 2.2.2. Efektivita projektu – výkonnostní architektura

| **Tabulka 13: Vysvětlete dopad projektu na hospodárnost, účelnost, účinnost, časovou a kvalifikační náročnost a na kvalitu služeb v organizaci (viz metodika TCO zveřejněná zde):** |
|---|
| Z hlediska nákladů současného stavu vybudování společného centra služeb znamená úsporu provozních nákladů na straně města i jeho organizací, organizace města nemusí vydávat prostředky na kybernetické zabezpečení a provoz běžných služeb.<br>Z hlediska transparentnosti a hospodárnosti díky veřejné zakázce dojde k výběru nejlepší nabídky.<br>Z hlediska efektivity provozu není nutné vynakládat značné náklady na nápravu škod vyplývajících z kybernetických událostí.<br>Z hlediska personálních nákladů u odborných útvarů jde zlepšení zastupitelnosti (část práce vykoná samoobslužný proces, jehož realizace bude možná díky adekvátnímu zabezpečení).<br>Z hlediska klienta (občana) jde o možnost nabízení vybraných služeb úřadu v režimu 24/7, jelikož bude disponovat k tomu adekvátními bezpečnostními opatřeními. Z toho vyplývá úspora času na straně klienta, není omezen otvírací dobou (úředními hodinami), ale i značná úspora na provozních nákladech městu, protože zajistit úřední hodiny 24/7 je mnohonásobně dražší než digitálně provedená služba.<br>Z hlediska služeb jde o výrazné snížení rizika odcizení citlivých data a úspěšného útoku na informační systém města.<br>Díky bezpečnostní dokumentaci ví každý, co má dělat, jak si počínat a škody tak nenásobí chaotické počínání.<br>Zvýšení povědomí pracovníků o kybernetických rizicích a především kodifikace pravidel předcházení těmto rizikům povede ke zvýšení prevence bezpečnostních rizik a následně ke snížení nákladů vynakládaných na jejich odstraňování.<br>Proto náklady vydané na zvýšení kybernetické bezpečnosti jsou z tohoto pohledu přijatelné, oprávněné a ekonomicky výhodné. |

| **Tabulka 14: Přehled požadovaných cílových parametrů SLA nových nebo měněných služeb** | | | |
|---|---|---|---|
| **Název v rámci projektu nově zřizované nebo měněné služby** | **Specifikace SLA parametru služby** | **Sjednaná mezní hodnota SLA parametru** | **Sjednaný způsob měření hodnoty SLA** |
| **Zvýšení odolnosti a dostupnosti infrastruktury** | Maximální doba souvislého výpadku | 8 hodin v PD | Interní monitorování služeb |
| **Zvýšení odolnosti a dostupnosti infrastruktury** | Doba dostupnosti infrastruktury | 24 x 7 mimo údržbu | Interní monitorování služeb |
| **Obecná SLA pro služby** | Kritická chyba | Do 8 hodin v PD | Servis desk technické podpory |
| **Obecná SLA pro služby** | Urgentní chyba | Do 48 hodin v PD | Servis desk technické podpory |
| **Obecná SLA pro služby** | Chyba | Do 80 hodin v PD | Servis desk technické podpory |
| **Obecná SLA pro služby** | Doba dostupnosti spisové služby | 99,99 % v pracovní době | Interní monitorování služeb |
| **AntiX ochrana** | Omezení nakažení stanice | 100% záchyt známého nebezpečí | Interní měření podle reálné práce |
| **IDM** | Omezení počtu uživatelů mimo IDM | Pouze povolené výjimky | Interní zdroje |
| **Pracovní doba (PD) je 6:00 – 18:00** | | | |

| Tabulka 15: Popis povinných objektivně ověřitelných ukazatelů výkonnosti (příklad získání a výpočtu hodnot je uveden v metodice k tomuto formuláři; pokud nejsou zde uváděné objektivně ověřitelné ukazatele běžně dostupné, jako mohou být např. údaje o spokojenosti uživatelů nebo preferencích el. služby před neelektronickou, musí být jejich získání zahrnuto do projektu a zohledněno ve zdrojích nezbytných pro jeho realizaci a provoz) | | | | | |
|---|---|---|---|---|---|
| **Název nově zřizované nebo měněné služby** | **Předpokládaný počet transakcí za rok** | **Náklady na dokončenou transakci bez DPH? [Kč]** | **Jaké % uživatelů je spokojeno s poskytovanou službou?** | **Jaké % transakcí je úspěšně dokončeno?** | **Jaké % uživatelů zvolí raději elektronickou formu služby než ne-elektronickou?** |
| **Systém není zaměřen na transakce.** | | | | | |

| Tabulka 16: Popis volitelných objektivně ověřitelných ukazatelů výkonnosti | | | | |
|---|---|---|---|---|
| **Název ukazatele** | **Předmět měření** | **Jednotka** | **Očekávaná hodnota od** | **Očekávaná hodnota do** |
| **AntiX ochrana** | Počet chráněných stanic a zařízení | **Počet** | 120 | 280 |
| **IDM – správa identit** | Počet uživatelů | Počet | 100 | 450 |
| **Zvýšení odolnosti a dostupnosti infrastruktury** | Doba obnovy | **Čas** | 8 hodin | 24 hodin |
| **Zvýšení odolnosti a dostupnosti infrastruktury** | Doba provozu systému | **Provozní doba v %** | 99% | 99,99% |
| **Penetrační test** | Počet vykonaných penetračních testů | **Počet** | 2 | 6 |

## 2.2.3. Byznys architektura

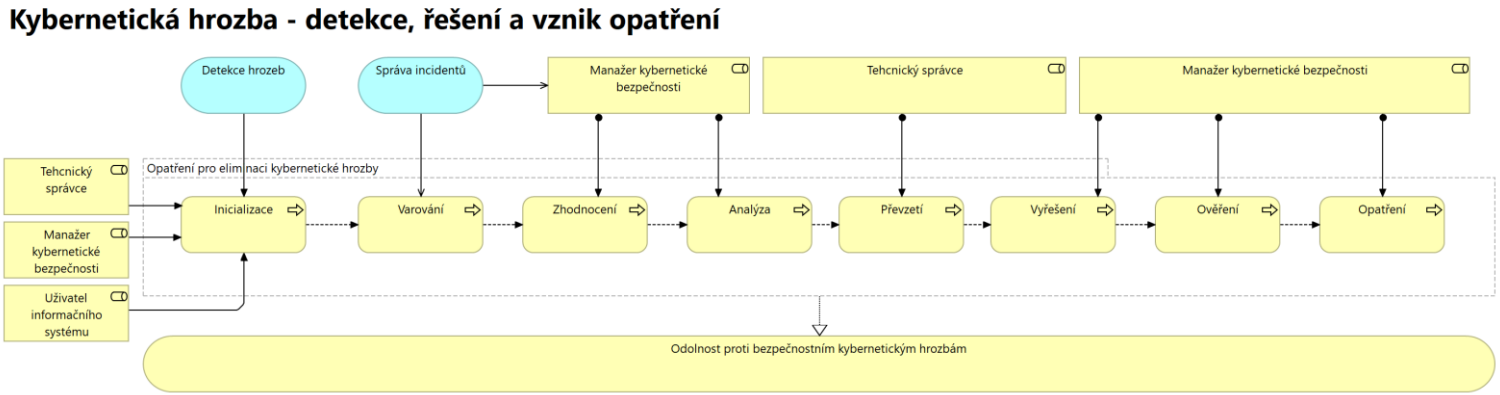
| Tabulka 17: Katalog prvků byznys architektury | | | |
|---|---|---|---|
| **ID** | **Typ prvku** | **Jméno prvku** | **Popis prvku** |
| **Prvky jsou uvedeny u odpovídajících modelů pro jejich lepší čitelnost.** | | | |

| Tabulka 18: **Využití front-office rozhraní předmětem projektu** | | | |
|---|---|---|---|
| **Rozhraní** | **Využití** | | **Popis využití rozhraní v projektu** |
| **Asistovaná přepážka** | | | |
| Umožnění asistovaného vyřízení podání či jiné služby v rámci projektu | Nerelevantní | | Projekt je zaměřen na kybernetickou bezpečnost |
| | **Č. žádosti o výjimku:** | | |
| Umožnění vyřízení služby na Kontaktním místě veřejné správy (Czech POINT) | Nerelevantní | | Neposkytuje služby, které by šlo využít na Czech POINT. |
| | **Č. žádosti o výjimku:** | | |
| **Webový portál** | | | |
| Identifikace úředních osob vstupujících do procesu je řešena v souladu s JIP/KAAS | Nerelevantní | | Taková identifikace není v projektu potřebná. |
| | **Č. žádosti o výjimku:** | | |
| Identifikace osob vstupujících do procesu je řešena v souladu se zákonem č. 250/2017 Sb., o elektronické identifikaci | Nerelevantní | | Projekt je zaměřen na kybernetickou bezpečnost |
| | **Č. žádosti o výjimku:** | | |
| | Nerelevantní | | Projekt je zaměřen na kybernetickou bezpečnost |

| Tabulka 18: **Využití front-office rozhraní předmětem projektu** | | | |
|---|---|---|---|
| **Rozhraní** | **Využití** | | **Popis využití rozhraní v projektu** |
| Portál poskytující služby klientům využívá design dle https://designsystem.gov.cz/ | **Č. žádosti o výjimku:** | | |
| **Datová zpráva (ISDS)** | | | |
| Využití Datových schránek pro účely doručování od OVM soukromoprávním subjektům a mezi OVM navzájem | Nerelevantní | | Projekt je zaměřen na kybernetickou bezpečnost |
| | **Č. žádosti o výjimku:** | | |
| Využití datových schránek pro účely dodávání mezi soukromoprávními subjekty navzájem | Nerelevantní | | Projekt je zaměřen na kybernetickou bezpečnost |
| | **Č. žádosti o výjimku:** | | |
| Využití Informačního systému datových schránek pro účely příjmu úkonů učiněných soukromoprávním subjektem vůči OVM (např. podání) | Nerelevantní | | Projekt je zaměřen na kybernetickou bezpečnost |
| | **Č. žádosti o výjimku:** | | |
| **Elektronicky podepsaný dokument do e-Podatelny** | **Nerelevantní** | | Projekt je zaměřen na kybernetickou bezpečnost |
| **Nepodepsaný dokument do e-Podatelny** | **Nerelevantní** | | Projekt je zaměřen na kybernetickou bezpečnost |
| **Listinnou cestou do podatelny** | **Nerelevantní** | | Projekt je zaměřen na kybernetickou bezpečnost |

| Tabulka 19: **Identifikace, autentizace a autorizace subjektů/uživatelů v jejich rolích** | | | |
|---|---|---|---|
| **Služba využívající identifikaci, autentizaci a autorizaci** | **Vysvětlete způsob identifikace a autentizace do služby** | **Použitý prostředek (Pokud není určený LoA v NIA) a druh autentizace** | **Vysvětlete autorizaci ve službě (přidělení role, mandáty, zastupování, atd.)** |
| Veškeré aplikační služby | Identitní systém města postavený na Active Directory a IDM | Jméno, heslo a čipová karta | Autorizace uživatele k jemu dostupným informačním systémům. |
| Privilegované účty | Transparentní přihlášení | Pro přístup k záznamům | Autorizace privilegovaného uživatele pro přístup k logům. |

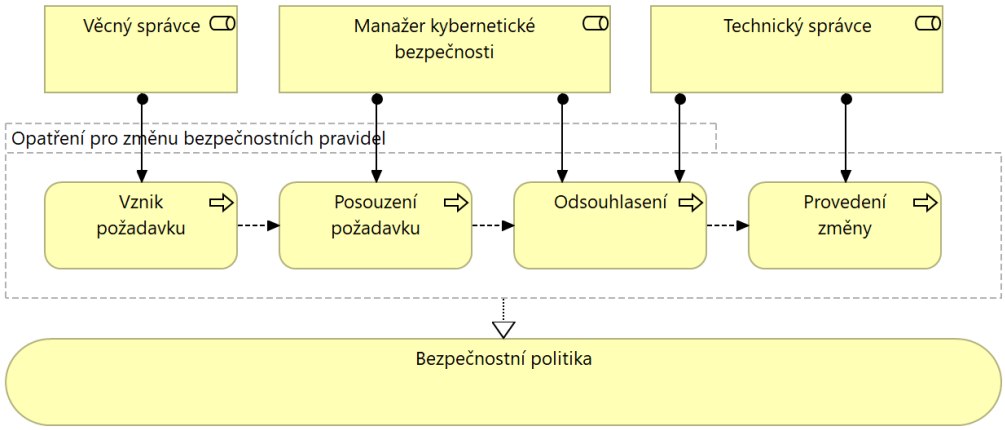
**Model byznys architektury (výkonu veřejné správy) – pohled činnostních funkcí**




| Prvek | Popis |
|---|---|
| **Byznys proces** | |
| Inicializace | Provedení inicializace detekce incidentu, který může být od automatické detekce, správce, manažera kybernetické bezpečnosti nebo uživatele. |

| | |
|---|---|
| Varování | Varování od aktivního reportingu sítě pro manažera kybernetické bezpečnosti. |
| Zhodnocení | Manažer kybernetické bezpečnosti zhodnotí varování. K získání dalších informací použije reporting. |
| Analýza | Manažer kybernetické bezpečnosti provede podrobnou analýzu varování, a pokud ji vyhodnotí jako hrozbu, přizve k součinnosti správce (administrátora) zařízení. V případě vážného nebo kritického incidentu informuje vedení úřadu. |
| Převzetí | Úsek informatiky převezme událost a provede opatření k jejímu vyřešení, případně eliminaci následků. |
| Vyřešení | Úsek informatiky předá vyřešený incident manažeru kybernetické bezpečnosti. |
| Ověření | Manažer kybernetické bezpečnosti ověří vyřešení incidentu, provede jeho evidenci a doplní nutné informace. |
| Opatření | Manažer kybernetické bezpečnosti navrhne opatření na eliminaci podobných hrozeb, případně navrhne změnu bezpečnostní politiky v organizaci. |
| **Byznys role** | |
| Manažer kybernetické bezpečnosti | Manažer kybernetické bezpečnosti spravuje bezpečnost ICT systému z pohledu kybernetické bezpečnosti. |
| Technický správce | Úsek ICT služeb – jeho pracovníci – správci systémů nebo infrastruktury. |
| Uživatel informačního systému | Uživatel informačního systému, který používá k výkonu své práce nebo agendy. Obecně jde o vnitřního uživatele, o jehož potřeby pečuje v oblasti ICT úsek ICT. |
| **Grouping** | |
| Opatření pro eliminaci kybernetické hrozby | Soubor procesů souvisejících s eliminací kybernetických hrozeb. |
| **Byznys služby** | |
| Odolnost proti bezpečnostním kybernetickým hrozbám | Zvýšení odolnosti proti kybernetickým bezpečnostním hrozbám, které mohou hrozit chráněných systémům. |
| **Aplikační služby** | |
| Detekce hrozeb | Detekce kybernetických hrozeb informačnímu systému. |
| Správa incidentů | Správa kybernetických incidentů. |

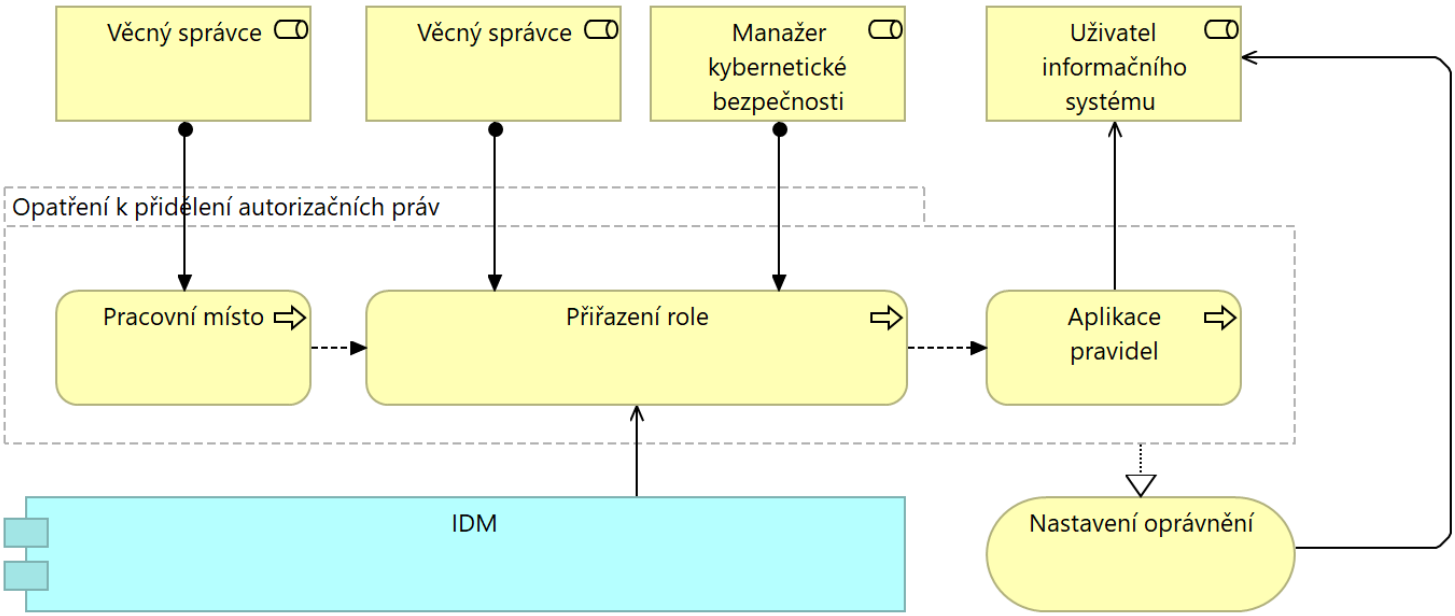
# Změna nebo vytvoření bezpečnostních pravidel




| Prvek | Popis |
|---|---|
| **Byznys proces** | |

| | |
|---|---|
| Vznik požadavku | Vznik požadavku na změnu bezpečnostních pravidel – např. nové zařízení, nové služby apod. Tuto změnu musí mít příslušný uživatel přímo schválenou nadřízeným, pak teprve může dojít k posouzení požadavku. V případě úseku informatiky jde požadavek přímo k posouzení. |
| Posouzení požadavku | Dojde k posouzení požadavku z obecného bezpečnostního hlediska, případně jsou posouzeny dopady na další systémy nebo pravidla. |
| Odsouhlasení | Odsouhlasení požadavku a jeho zařazení do bezpečnostní politiky resp. pravidel organizace. |
| Provedení změny | Vlastní realizace změny a její zavedení do praxe. |
| **Byznys role** | |
| Manažer kybernetické bezpečnosti | Manažer kybernetické bezpečnosti spravuje bezpečnost ICT systému z pohledu kybernetické bezpečnosti. |
| Technický správce | Úsek ICT služeb – jeho pracovníci – správci systémů nebo infrastruktury. |
| Věcný správce | Garant primárních aktiv, který je (interním) klientem útvaru IT, u kterého uplatňuje své odůvodněné požadavky na IT služby pro podporu výkonu svých agend VS |
| **Grouping** | |
| Opatření pro změnu bezpečnostních pravidel | Soubor procesů souvisejících se změnou bezpečnostních pravidel a směrnic. |
| **Byznys služby** | |
| Bezpečnostní politika | Bezpečnostní politika organizace tvořící zásady bezpečnosti v oblasti kybernetických incidentů pro jejich předcházení a eliminaci dopadů. |

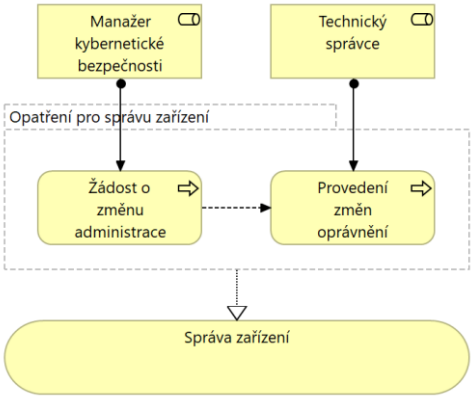
# Nástupy nebo změny v zařazení pracovníků/zařízení




| Prvek | Popis |
|---|---|
| **Byznys proces** | |
| Pracovní místo | Proces pracovní místo reprezentuje procesy spojené s vybavením nového zaměstnance prostředky ICT a jeho přístup do vnitřní sítě. Může se jednat také o nové zařízení. |
| Přiřazení role | Proces zařazení nového pracovníka nebo zařízení do sítě organizace. Např. klientská stanice nebo referent. |
| Aplikace pravidel | Aplikace pravidel podle přidělené role. Z těchto pravidel vyplývají oprávnění na služby nebo přístup k datům AIS. Aplikací pravidel se také rozumí jejich odebrání při odchodu pracovníka. |
| **Byznys role** | |
| Manažer kybernetické bezpečnosti | Manažer kybernetické bezpečnosti spravuje bezpečnost ICT systému z pohledu kybernetické bezpečnosti. |
| Personální oddělení | Personální oddělení organizace mající za úkol péči o lidské zdroje. |

| | |
|---|---|
| Věcný správce | Garant primárních aktiv, který je (interním) klientem útvaru IT, u kterého uplatňuje své odůvodněné požadavky na IT služby pro podporu výkonu svých agend VS |
| Uživatel informačního systému | Uživatel informačního systému z pohledu kybernetické bezpečnosti správce aktiva. |
| **Grouping** | |
| Opatření k přidělení autorizačních práv | Soubor procesů souvisejících s příchodem, odchodem nebo změnou zařazení pracovníka. |
| **Byznys služby** | |
| Nastavení oprávnění | Přidělení práv pro příslušnou roli. Práva může získat prostřednictvím zařízení, které je jí přiděleno nebo prostřednictvím své role (funkce). Případně také jejich odebrání. |
| **Aplikační komponenta** | |
| IDM | IDM je základní autoritou pro ověřování oprávnění. |

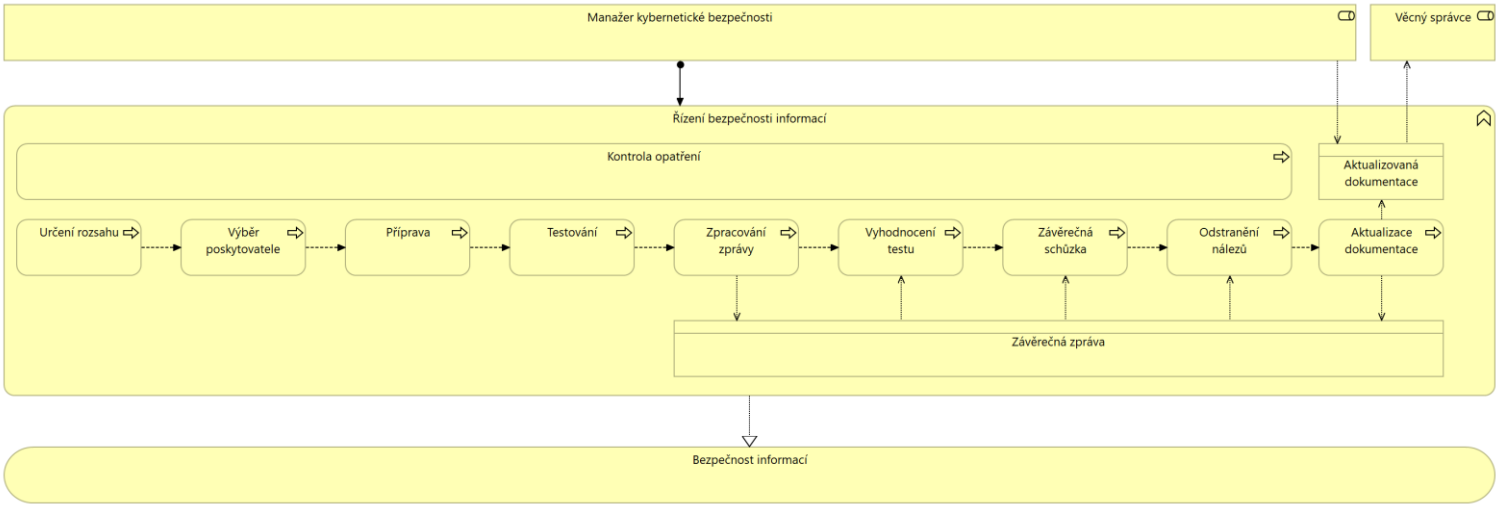
## Správa zařízení




| Prvek | Popis |
|---|---|
| **Byznys proces** | |
| Žádost o změnu správy zařízení | Žádost o změnu administrace zařízení s ohledem na potřeby organizace, případně rozvoj personálních kompetencí. |
| Provedení změn oprávnění | Provedení změn oprávnění u zařízení nebo prostředku. |
| **Byznys role** | |
| Manažer kybernetické bezpečnosti | Manažer kybernetické bezpečnosti spravuje bezpečnost ICT systému z pohledu kybernetické bezpečnosti. |
| Technický správce | Úsek ICT služeb – jeho pracovníci – správci systémů nebo infrastruktury. |
| **Grouping** | |
| Opatření pro správu zařízení | Soubor procesů souvisejících se správou zařízení a jeho zabezpečením v síti. |
| **Byznys služby** | |
| Správa zařízení | Služba zaručuje, že za každé zařízení v síti někdo nese zodpovědnost a má na starosti jeho správu. |

### Ověření technických opatření

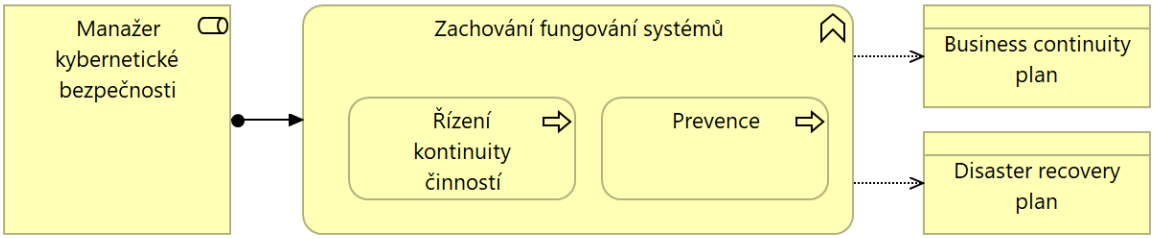
## Penetrační testování




| Proces | Popis |
|---|---|
| **Byznys role** | |
| Věcný správce | Garant primárních aktiv, který je (interním) klientem útvaru IT, u kterého uplatňuje své odůvodněné požadavky na IT služby pro podporu výkonu svých agend VS |
| Manažer kybernetické bezpečnosti | Manažer kybernetické bezpečnosti spravuje bezpečnost ICT systému z pohledu kybernetické bezpečnosti. |
| **Byznys služba** | |
| Bezpečnost informací | Bezpečnost informací uchovávaných v prostředcích města. |
| **Byznys funkce** | |
| Řízení bezpečnosti informací | Tento systém je tvořen zavedením a udržováním jednotlivých opatření kybernetické bezpečnosti. |
| **Byznys proces** | |
| Určení rozsahu | Specifikuje jaké systémy, IP adresy (odkazující například na aplikace, webové servery, databáze nebo operační systémy) a další případná aktiva organizace budou podrobena penetračnímu testování. |
| Výběr poskytovatele | Provedení výběru poskytovatele. S ohledem na složitost problematiky budou vybírání certifikovaní poskytovatelé nebo testeři. |
| Příprava | Příprava prostředí počínaje zálohou přes vytvoření příslušných účtů a konče informováním příslušných osob. Tato fáze zajišťuje, že se testování nedotkne běžného provozu nebo nedojde k nechtěné ztrátě dat. |
| Testování | Testování lze rozdělit na několik dílčích fází:<br>• Plánování a průzkum – tato fáze se skládá z pasivního a aktivního získávání informací o objednateli. Výstupem jsou rozsahy IP adres a informace o zaměstnancích (např. telefonní čísla, e-mailové adresy).<br>• Skenování – jedná se o proces testování cílené stanice se záměrem získání užitečných informací, které by mohly být využity v pozdějších fázích testování.<br>• Enumerace – je proces extrahování informací z cíleného systému z důvodu získání bližšího určení specifikací systému. Výstupem této fáze mohou být uživatelé a skupiny, sdílené složky, jména strojů atd.<br>• Zisk přístupu – jedná se o komplexní fázi, která se dělí do více kroků jako lámání hesel ke kompromitaci účtu, eskalování privilegií z běžného uživatele na administrátora apod. |
| Zpracování zprávy | Proces zpracování zprávy na straně poskytovatele služby. Výstupem je Závěrečná zpráva. |
| Vyhodnocení testu | Cílem této fáze je jednotlivé nálezy posoudit v kontextu samotné organizace, určit priority k nápravě a zadat jednotlivé úkoly. Probíhá formou diskusí s testery, případnými dalšími odborníky. |
| Závěrečná schůzka | V rámci diskuze dojde k vyjasnění nálezů a doporučení, jak se s těmito nálezy vypořádat. Cílem závěrečné schůzky je lepší vysvětlení nálezů, zlepšení vzájemného vztahu a poskytnutí zpětné vazby všem účastníkům. |
| Odstranění nálezů | Na základě výsledku testu je potřeba stanovit úkoly vedoucí k nápravě nevyhovujícího stavu včetně termínu jejich provedení. Po jejich splnění je často realizován retest nálezů. Retest nálezů zkoumá, zda byly zjištěné nedostatky napraveny. Nejedná se o opakování penetračního testu. |

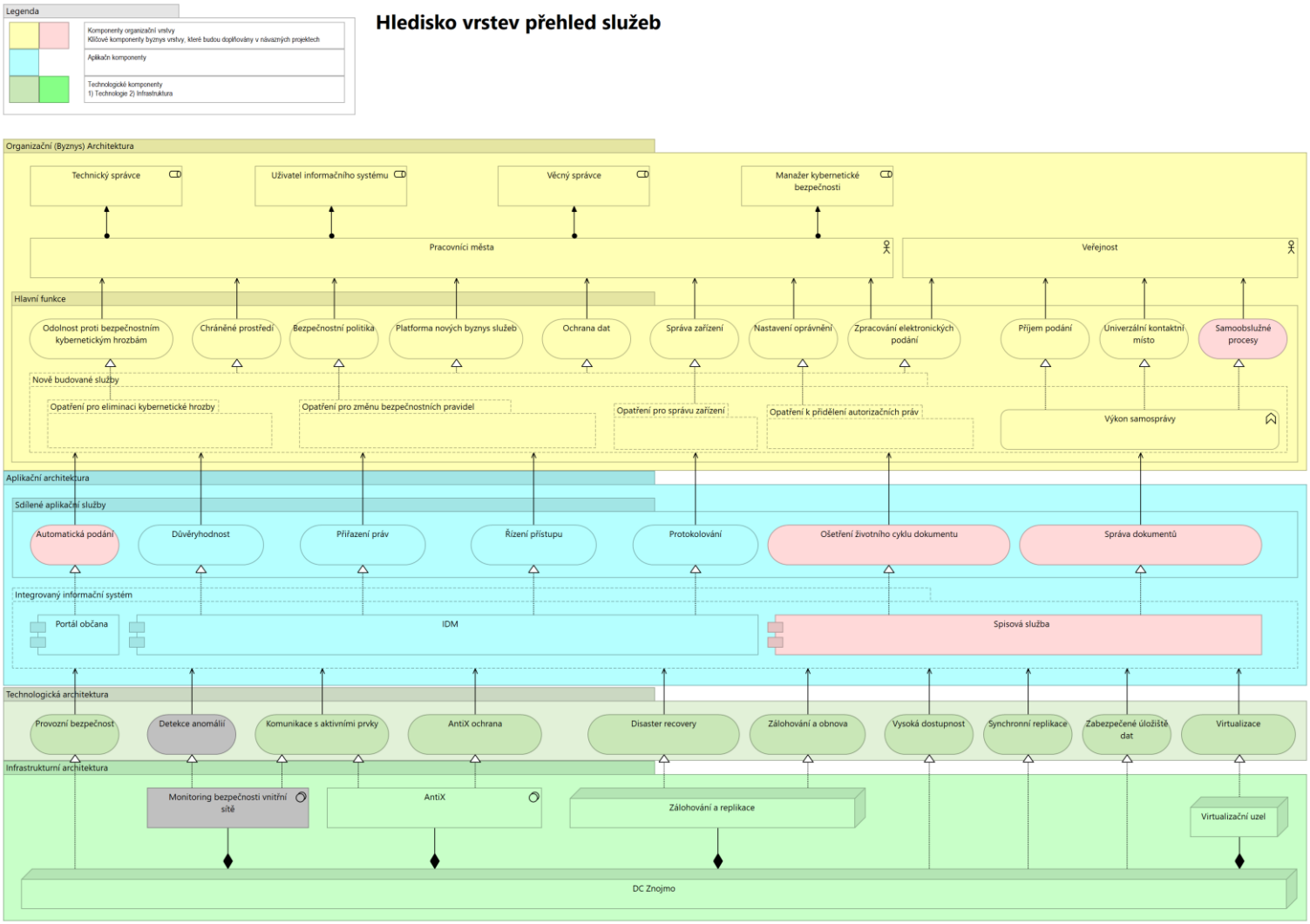
| | |
|---|---|
| Kontrola opatření | Kontrola opatření nastavených v organizaci a jejich dodržování včetně technických prostředků k jejich kontrole. |
| Aktualizace dokumentace | Aktualizace dokumentace o výsledky prověřování, či jiné zdroje např. informace z jiných úřadů, znalostní báze apod. |
| **Byznys objekt** | |
| Závěrečná zpráva | Jedná se o dokument, který je poskytnut objednateli jako důkaz o tom, co bylo vykonáno. Závěrečná zpráva zpravidla obsahuje:<br>• manažerské shrnutí,<br>• harmonogram testu,<br>• přesné zadání testu,<br>• omezení testu,<br>• použitou metodologii,<br>• nalezené problémy,<br>• detailní popis zranitelností,<br>• doporučení k odstranění nálezů,<br>• přehledové tabulky (tabulka nálezů, tabulka systémů apod.). |
| Aktualizovaná dokumentace | Aktualizace dokumentace o výsledky prověřování, či jiné zdroje např. informace z jiných úřadů, znalostní báze apod. |

# Řízení kontinuity činností




| Proces | Popis |
|---|---|
| **Byznys role** | |
| Manažer kybernetické bezpečnosti | Manažer kybernetické bezpečnosti spravuje bezpečnost ICT systému z pohledu kybernetické bezpečnosti. |
| **Byznys funkce** | |
| Zachování fungování systémů | Zajišťuje zachování / obnovu fungování systémů i po haváriích a tak zajišťuje podporu výkonu samosprávy a zejména její kontinuity. |
| **Byznys proces** | |
| Řízení kontinuity činností | Cílem procesu je zajištění obnovy funkčnosti organizace v případě výskytu mimořádné události. |
| Prevence | Soubor činností (procesů) pro předcházení havarijním stavům a příprava na případné mimořádné události. |
| **Byznys objekt** | |
| Business continuity plan | Plán obnovy. |
| Disaster recovery plan | Havarijní plán. |

**Model byznys architektury (výkonu veřejné správy) – pohled služeb veřejné správy**




| Prvek | Popis |
|---|---|
| **Grouping (seskupení)** | |
| Opatření pro eliminaci kybernetické hrozby | Soubor procesů souvisejících s eliminací kybernetických hrozeb. |
| Opatření pro změnu bezpečnostních pravidel | Soubor procesů souvisejících se změnou bezpečnostních pravidel a směrnic. |
| Opatření pro správu zařízení | Soubor procesů souvisejících se správou zařízení a jeho zabezpečením v síti. |
| Opatření k přidělení autorizačních práv | Soubor procesů souvisejících s příchodem, odchodem nebo změnou zařazení pracovníka. |
| Nově budované služby | Soubor nově budovaných byznys služeb vyplývajících z prostředí. Součástí jsou také nové služby, které budou postupně přidávány. |
| **Aktéři** | |
| Pracovníci města | Pracovníci organizací města jako celku včetně MěÚ. |
| Veřejnost | Obecně kdokoliv, kdo má právo nebo možnost znát informace uveřejněné na portálech nebo používat jejich služby. |
| **Role** | |
| Technický správce | Úsek ICT služeb – jeho pracovníci – správci systémů nebo infrastruktury. |
| Manažer kybernetické bezpečnosti | Manažer kybernetické bezpečnosti spravuje bezpečnost ICT systému z pohledu kybernetické bezpečnosti. |
| Věcný správce | Garant primárních aktiv, který je (interním) klientem útvaru IT, u kterého uplatňuje své odůvodněné požadavky na IT služby pro podporu výkonu svých agend VS |
| Uživatel informačního systému | Uživatel informačního systému, který používá k výkonu své práce nebo agendy. Obecně jde o vnitřního uživatele, o jehož potřeby pečuje v oblasti ICT úsek ICT. |

| | |
|---|---|
| **Byznys služby** | |
| Odolnost proti bezpečnostním kybernetickým hrozbám | Zvýšení odolnosti proti kybernetickým bezpečnostním hrozbám, které mohou hrozit chráněných systémům. |
| Bezpečnostní politika | Souhrn opatření k definici bezpečnostní politiky za účelem zajištění pravidel udržující bezpečnost prostředí. |
| Nastavení oprávnění | Nastavení oprávnění pro příslušnou roli. Oprávnění uživatel může získat prostřednictvím zařízení, které je jí přiděleno nebo prostřednictvím své role (funkce). |
| Správa zařízení | Služba zaručuje, že za každé zařízení v síti někdo nese zodpovědnost a má na starosti jeho správu. |
| Zpracování elektronických podání | Zpracování elektronických podání pomocí spisových služeb. |
| Ochrana dat | Ochrana poskytnutých dat před zničením nebo zcizením. |
| Chráněné prostředí | Ochrana prostředí pro výkon digitalizovaných služeb města. |
| Platforma nových byznys služeb | Platforma nových byznys služeb pro organizace města, které je mohou v budoucnu přidávat. |
| Univerzální kontaktní místo | Univerzální kontaktní místo je služba portálu občana umožňující udělat podání z jednoho místa pro všechny služby. |
| Příjem podání | Základní služba úřadu na přepážce dochází k příjmu podání. Pokud je uskutečněno přes ISDS nebo elektronickou podatelnou, dochází k jeho ručnímu zpracování. Rozšíření služeb spočívá v elektronizaci a automatizaci příjmu a vyřízení podání. |
| Samoobslužné procesy | Samoobslužné procesy veřejné správy v samosprávě, které jsou nabízeny v rámci portálu občana (místní poplatky apod.) |
| **Byznys funkce** | |
| Výkon samosprávy | Výkon samosprávy podle zákonů. Mění se pouze forma způsobu poskytování služeb samosprávy. |
| **Aplikační služby** | |
| Automatická podání | Automatická podání veřejné správy v samosprávě, která jsou nabízena v rámci portálu občana (místní poplatky apod.) |
| Důvěryhodnost | Důvěryhodnost prostředí a autenticity přistupujících osob. |
| Přiřazení práv | Přiřazení práv přistupujícím osobám. |
| Řízení přístupu | Služby pro autorizaci a identifikaci komponenty IDM. Obsahuje také přístupovou bránu pro externí uživatele. |
| Protokolování | Protokolování skutečností souvisejících s aktivitou v rámci IDM. |
| Ošetření životního cyklu dokumentu | Ošetření životního cyklu dokumentu v elektronické podobě od vstupu nebo výstupu přes archivaci až ke skartaci. |
| Správa dokumentů | Správa dokumentů a jejich řízení s ohledem na přístup. |
| **Aplikační komponenty** | |
| Portál občana | Prostředek pro vzdálený přístup občana ke službám nebo agendám a jejich obsluha. |
| IDM | Řídicí systém pro správu identit a s nimi spojených prostředků. |
| Spisová služba | Systém pro řízení oběhu dokumentů a přístupu k informacím v nich obsažených podle závazných normativů. Reprezentuje spisové služby v rámci celé veřejnoprávní korporace. Klíčová komponenta pro oběh dokumentů a spisů zajišťující obsluhu dle zákona č. 167/2012 Sb., kterým se mění zákon č. 499/2004 Sb., o archivnictví a spisové službě. |
| **Technologické nody** | |
| Zálohování a replikace | Infrastrukturní celek poskytující služby zálohování, ochrany dat před neoprávněnou činností a obnovy. |
| Virtualizační uzel | Virtualizační uzel obsahuje veškeré komponenty nutné k běhu virtualizovaných aplikací nebo infrastruktury. |
| DC Znojmo | Technologické centrum, resp. datové centrum. Infrastrukturní celek poskytující základní služby pro fungování aplikací. |
| **Technologické služby** | |
| Provozní bezpečnost | Služba provozní bezpečnosti monitoruje jednotlivá zařízení z pohledu jejich funkcí a chodu. Dává včasnou výstrahu o technických problémech a diagnostiku zařízení v síti. |
| Detekce anomálií | Detekce hrozeb, anomálií, porušení bezpečnostních pravidel v rámci kybernetické bezpečnosti. |
| Komunikace s aktivními prvky | Komunikace s aktivními prvky pro blokování nežádoucí aktivity. |
| AntiX ochrana | Služba infrastruktury chránící infrastrukturu před kybernetickými hrozbami. |
| Disaster recovery | Služba okamžitého produkčního spuštění virtuálních serverů současně, přímo ze záložní storage (z úložiště dat) a s možností následné online migrace na cílovou produkční storage jako součást DR plánu. |
| Zálohování a obnova | Zálohování a obnova dat. Základní služba infrastruktury s ohledem na bezpečnost. |
| Vysoká dostupnost | Vysoká dostupnost infrastruktury. |

| | |
|---|---|
| Synchronní replikace | Zajištění bezvýpadkového provozu synchronní replikací v režimu active–active, tzn. že data budou poskytována současně z obou uložišť. |
| Zabezpečené úložiště dat | Ukládání záloh a logů pro jejich ochranu. |
| Virtualizace | Virtualizace infrastruktury. |
| **Infrastrukturní software** | |
| Monitoring bezpečnosti vnitřní sítě | Monitoring bezpečnosti vnitřní sítě s odpovídajícími funkcemi a službami. |
| AntiX | Vlastní software provádějící ochranu před útoky nebo malware. |

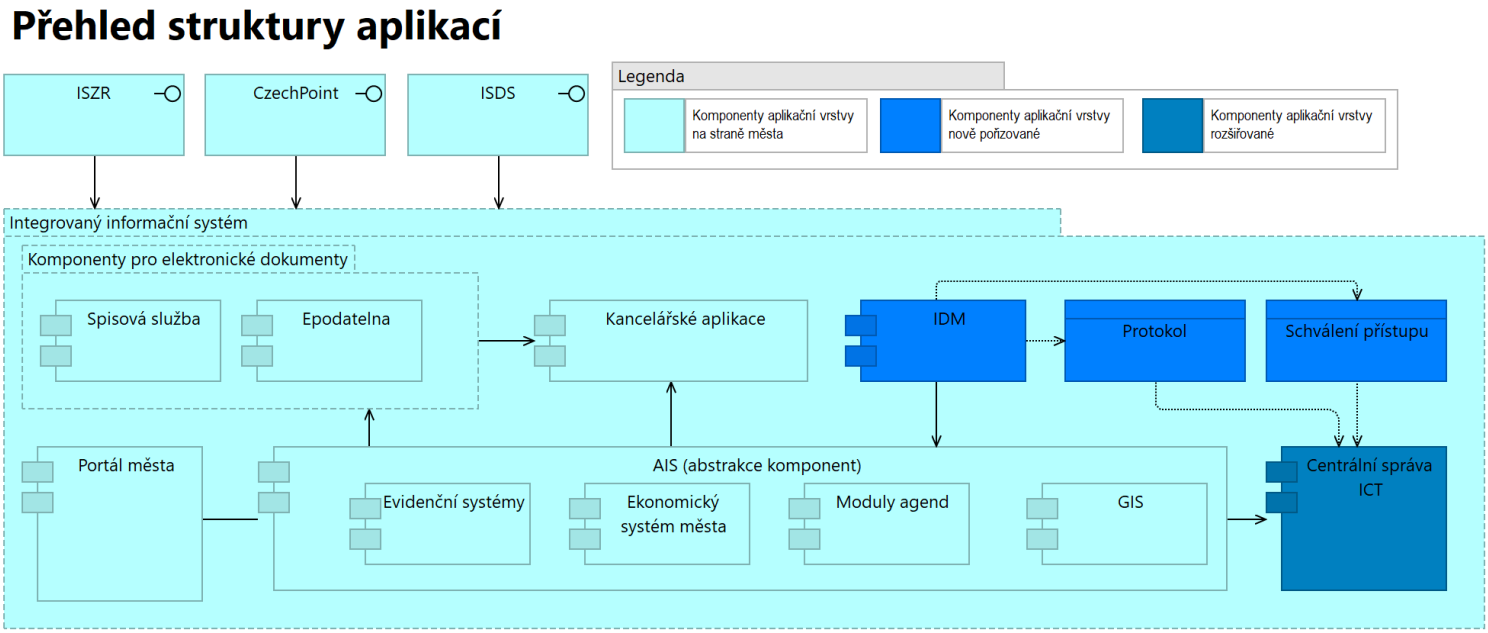
| Tabulka 20: **Vysvětlení kontextu byznys architektury úřadu** |
|---|
| **a) jaké k projektu existují či vznikají duplicity a proč?** |
| Ne. |
| **b) jsou využity všechny sdílené služby?** |
| X |
| **Vysvětlení byznys architektury projektu:** |
| Byznys architektura obsahuje především procesy spojené s kybernetickými hrozbami, ale i novými službami.<br>Primárním cílem je zvýšení kybernetické bezpečnosti organizace a snížení dopadů kybernetických rizik. Nejdůležitější je v tomto ohledu manažer kybernetické bezpečnosti a vedení úřadu (tajemník). Tyto role bude mít odpovědnost za řízení a rozvoj kybernetické bezpečnosti v organizaci. Manažer kybernetické bezpečnosti je zodpovědný za nastavení systému řízení bezpečnosti informací, především za určení aktiv a jejich zranitelnosti, nastavení bezpečnostních opatření, řízení rizik a jejich kontrolu. Nastavení bezpečnostních opatření v organizaci je nutné pravidelně vyhodnocovat. Pravidelné vyhodnocování bude zajištěno prostřednictvím auditování kybernetické bezpečnosti nezávisle prováděnými penetračními testy, které budou sloužit jako audit bezpečnosti.<br>Manažer kybernetické bezpečnosti má podle povahy incidentu povinnost – drobnější incidenty vyřešit, incidenty střední závažnosti hlásit vedení úřadu (tajemník, který rozhodne o uvolnění prostředků na pomoc s řešením incidentu), dále podle povahy incidentu na servis desk poskytovale služby bezpečnostního dohledu s požadavkem na pomoc při řešení. V případě incidentu souvisejícího s KIVS a CMS má povinnost oznámit incident na Servis Desk CMS. V případě masivního útoku a kritických incidentů je povinen tyto události hlásit na CERT NUKIB.<br>Ve všech případech je manažer kybernetické bezpečnosti povinnen zhodnotit účinnost dosavadních bezpečnostních politik a opatření. Podle výsledku hodnocení provést změny v bezpečnostní politice, případně navrhnout další řešení.<br>Incidenty jsou vždy řešeny ve spolupráci se správou ICT. |

## 2.2.4. Architektura informačních systémů (aplikací a dat)

### *2.2.4.1. Architektura informačních systémů – část: Aplikační architektura*

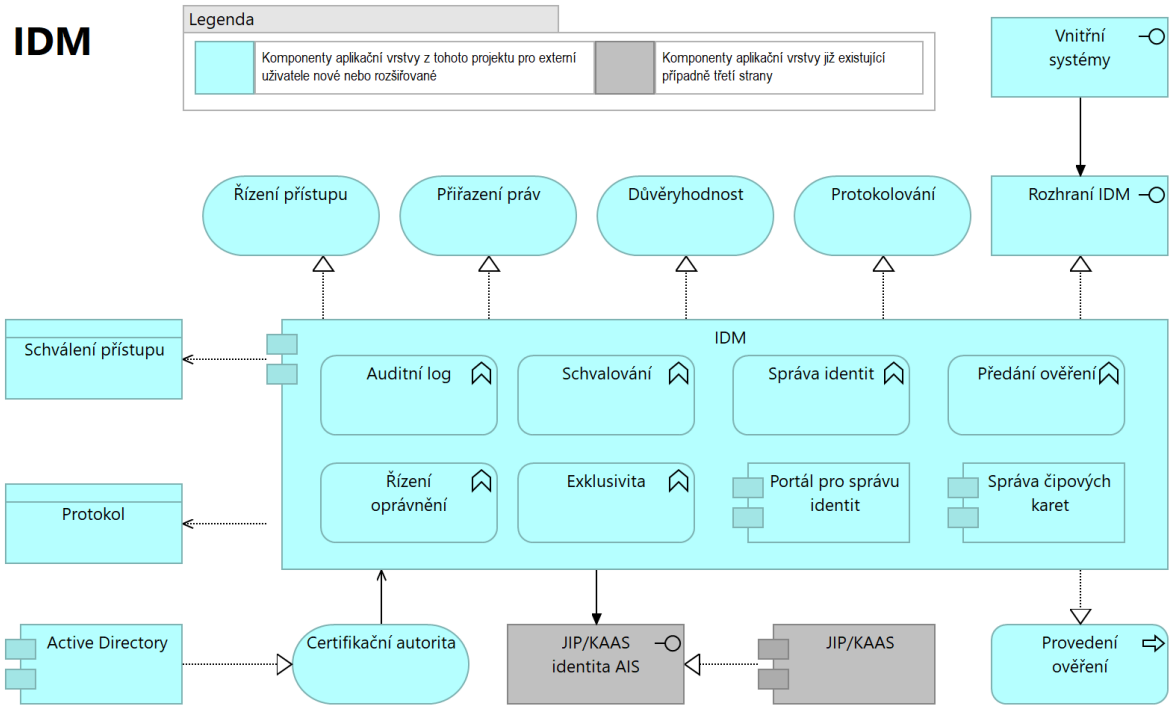
| **Tabulka 21: Katalog všech aplikačních komponent řešení a klíčových aplikačních funkcí** | | | |
|---|---|---|---|
| **ID** | **Typ prvku** | **Jméno prvku** | **Popis prvku** |
| **Prvky jsou uvedeny u odpovídajících modelů pro jejich lepší čitelnost.** | | | |

**Diagram aplikační architektury – pohled struktury aplikací**




| Prvek | Popis |
|---|---|
| **Grouping** | |
| Integrovaný informační systém | Komplexní informační systém města včetně jeho organizací. |
| Komponenty pro elektronické dokumenty | Komponenty zajišťující zpracování elektronických dokumentů. |
| **Komponenty** | |
| AIS (abstrakce komponent) | Agendový informační systém jako zjednodušená komponenta pro vyjádření všech funkcí, kterými disponuje s ohledem na vykonávané agendy. |
| Epodatelna | Aplikace je určena pouze pro uživatele disponující uznávaným elektronickým podpisem, který je založen na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb pro elektronické podání. |
| Evidenční systémy | Různé evidenční systémy města. |
| Ekonomický systém města | Komplexní řešení ekonomiky města (ERP systém). |
| GIS | Geografický informační systém města pro tvorbu mapových vrstev a podkladů. |
| Kancelářské aplikace | Aplikace pro zpracování textů, tabulek a prezentací. |
| Moduly agend | Moduly pro zpracování agend. |
| Portál města | Portál ke zveřejňování informací. |
| Spisová služba | Klíčová komponenta pro oběh dokumentů a spisů zajišťující obsluhu dle zákona č. 167/2012 Sb., kterým se mění zákon č. 499/2004 Sb., o archivnictví a spisové službě. |
| Centrální správa ICT | Komponenta zajišťující správu informačního systému z pohledu jeho chodu jako nástroj pro správu provozních parametrů včetně sběru požadavků (konfigurace, profylaxe apod., ale také helpdesk). |
| IDM | Řídicí systém pro správu identit a s nimi spojených prostředků. |
| **Rozhraní** | |
| CzechPoint | Využití CzechPOINTu, konkrétně CzechPOINT@Office dle vzoru sdílených služeb, aby tudy mohli přistupovat uživatelé bez vlastního AIS a tedy komunikující systémem asistované správy CZP. |
| ISDS | Přístup do systému datových schránek prostřednictvím ESSL. |
| ISZR | Přístup do systému základních registrů. Vyžadující konektor obecného agendového informačního systému na ISZR, který je napojen podle zákona 365/2000 v rámci CMS. |
| **Datové objekty** | |
| Protokol | Protokol aktivit IDM. |
| Schválení přístupu | Záznam schválení přístupových práv. |

**Diagram aplikační architektury – pohled komunikace aplikací**




| Prvek | Popis |
|---|---|
| **Aplikační komponenta** | |
| IDM | Řídicí systém pro správu identit a s nimi spojených prostředků. |
| Active directory | Active directory je základní autoritou pro ověřování oprávnění. |
| JIP/KAAS | Komponenta jednotného identitního prostoru / katalogu autentizačních a autorizačních služeb. |
| Portál pro správu identit | Portál pro správu identit pro externí organizace a jejich správce. |
| Správa čipových karet | Manuální správa dat čipové karty, změna a odblokování bezpečnostních kódů čipové karty uživatelem. |
| **Aplikační služby** | |
| Certifikační autorita | Profily certifikátů fungují se službou Active Directory Certificate Services a s rolí NDES (Network Device Enrollment Service). Poskytuje uživatelům potřebné certifikáty také pro připojení k síti VPN a bezdrátovým připojením. |
| Přiřazení práv | Přiřazení práv přistupujícím osobám. |
| Důvěryhodnost | Důvěryhodnost prostředí a autenticity přistupujících osob. |
| Protokolování | Protokolování skutečností souvisejících s aktivitou v rámci IDM. |
| Řízení přístupu | Služby pro autorizaci a identifikaci komponenty IDM. Obsahuje také přístupovou bránu pro externí uživatele. |
| **Aplikační proces** | |
| Provedení ověření | Provedení sekvence kroků vedoucích k ověření uživatele. Je spuštěno při požadavku na ověření a zajišťuje sjednocení informací. |
| **Aplikační funkce** | |
| Předání ověření | Předání ověření dalším aplikacím. |
| Řízení oprávnění | Řízení oprávnění Role-Based Access Control (RBAC), které využívá opakovaně přidělitelné objekty – role. Uživatel mající roli pak získá oprávnění nepřímo přes tuto přidělenou roli. Role samotná pak bude obsahovat další atributy, kromě názvu například i schvalovatele či vlastníka role a popis. |

| | |
|---|---|
| Exklusivita | Segregation of Duties (SoD) Např. uživatel nemůže mít roli, která jej opravňuje k vydávání faktur společně s rolí, která faktury kontroluje. |
| Schvalování | Schvalování přístupů a práv. |
| Správa identit | Správa identit a správu rolí jak pracovníků úřadu, tak externistů/fyzických a právnických osob. Zahrnuje v sobě také:<br>Identifikace – jednoznačné rozlišení osoby.<br>Autentizace – ověření identity osoby pro přihlášení k systému a jeho službám.<br>Autorizace – udělení práva osoby použít funkci/službu systému. |
| Auditní log | Systém zaznamená všechny vykonané akce do auditního záznamu, ze kterého bude jasné, kdo komu přidělil oprávnění, kdy se to stalo, kdo o to požádal, kdo požadavek schválil apod. |
| **Rozhraní** | |
| Zařízení pro ověření | Rozhraní zařízení vlastněné uživatelem, které dodá další faktor po ověření (push zpráva, SMS, karta apod.) |
| Vnitřní systémy | Rozhraní vnitřních systémů (AIS) požadující ověření přistupujících. |
| Rozhraní IDM | Obecné rozhraní IDM, do kterého budou doplňovány konektory. |
| JIP/KAAS identita AIS | Poskytující konektor jednotného identitního prostoru / katalogu autentizačních a autorizačních služeb pro agendový informační systém. |
| **Datový objekt** | |
| Schválení přístupu | Záznam schválení přístupových práv. |
| Protokol | Protokol aktivit IDM. |

| Tabulka 22: **Vysvětlení v kontextu aplikační architektury úřadu** |
|---|
| **a) jaké k projektu existují či vznikají duplicity?** |
| Ne |
| **b) proč a jsou využity všechny sdílené služby?** |
| Ano, protože je to účelné, hospodárné a v souladu se strategickými dokumenty města. |
| **Vysvětlení aplikační architektury projektu:** |
| Dodané aplikační komponenty chrání zejména vnitřní informační systém, ale i systémy poskytující služby občanům, jako je portál občana. |

### *2.2.4.2. Architektura informačních systémů – část: Datová architektura*

Tabulka 23: **Katalog objektů a subjektů:**

| **Objekt nebo subjekt, který je předmětem evidence** | **Vysvětlení objektu nebo subjektu** | **Označení objektu nebo subjektu dle Agend VS** | **Je objekt čerpán nebo poskytován jiným subjektům?** |
|---|---|---|---|
| Protokol | Protokol aktivit IDM. | *Nejedná se o agendový údaj* | Není poskytován ani čerpán |
| Schválení přístupu | Záznam schválení přístupových práv. | *Nejedná se o agendový údaj* | Není poskytován ani čerpán |

| **Tabulka 24: Využití datového fondu základních registrů a dalších agend** | | | |
|---|---|---|---|
| **Název** | **Použito** | | **Vysvětlení** |
| **Základní registry** | | | |
| **Způsob vedení datového kmene** | Nerelevantní | | Projekt se týká kybernetické bezpečnosti. Neřeší datový fond. Vedení datového kmene je v tomto případě nerelevantní. |
| **Čtení údajů ROB** | Nerelevantní | | |
| | **Č. žádosti o výjimku:** | | |

| Tabulka 24: Využití datového fondu základních registrů a dalších agend | | | |
|---|---|---|---|
| **Název** | **Použito** | | **Vysvětlení** |
| **Editace údajů ROB** | Nerelevantní | | <popište včetně zákonného zmocnění> |
| | **Č. žádosti o výjimku:** | | |
| **Čtení údajů ROS** | Nerelevantní | | <popište včetně zákonného zmocnění> |
| | **Č. žádosti o výjimku:** | | |
| **Editace údajů ROS** | Nerelevantní | | <popište včetně zákonného zmocnění> |
| | **Č. žádosti o výjimku:** | | |
| **Čtení údajů RÚIAN** | Nerelevantní | | |
| | **Č. žádosti o výjimku:** | | |
| **Editace údajů RÚIAN** | Nerelevantní | | < popište včetně zákonného zmocnění > |
| | **Č. žádosti o výjimku:** | | |
| **Čtení údajů RPP** | Nerelevantní | | < popište včetně zákonného zmocnění > |
| | **Č. žádosti o výjimku:** | | |
| **Editace údajů RPP** | Nerelevantní | | < popište včetně zákonného zmocnění > |
| | **Č. žádosti o výjimku:** | | |
| **Evidujeme subjekty nebo objekty, které nejsou v základních registrech** | Ne | | < popište, o jaké subjekty se jedná a proč ><br>*<příklad: agenda eviduje cizince bez pobytového statutu v ČR z důvodu zákonné potřeby je evidovat viz §1 zákon č. 100/1990>* |
| **Využití údajů publikovaných prostřednictvím kompozitních služeb editorů Základních registrů** | | | |
| **Evidence obyvatel (ISEO)** | *Nerelevantní* | | < popište včetně zákonného zmocnění > |
| | **Č. žádosti o výjimku:** | | |
| **Cizinecký informační systém (CIS)** | *Nerelevantní* | | < popište včetně zákonného zmocnění > |
| | **Č. žádosti o výjimku:** | | |
| **Evidence občanských průkazů (AISEOP)** | Nerelevantní | | < popište včetně zákonného zmocnění > |
| | **Č. žádosti o výjimku:** | | |
| **Evidence cestovních dokladů (AISECD)** | Nerelevantní | | < popište včetně zákonného zmocnění > |
| | **Č. žádosti o výjimku:** | | |
| **Informační systém sdílené služby (ISSS dříve jako eGSB)** | | | |
| **Čerpání dat přes ISSS** | Nerelevantní | | < popište včetně zákonného zmocnění s odkazem na kontexty https://archi.gov.cz/nap:kontext, pokud neexistuje kontext, jaké objekty či subjekty z tabulky 23 by se požadovaly po jiných agendách> |
| | **Č. žádosti o výjimku:** | | |
| **Publikování vlastních dat přes ISSS** | Nerelevantní | | < popište včetně zákonného zmocnění, a jakých objektů či subjektů z tabulky 23 se bude týkat> |
| | **Č. žádosti o výjimku:** | | |
| **Komunikace mimo propojený datový fond** | | | |

| Tabulka 24: Využití datového fondu základních registrů a dalších agend | | |
|---|---|---|
| **Název** | **Použito** | **Vysvětlení** |
| **Využívání vlastních proprietárních rozhraní** | Nerelevantní<br>**Č. žádosti o výjimku:** | < popište jakých objektů či subjektů z tabulky 23 se bude týkat> |
| **Využívání Czech POINT pro přístup nebo editaci údajů PPDF** | Ne | < popište, zda a jak využíváte pro přístup k údajům objektů či subjektů práva Czech POINT nebo zda jej využíváte pro editaci údajů do jiných ISVS> |

| Tabulka 25: Způsob zajištění vedení datového kmene | | |
|---|---|---|
| **Požadavek** | **Použito** | **Vysvětlení** |
| **Zajištění přístupu k datům pro správce předmětu projektu** | | |
| **Budete mít zajištěn přístup k veškerým datům vedeným v databázích dotčených předmětem projektu ve strojově čitelném a otevřeném formátu?** | Nerelevantní<br>**Č. žádosti o výjimku:** | Projekt jako takový neřeší přístup datům v informačních systémech města. Přístup k datům z komponent, které se podílejí na zajišťování kybernetické bezpečnosti, je však zajištěn, a to za účelem detekce hrozeb. |
| **Budete mít výše popsaný přístup k datům zajištěn bez dodatečných finančních nákladů?** | Nerelevantní<br>**Č. žádosti o výjimku:** | Data jsou vždy vlastnictvím města. |
| **Budete moci se zpřístupněnými daty libovolně nakládat?** | Nerelevantní<br>**Č. žádosti o výjimku:** | |
| **Publikace výstupů ve formátu otevřených dat** | | |
| **Budou data vedená v databázích dotčených předmětem projektu zveřejňována jako otevřená data?** | Ano<br>**Č. žádosti o výjimku:** | Budou publikovány počty zachycených kybernetických incidentů. |
| **Jaké datové oblasti plánujete zveřejňovat jako otevřená data, kdy a na jakém stupni otevřenosti?** | | Jednou měsíčně bude dodán přehled na stupni otevřenosti 3 (předpokládaný standard CSV, nebo XML). |

| Tabulka 26: **Nakládání s osobními a citlivými údaji** | | | |
|---|---|---|---|
| **Způsoby identifikace subjektů (FO, PO) v informačním systému** | AIFO | Ne | *Projekt neřeší identifikaci subjektů, je zaměřen na kybernetickou bezpečnost. Nerelevantní.* |
| | IČO | Ne | *<popište>* |
| | Rodné číslo | Ne | *<popište>* |
| | Vlastní klientský identifikátor | Ne | *<popište včetně zákonného zmocnění a pravidel správy tohoto identifikátoru dle https://archi.gov.cz/nap:evidence_udaju_o_subjektech >* |
| | Jiný identifikátor | Ne | *<popište>* |
| **Předpokládaný počet subjektů údajů dotčených zpracováním osobních údajů v systému (orientační počet osob, jejichž údaje budou v systému zpracovávány)** | | Město Znojmo má včetně správního obvodu cca 91 000 obyvatel. | |
| **Způsoby zavedení základních principů práce s osobními a citlivými údaji dle GDPR a zákona o zpracování osobních údajů** | | | |
| **Zabezpečení zpracování:** | | Informační systém města zpracovává osobní data v rozsahu daném zákony. Zabezpečení je realizováno na základě identifikace v systému, tj. subjekt, útvar, | |

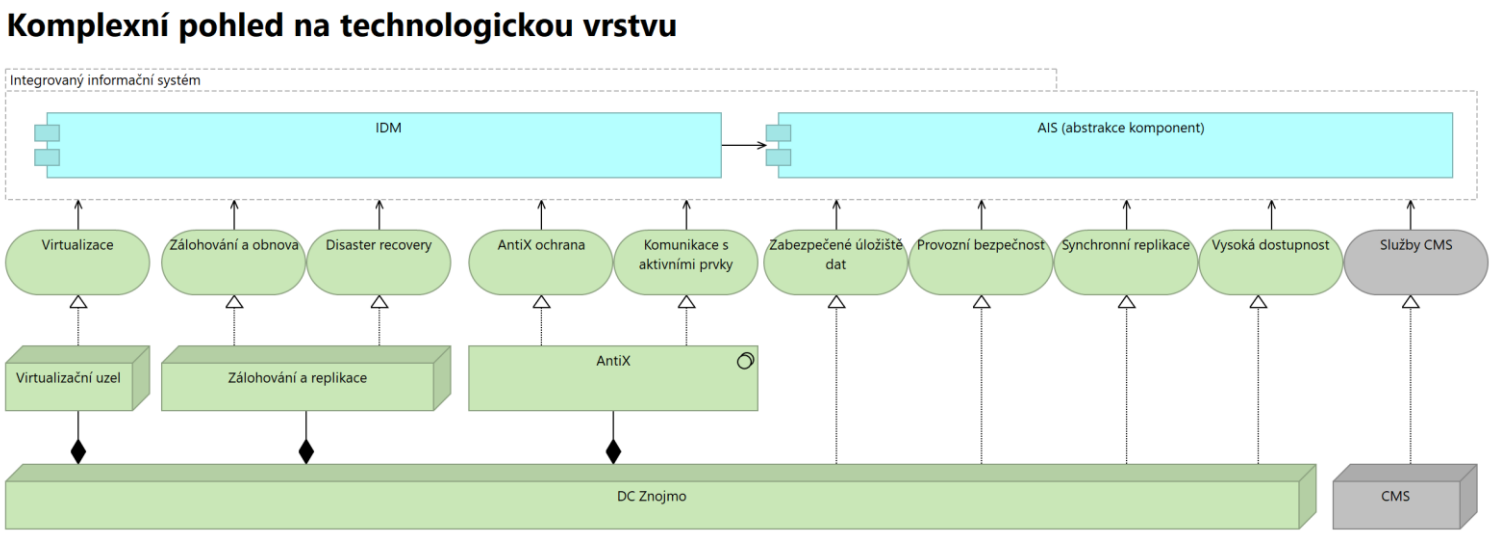
| Tabulka 26: **Nakládání s osobními a citlivými údaji** | |
|---|---|
| | funkční místo, uživatelská identita, uživatelská skupina, agenda, agendová činnostní role, aplikace, skupina aplikací, aplikační role. |
| **Logování přístupů k osobním a citlivým údajům:** | Je požadován komplexní audit všech operací (logování). |
| **Používáte nakládání s osobními údaji na základě doloženého souhlasu subjektu údajů:** | Ano, pokud je jejich poskytnutí dobrovolné.<br>Ne, pokud je jejich poskytnutí nutné s ohledem na zpracovávanou agendu. |
| **Ostatní:** | Vymazání osobních dat na základě žádosti nebo po uplynutí nezbytné lhůty. |

| Tabulka 27: **Vysvětlení v kontextu datové architektury úřadu** |
|---|
| **a) jaké k projektu existují či vznikají duplicity?** |
| **Ne.** |
| **b) jsou využity všechny sdílené služby?** |
| **Ano, protože je to účelné, hospodárné a v souladu se strategickými dokumenty města.** |
| **Vysvětlení datové architektury projektu:** |
| Data jsou vždy majetkem města, jejich použití limitují zákony nebo jiná obecně platná omezení vyplývající ze zvyklostí či etiky. Data jsou jako archiválie poskytovány Národním archívu podle zákona. |

## 2.2.5. Technologická architektura – vrstva IT technologie (HW a SW)

| **Tabulka 28: Katalog uzlů a klíčových funkcí nebo služeb** | | | |
|---|---|---|---|
| **ID** | **Typ prvku** | **Jméno prvku** | **Popis prvku** |
| **Prvky jsou uvedeny u odpovídajícího modelu pro lepší čitelnost.** | | | |

**Diagram technologické architektury – pohled struktury IT technologické architektury**



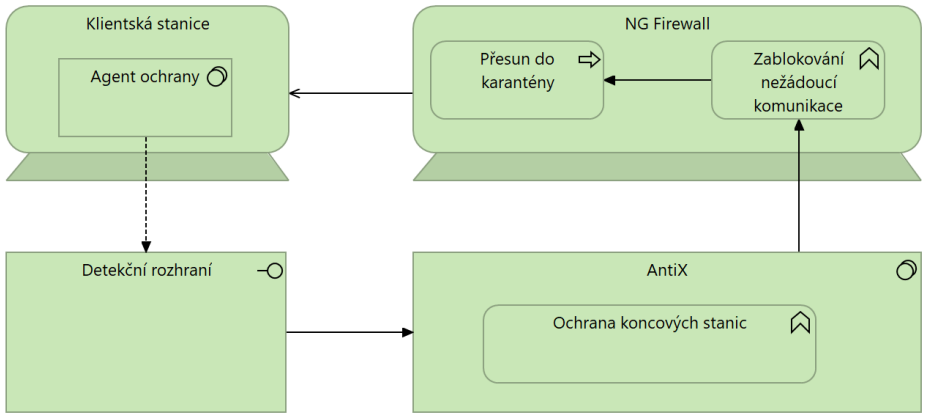

| **Prvek** | **Popis** |
|---|---|
| **Grouping** | |
| Integrovaný informační systém | Komplexní informační systém města včetně jeho organizací. |
| **Aplikační komponenty** | |
| IDM | Řídicí systém pro správu identit a s nimi spojených prostředků. |
| AIS (abstrakce komponent) | Agendový informační systém jako zjednodušená komponenta pro vyjádření všech funkcí, kterými disponuje s ohledem na vykonávané agendy. |
| **Nody** | |
| Virtualizační uzel | Virtualizační uzel obsahuje veškeré komponenty nutné k běhu virtualizovaných aplikací nebo infrastruktury. |

| | |
|---|---|
| Zálohování a replikace | Infrastrukturní celek poskytující služby zálohování a obnovy. |
| DC Znojmo | Datové centrum. Infrastrukturní celek poskytující základní služby pro fungování aplikací. |
| CMS | Centrální místo služeb, které je hlavním přípojným a propojovacím místem pro všechny základní služby eGovernmentu, ať už existující nebo nově budované. |
| **Služby** | |
| Virtualizace | Virtualizace infrastruktury. |
| Zálohování a obnova | Zálohování a obnova dat. Základní služba infrastruktury s ohledem na bezpečnost. |
| Disaster recovery | Služba okamžitého produkčního spuštění virtuálních serverů současně, přímo ze záložní storage (z úložiště dat) a s možností následné online migrace na cílovou produkční storage jako součást DR plánu. |
| AntiX ochrana | Služba infrastruktury chránící infrastrukturu před kybernetickými hrozbami. |
| Komunikace s aktivními prvky | Komunikace s aktivními prvky pro blokování nežádoucí aktivity. |
| Zabezpečené úložiště dat | Ukládání záloh a logů pro jejich ochranu. |
| Provozní bezpečnost | Služba provozní bezpečnosti monitoruje jednotlivá zařízení z pohledu jejich funkcí a chodu. Dává včasnou výstrahu o technických problémech a diagnostiku zařízení v síti. |
| Synchronní replikace | Zajištění bezvýpadkového provozu synchronní replikací v režimu active–active, tzn. že data budou poskytována současně z obou uložišť. |
| Vysoká dostupnost | Vysoká dostupnost infrastruktury. |
| Služby CMS | Nabízené služby CMS zejména napojení na ISZR, ale také další poskytované služby. |
| **Systémový software** | |
| AntiX | Vlastní software provádějící ochranu před útoky nebo malware. |

**Prvky jsou popsány v dílčích modelech, které následují níže.**

Technologické prvky spolu spolupracují, ať už se jedná o pokus o vynesení dat nebo narušení jiné bezpečnostní politiky například pokusem o útok na chráněná aktiva. Ve spolupráci s aktivními prvky bude tato komunikace blokována nebo omezena.

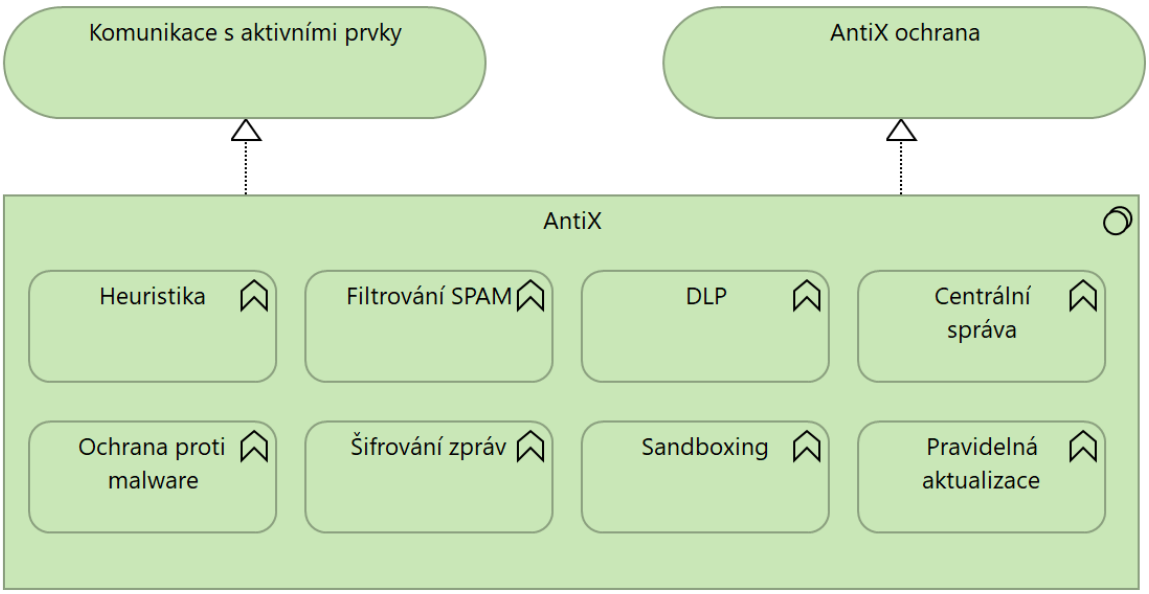
## Spolupráce technologických prvků




| Prvek | Popis |
|---|---|
| **Zařízení** | |
| NG Firewall | NG Firewall, který má nad sebou ještě další službu (filtrování, nebo nějaký spam detektor, detektor útoku atp.) |
| Klientská stanice | Lokální stanice klienta využívajícího služby nabízené technologickým centrem. |
| **Systémový SW** | |
| Agent ochrany | Agent ochrany koncového bodu napojený do centrálního rozhraní. |
| AntiX | Vlastní software provádějící ochranu před útoky nebo malware. |
| **Technologické rozhraní** | |

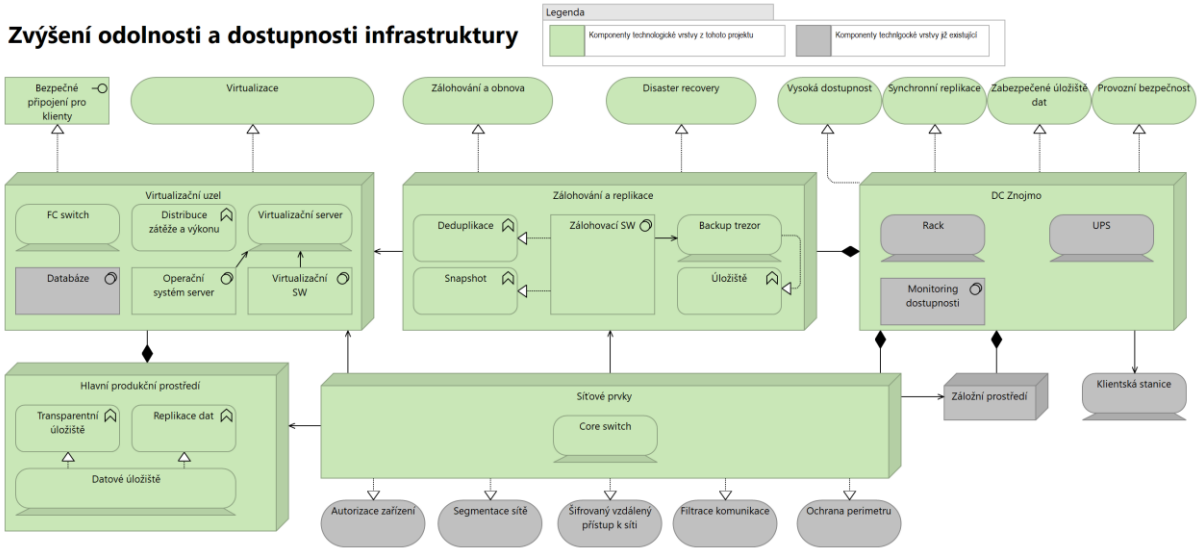
| | |
|---|---|
| Detekční rozhraní | Detekční rozhraní sbírající události nebo zprávy z koncových zařízení nebo dalších prvků umístěných v síti. |
| **Funkce** | |
| Zablokování nežádoucí komunikace | Na základě reportu provede zablokování nežádoucí komunikace v rámci sítě. |
| Ochrana koncových stanic | Bezpečnostní funkce, která zabraňuje kybernetickým útokům, detekuje škodlivé aktivity a poskytuje možnost okamžité nápravy. |
| **Technologická procedura** | |
| Přesun do karantény | Přesun prvku do karantény do vyřešení problému správcem, zabránění šíření nebo další komunikace a notifikace správce. |

# AntiX ochrana




| Prvek | Popis |
|---|---|
| **Služby** | |
| AntiX ochrana | Služba infrastruktury chránící infrastrukturu před kybernetickými hrozbami. |
| Komunikace s aktivními prvky | Komunikace s aktivními prvky pro blokování nežádoucí aktivity. |
| **Infrastrukturní SW** | |
| AntiX | Vlastní software provádějící ochranu před útoky nebo malware. |
| **Funkce** | |
| Heuristika | Heuristická analýza pro zjištění a detekci dosud neznámých počítačových virů. |
| Filtrování SPAM | Filtr příchozí / odchozí pošty odstraňující SPAM chránící síť. |
| Ochrana proti malware | Ochrana proti malware a jiným kybernetickým útokům koncových bodů včetně mobilních zařízení nebo virtuálního prostředí. |
| DLP | Slouží k identifikaci a ochraně citlivých dat a informací před jejich ztrátou či odcizením. |
| Sandboxing | Sandbox poskytuje procesům, které v něm běží, omezený přístup ke zdrojům hostitelského počítače. Přístup k disku je typicky omezen na vybrané adresáře, přístup k síti na vybrané servery a porty apod. |
| Šifrování zpráv | Šifrování zpráv založené na identitě uživatele, bez potřeby dalšího hardware, software. |
| Centrální správa | Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). |

| | |
|---|---|
| Pravidelná aktualizace | Stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. |




| Prvek | Popis |
|---|---|
| **Nod** | |
| Virtualizační uzel | Virtualizační uzel obsahuje veškeré komponenty nutné k běhu virtualizovaných aplikací nebo infrastruktury. |
| Zálohování a replikace | Infrastrukturní celek poskytující služby zálohování, ochrany dat před neoprávněnou činností a obnovy. |
| DC NEMBO | Datové centrum. Infrastrukturní celek poskytující základní služby pro fungování aplikací. |
| Hlavní produkční prostředí | Hlavní produkční prostředí pro běh informačních systémů |
| Síťové prvky | Výpočetní uzel obsahující síťové prvky (přepínače) a další vybavení potřebné k dosažení cílů aktivity. |
| Záložní prostředí | Záložní prostředí pro běh informačních systémů. |
| **Služby** | |
| Virtualizace | Komplexní virtualizace infrastruktura a desktopových prvků. |
| Zálohování a obnova | Zálohování a obnova dat. Základní služba infrastruktury s ohledem na bezpečnost. |
| Disaster recovery | Služba okamžitého produkčního spuštění virtuálních serverů současně, přímo ze záložní storage (z úložiště dat) a s možností následné online migrace na cílovou produkční storage jako součást DR plánu. |
| Vysoká dostupnost | Vysoká dostupnost infrastruktury. |
| Synchronní replikace | Zajištění bezvýpadkového provozu synchronní replikací v režimu active–active, tzn. že data budou poskytována současně z obou uložišť. |
| Zabezpečené úložiště dat | Ukládání záloh a logů pro jejich ochranu. |
| Provozní bezpečnost | Služba provozní bezpečnosti monitoruje jednotlivá zařízení z pohledu jejich funkcí a chodu. Dává včasnou výstrahu o technických problémech a diagnostiku zařízení v síti. |
| Autorizace zařízení | Autorizace zařízení pro přístup do vnitřní sítě. |
| Segmentace sítě | Služby pro vytváření segmentu sítě a jejich realizaci. |
| Šifrovaný vzdálený přístup k síti | Nastavení vzdáleného přístupu (VPN). |
| Filtrace komunikace | Filtrace komunikace, zamezení nepovolené komunikace mezi segmenty a omezení vstupu škodlivého kódu, či potenciálně nebezpečných aktivit. |
| Ochrana perimetru | Služby ochrany perimetru sítě. |
| **Zařízení** | |
| Klientská stanice | Klientská stanice využívající služby infrastruktury. |

| | |
|---|---|
| Backup trezor | Dedikované zařízení na uchovávání a správu záloh se speciální ochranou proti kryptování |
| Rack | Skříně pro uložení infrastruktury. |
| Virtualizační server | Virtualizační servery pro provoz virtuálních strojů. |
| Datové úložiště | Produkční datové úložiště pro virtuální infrastrukturu. |
| UPS | Zařízení pro zálohování výpadků napájení pro servery, páteřní prvky a koncové prvky. |
| Core switch | Vysokokapacitní switch umístěný v páteři nebo fyzickém jádru sítě. Core switche slouží jako brána do rozlehlé sítě (WAN) nebo internetu. |
| FC switch | Propojení mezi prostředky infrastruktura typicky server a datové pole. |
| **Systémový software** | |
| Zálohovací SW | Zálohovací SW pro virtuální i klasická data. |
| Databáze | Databáze informačních systémů. |
| Operační systém server | Operační systém serverové úrovně pro běh virtuálních strojů. |
| Virtualizační SW | Virtualizační SW pro běh informačního systému města. |
| Monitoring dostupnosti | Poskytuje jednotné řešení pro monitorování sítí, serverů, IP adres a switch portů, správu konfiguraci šířky pásma a sítě, analýzu pravidel, protokolů a zásad brány firewall, sledování využití aplikace a monitorujte úložná zařízení. |
| **Technologické rozhraní** | |
| Bezpečné připojení pro klienty | Bezpečné připojení pro klienty pro virtualizovanou infrastrukturu k jejím službám. |
| **Technologické funkce** | |
| Distribuce zátěže a výkonu | Distribuce zátěže a výkonu služeb. |
| Úložiště | Zálohování pro systémy organizace s nativní podporou všech hlavních aplikací organizace a jejich obnovy. |
| Deduplikace | Zabraňuje ukládání stejných datových bloků na jednom úložišti |
| Snapshot | Vytváření nezměnitelných uzamčených snapshotů, ze kterých je možné kdykoliv instantně obnovit produkční prostředí. |
| Transparentní úložiště | Bezpečné a vysoce dostupné úložiště pro zajištění plynulého chodu infrastruktury |
| Replikace dat | Funkce zabezpečuje synchronní replikací v režimu active–active. |

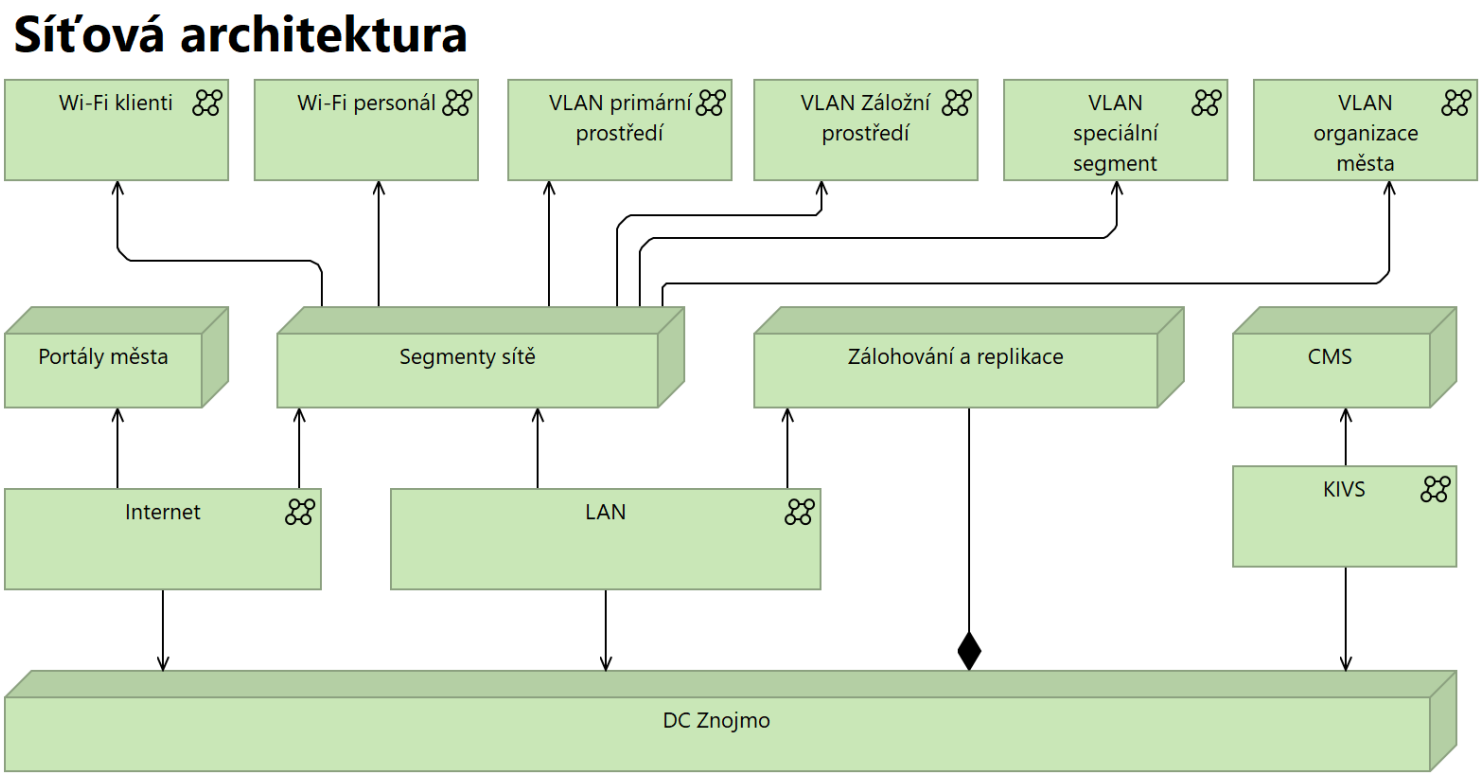
| Tabulka 29: **Vysvětlení v kontextu technologické architektury úřadu** |
|---|
| **a) jaké k funkčnímu celku existují či vznikají duplicity?** |
| Duplicity vznikají jako provozní redundance – z důvodu vysoké dostupnosti. Stávající infrastruktura vytváří záložní provozní prostor. |
| **b) jsou využity všechny sdílené služby?** |
| **Ano, protože je to účelné, hospodárné a v souladu se strategickými dokumenty města.** |
| **Vysvětlení technologické architektury projektu:** |
| Město Znojmo vytváří technologické / datové centrum pro své organizace a provoz budoucích aplikací odolné proti kybernetickým hrozbám. Jelikož je předmět projektu orientován na zvýšení kybernetické bezpečnosti, je v modelu věnována pozornost především souvisejícím službám a zařízením, jako jsou firewally, sondy, zálohovací zařízení a monitorovací služby, které jsou uvedeny v jednotlivých modelech.<br>Routování do CMS je zajištěno prostřednictvím ITS MVČR, přičemž město má v této síti vyhrazený subnet. K CMS budou přistupovat pouze povolená a ověřená zařízení ve vyhrazeném segmentu příslušnému dané aplikaci. |

## 2.2.6. Technologická architektura – vrstva komunikační infrastruktury

| **Tabulka 30: Katalog infrastrukturních komunikačních funkcí, sítí, cest a klíčových služeb** | | | |
|---|---|---|---|
| **ID** | **Typ prvku** | **Jméno prvku** | **Popis prvku** |
| | Comunication Network | LAN | Využito pro běžnou práci uvnitř organizace |

| Tabulka 30: Katalog infrastrukturních komunikačních funkcí, sítí, cest a klíčových služeb | | | |
|---|---|---|---|
| **ID** | **Typ prvku** | **Jméno prvku** | **Popis prvku** |
| | Comunication Network | Internet | Využito pro komunikaci s portálem města a dalšími portály |
| | Comunication Network | KIVS | Komunikační infrastruktura veřejné správy |
| | Comunication Network | Wi-Fi klienti | Wi-Fi pro klienty úřadu – úplně oddělená síť. |
| | Comunication Network | Wi-Fi personál | Zabezpečená a šifrovaná Wi-Fi. |
| | Comunication Network | VLAN primární prostředí | VLAN primární prostředí pro běh informačního systému. |
| | Comunication Network | VLAN Záložní prostředí | VLAN Záložní prostředí pro běh v záložní lokalitě. |
| | Comunication Network | VLAN speciální segment | Obecný prvek pro VLAN, kde jsou umístěny speciální segmenty jako například chráněná záloha, vyhrazená síť pro odbor apod. |
| | Comunication Network | VLAN organizace města | VLAN organizace města, kde může přistupovat k vybraným službám. |
| | Node | DC Znojmo | Technologické centrum. Infrastrukturní celek poskytující základní služby pro fungování aplikací. |
| | Node | Zálohování | Infrastrukturní celek poskytující služby zálohování a obnovy. |
| | Node | Portály města | Portálové služby města pro webovou prezentaci, sdílení informací s veřejností a digitální služby. |
| | Node | Segmenty sítě | Infrastrukturní celek poskytující služby síťové komunikace. |
| | Node | CMS | Centrální místo služeb, které je hlavním přípojným a propojovacím místem pro všechny základní služby eGovernmentu, ať už existující nebo nově budované. |

**Diagram technologické architektury – pohled struktury komunikační infrastruktury**




| Tabulka 31: Využití sdílených služeb komunikační infrastruktury | | | |
|---|---|---|---|
| **Název** | **Popis** | **Použito** | **Č. žádosti o výjimku** |
| **CMS** | Pro publikaci služeb tohoto projektu je využito Centrální místo služeb – aplikace jsou publikovány prostřednictvím CMS | Nerelevantní | Služby nepublikujeme, ale CMS využíváme |
| **KIVS** | Využití komunikační infrastruktury veřejné správy, tj. fyzického propojení infrastruktury úřadů připojení k CMS | Ano | |
| **NDC** | Umístění technologií do Národních datových center v perimetru CMS | Ne | |
| **Housing (IaaS)** | Využití umístění vlastní HW infrastruktury do prostor datového centra třetí strany | Ne | |

| Tabulka 32: **Vysvětlení v kontextu architektury komunikační infrastruktury úřadu** |
|---|
| **a) jaké k projektu existují či vznikají duplicity a proč?** |
| **Po dobu testovacího provozu budou zachovány komunikační propojení současné infrastruktury.** |
| **b) jsou využity všechny sdílené služby?** |
| Bude využit KIVS a CMS pro napojení na ISZR v souladu s požadavky zákona o ISVS 365 / 2000**.** Komunikace do CMS je kontrolována pomocí aktivních prvků a bezpečnostních politik. |
| **Vysvětlení architektury komunikační infrastruktury projektu:** |
| Komunikační vrstva zajišťuje tok dat mezi jednotlivými aplikacemi města a dále zajišťuje komunikaci s vnějším světem. Tyto úkoly komunikační vrstvy jsou zajišťovány prostřednictvím sítí poskytujících síťové služby.<br>LAN je rozčleněna pomocí síťových prvků na VLAN, kde jsou nastaveny pravidla a politiky podle potřeby. |

## 2.2.7. Bezpečnostní architektura

| Tabulka 33: Katalog bezpečnostní architektury projektu | | |
|---|---|---|
| **Dotčený nebo bezpečnostní prvek** | **Hrozba / riziko** | **Vysvětlení způsobu zmírnění hrozby / rizika prvkem architektury včetně technických a organizačních opatření** |
| AIS | **Autentizace uživatele**<br>Při prolomení hesla může dojít ke zneužití služeb IS města. | Pro zamezení zneužití služeb IS města při prolomení hesla bude zavedena dvoufaktorová autentizace prostřednictvím bezpečnostního tokenu zaslaného na mobilní telefon nebo čipové karty. |
| Vnitřní síť | **AntiX ochrana**<br>Škodlivý kód by se šířil bez zábran. | Vícevrstvá ochrana antiviru umožňuje bojovat proti celé řadě škodlivých činností, zejména proti krádeži hesel a účtů, neoprávněné těžbě kryptoměn, zašifrování souborů pomocí ransomwaru, získání citlivých osobních údajů, spamu, podvodům a dalším formám kybernetických útoků. |
| AIS | **Ochrana aplikace**<br>Služby vykonávané aplikacemi potřebují důslednější ochranu. | Nastavení AntiX ochrany a monitorování provozu. Zakoupení služeb bezpečnostního dohledu. |
| Datové centrum města | **Rozčlenění technologických prvků v lokalitách**<br>V současném stavu nejsou rozčleněny prvky v různých místnostech, aby se snížily škody v případě havárií. | Účelem této aktivity je vybudování a připojení druhé lokality ke stávajícímu primárnímu datacentru, která zajistí bezodstávkový provoz v případě výpadku kteréhokoliv datového úložiště nebo celé lokality. |
| Datové centrum města | **Nedostatečná kapacita zálohování**<br>Současná kapacita není dostatečná k provedení záloh systémů a jeho rychlé obnově. | Doplnění kapacity zálohování, sestavení plánu kontinuity činností a zrychlení obnovení provozu. |
| AIS | **Ochrana aplikací, informací a transakcí**<br>Ochrana aplikací, informací a transakcí před neoprávněnou činností a popřením provedených činností. | Zajištění ochrany proti lidskému faktoru, která umožňuje instantně vrátit libovolnou destruktivní operaci provedenou na datovém úložišti do původního stavu. Systém nabízí jediný dvouvrstvý přístup k úložišti záloh s vrstvou nesměřující k síti, zpožděným mazáním a neměnnými objekty pro obnovu. |
| AIS | **Nedostupnost informačního systému**<br>Informační systém města může být vyřazen útokem nebo nedostatečnou kapacitou infrastruktury. | Doplnění vhodných prvků pro provoz informačních systémů pro zajištění jejich dostupnosti i v případě útoku zaměřeného na snížení dostupnosti. |
| Datové centrum města<br>AIS<br>Vnitřní síť | **Ověření funkčnosti opatření**<br>Není systematicky prověřováno zabezpečení systémů. | Provádění penetračních testů a zavedení organizačního opatření na realizaci doporučení z nich vyplývajících. |
| Datové centrum města<br>AIS<br>Vnitřní síť | Bezpečnostní incident II a III kategorie. | V případě výskytu bezpečnostního incidentu kategorie II a III dle §31 odst. 1) vyhlášky č. 316/2014 Sb., vyhlášky o kybernetické bezpečnosti na lokální síti připojené do prostředí CMS obec tuto skutečnost nahlásí na ServiceDesk CMS. |

Tabulka 34: **Dopady narušení bezpečnosti informací v systému**

| | |
|---|---|
| **Možné dopady v případě narušení dostupnosti** | *V případě nedostupnosti systému by bylo dotčeno cca 247 zaměstnanců MěÚ, zaměstnanců organizací města a cca 91 000 obyvatel města a správního obvodu. Došlo by k omezení příjmu podání nebo obecně elektronických dokumentů, či by bylo omezeno nebo znemožněno provozování elektronických služeb.* |
| **Možné dopady v případě narušení důvěrnosti** | *Narušení důvěrnosti informací v systému může mít dopad na snížení důvěryhodnosti organizace vůči veřejnosti a ostatním partnerským organizacím. V systému budou zpracovávány osobní data nebo jinak chráněná aktiva.* |
| **Možné dopady v případě narušení integrity** | *Při narušení integrity informací v systému může dojít k chybnému výkonu veřejné správy, mohou být učiněny nesprávné závěry (např. ve správních řízeních apod.) mající dopad na majetková nebo osobní práva občanů.* |
| **Je v rámci Vaší organizace určen jakýkoliv prvek kritické infrastruktury?** | Ne |
| **Případně specifikujte ty určené prvky KI, jejichž činnost významně nebo zcela ovlivňuje tento posuzovaný informační systém:** | |

Tabulka 35: **Bezpečnostní opatření a zohlednění principu „security by design“**

| **Bezpečnostní opatření dle Minimálního bezpečnostního standardu NÚKIB** (dále jen „**MBS**“) | **Odpověď** | **Popis realizace, případně odůvodnění nezavedení** |
|---|---|---|
| **Organizační opatření** | | |
| Plán zavádění bezpečnostních opatření (kapitola 2.1 MBS) | Ano | V organizaci existuje útvar ICT, který má v náplni práce zajištění kybernetické bezpečnosti.<br>Dále budou nakoupeny služby bezpečnostního dohledu, který bude pomáhat při zvládání kybernetického incidentu. |
| Klasifikace a ochrana informací (kapitola 3 MBS) | Ano | Řešeno vnitřní směrnicí. |
| Řízení dodavatelů (kapitola 4 MBS) | Ano | Řešeno vnitřní směrnicí a schvalováním smluvních ujednání. Řízení a kontrola přístupů přes VPN do vnitřní sítě a monitoring zásahů pod privilegovanými účty. |
| Řízení lidských zdrojů (kapitola 5 MBS) | Ano | Řešeno vnitřní směrnicí, pravidelným proškolením a mystery shopingem. |
| Řízení změn (kapitola 6 MBS) | Ano | Řešeno vnitřní směrnicí, bezpečnostní politikou a kontrolami úseku ICT zaměřených na problematiku kybernetické bezpečnosti. |
| Řízení kontinuity činností (kapitola 7 MBS) | Ano | Směrnice definující kritické IS, nastavující standardy RTO a RPO. |
| Audit kybernetické bezpečnosti (kapitola 8 MBS) | Ano | Provádí se pravidelná kontrola, za kterou je zodpovědný úsek ICT, který doplní kapacity ze svých interních zdrojů (město je od něj nakoupí). V rámci projektu je naplánován také penetrační test, který prověří bezpečnostní nastavení. |
| Další opatření | Ano | Do projektu je zařazena aktivita Penetrační test, který prověří platnost bezpečnostních opatření a plán řešení krizových situací. |
| **Technická opatření** | | |
| Fyzická bezpečnost (kapitola 9 MBS) | Ano | K serverovně je řízen přístup, podmínky jsou kontrolovány čidly. |

| | | |
|---|---|---|
| Řízení přístupů<br>(kapitola 10 MBS) | Ano | Město využívá jako základ pro řízení přístupu Active Directory. Ověřování zařízení bude doplněno v projektu.<br>Pro řízení přístupu k digitálním službám bude využita NIA. |
| Ochrana před škodlivým kódem (kapitola 11 MBS) | Ano | Vnitřní síť je za ochrannou zdí firewallů, servery jsou pod monitoringem AntiX SW, mailové zprávy jsou systematicky kontrolovány na úrovni serveru a stanice mají také svůj AntiX SW. Projekt tuto kontrolu vylepšuje a rozšiřuje na další prvky infrastruktury mezi kterými doplňuje komunikaci. |
| Řešení kyberbezpečnostních událostí a incidentů (kapitola 12 MBS) | Ano | Město má zpracovány plány a postupy reakcí v případě kybernetického incidentu. Za jejich pravidelnou aktualizaci je zodpovědný úsek ICT. Projekt doplňuje detekční systémy pro odhalení kybernetických událostí.<br>Služba bezpečnostního dohledu bude nápomocna svými kapacitami ke zvládnutí kybernetického incidentu. |
| Aplikační bezpečnost (kapitola 13 MBS) | Ano | Aplikační bezpečnost je řešena v projektu pomocí rozšíření zálohování. |
| Kryptografické prostředky (kapitola 14 MBS) | Ano | Město doplní tuto schopnost informačního systému v rámci projektu. Veškeré služby nebo připojení na infrastrukturu bude realizováno pomocí šifrovaného připojení.<br>Komunikace s ISZR probíhá uvnitř zabezpečeného prostředí CMS. |
| Zajišťování úrovně dostupnosti informací (kapitola 15 MBS) | Ano | Projekt navrhuje dostupnost tak, aby nebyly omezeny služby informačního systému jak v případě havárie, tak v případě útoku zaměřeného na nedostupnost služeb. |
| Požadavky v oblasti cloudových služeb (kapitola 16 MBS) | Ano | Projekt nevyužívá služeb externího cloudu poskytovaného komerční organizací, ale využívá externí podporu pro správu incidentů a pomoc se zvládáním kybernetických hrozeb. |
| Řízení výjimek běhu, chyb a hlášení (kapitola 17.1 MBS) | Ano | Projekt doplňuje monitoring provozu na síti a jsou pořizována zařízení schopná napojení na SW pro detekci kybernetických událostí. |
| Ochrana webových aplikací (kapitola 17.2 MBS) | Ano | Bude aplikován standard OWASP pro služby poskytované jako internet (mail, messaging) nebo standardy pro vzdálený přístup VPN apod. |
| Zabezpečení komunikace s externími systémy (kapitola 17.4 MBS) | Ano | Projekt je zaměřena na vybudování takových možností. |
| Další opatření | Ano | Po přechodu do provozní fáze bude systém provozován 2 měsíce ve stavu zvýšeného dohledu se součinností dodavatele a správy sítě pro odladění plánů a chybových stavů aplikace, ale zejména pro odstranění nedostatků odhalených penetračním testem. |

| Tabulka 36: **Vysvětlení bezpečnostní architektury projektu** |
|---|
| Zvýšení bezpečnosti (konkrétně kybernetické bezpečnosti) je hlavním cílem, který realizace projektu sleduje. Bezpečnostní architektura se neomezuje pouze na některou z vrstev (aplikační, technologická), se kterou bývá kybernetická bezpečnost tradičně spojována, nicméně prolíná se všemi vrstvami architektury včetně byznysové. Nejnovější nástroje pro detekci bezpečnostních hrozeb totiž nestačí, pokud nejsou řádně nastavena pravidla pro detekci a hlášení bezpečnostních incidentů a také pravidla, která je nutná dodržovat pracovníky města za účelem předcházení bezpečnostním incidentům. |

## 2.2.8. Shoda s pravidly, standardizace a dlouhodobá udržitelnost

Tabulka 37: **Uveďte, které licence standardizovaných SW produktů nebo HW produktů budete pořizovat formou centrálních rámcových smluv zajištěných Ministerstvem vnitra. Pokud tuto formu nevyužijete, vysvětlete proč:**

V rámci požadavků na předložení nabídky neupřednostňujeme žádný konkrétní softwarový produkt. Dodavatel portálu bude vybrán v otevřeném výběrovém řízení. V zadávací dokumentaci bude specifikováno, že úřad akceptuje pořízení softwarových licencí k uvedeným produktům mimo centrální nákup pouze v případě výhodnější cenové nabídky.
Centrální nákup zvažujeme v případě KIVS.

| Rámec | Odpověď | Vysvětlení důvodů nepoužití |
|---|---|---|
| Centrální nákup produktů Cisco Systems | Ano | |
| Centrální nákup produktů IBM | Ano | |
| Centrální nákup produktů Microsoft | Ano | |
| Centrální nákup produktů Oracle | Ano | |
| Centrální nákup produktů VMware | Ano | |
| Centrální nákup CITRIX | Ano | |
| Centrální nákup ICT komodit | Ano | |
| Centrální soutěžení KIVS | Ano | |

**Tabulka 38: Cloud Computing**

| Požadavek | Odpověď | Vysvětlení |
|---|---|---|
| **Bude pro řešení využito služeb cloud computingu dle výsledku ekonomické výhodnosti provozu?** | Ne | Město nevyužije pro provoz systému komerčně poskytovaný cloud.<br>Pro svoje organizace bude datové centrum poskytovat služby, protože sjednocení služeb je výhodnější. |
| **Uveďte odkaz na poptávku, nabídku nebo využívání z katalogu cloud computingu** | | |

**Tabulka 39: Shoda se strategickými dokumenty**

| Požadavek | Odpověď | Číslo žádosti o výjimku | Vysvětlení |
|---|---|---|---|
| **Je řešení v souladu s Informační koncepcí úřadu?** | Ano | | Strategický plán rozvoje ICT města Znojmo<br>Vize:<br>7.4 Vize rozvoje ICT v oblasti bezpečnosti<br><br>Dopad:<br>Tato aktivita v sobě zahrnuje obecnou snahu o digitalizaci agend v souladu s centrálními strategiemi státu.<br>Na základě této aktivity je zpracován tento projekt.<br><br>Informační koncepce tyto cíle přejímá a dále je řeší v kapitole 6. Řízení bezpečnosti informačních systémů.<br>Projekt je součástí akčního plánu. |
| **Je řešení v souladu s Informační koncepcí ČR a cíli či principy Digitálního Česka?** | Ano | | Je v souladu s cílem „Rozvoj prostředí podporujícího digitální technologie v oblasti eGovernmentu“ a projektovým okruhem „Kybernetická bezpečnost“. |
| **Je řešení v souladu s NAP?** | Nerelevantní | | Předmět projektu se týká zvýšení kybernetické bezpečnosti města.<br>Národní architektonický plán cílí |

| Tabulka 39: Shoda se strategickými dokumenty | | | |
|---|---|---|---|
| **Požadavek** | **Odpověď** | **Číslo žádosti o výjimku** | **Vysvětlení** |
| | | | především na řádné využívání centrálních sdílených služeb, což však není předmětem tohoto projektu. Proto nerelevantní. |

| Tabulka 40: **Legislativní update** | |
|---|---|
| **Bude podpora zahrnovat rovněž udržování řešení v souladu s novými právními předpisy** (tzv. legislativní update)**?**<br>**Vysvětlete, v jakém rozsahu:** | **Jakým způsobem bude legislativní update hrazen?** |
| Ano. Legislativní upgrade je nezbytnou součástí podpory, protože jedním z důvodů existence informačního systému spisové služby je zákonný důvod. | Součást smlouvy o provozu a podpoře |

| Tabulka 41: **Jak je zajištěno řízené ukončení životnosti jednotlivých výstupů projektu a případný přechod na další řešení, či případná výměna dodavatele nad stejným řešením** (tzv. Exit strategie): |
|---|
| Předpokládaná délka spolupráce je daná dobou udržitelnosti, která je stanovena v délce 5 let. Po tuto dobu bude provozní a legislativní podporu udržovat vybraný dodavatel vzešlý z veřejné zakázky. Tato zakázka je plánována jako zahajovací krok investiční etapy.<br><br>Licence budou u běžných modulů nakupovány jako nevýhradní licence v časově neomezené variantě, aby bylo možné tyto získané licence provozovat po dobu, kterou žadatel uzná za vhodnou. Naopak moduly, které se vytvoří na míru zadavateli, budou licenčně ve vlastnictví žadatele.<br><br>Klíčovou částí dodaného systému jsou data, která jsou do systému migrována a také v něm vytvářená. Zde bude platit bez výjimky uplatňování zásady, že data jsou vždy majetkem města. Aby tato data byla použitelná i v jiných systémech, tak bude vždy vyžadována implementace exportních standardů s ohledem především na dokumenty. Tyto data bude možno migrovat v libovolnou dobu jako celek. Typicky půjde o požadavek na otevřený a strojově čitelný formát dat, kde bude zaručena kompatibilita v případě migrace, protože data v nesystematizované podobě či strojově nečitelném formátu jsou obvykle neupotřebitelná.<br><br>Další součástí je dokumentace, která umožní převzetí. V rámci veřejné zakázky bude požadována dokumentace v odpovídajícím rozsahu.<br><br>Ne vše je však možné realizovat bez součinnosti nahrazovaného dodavatele. Součástí servisních ujednání musí být i položka vynucující pod sankcí součinnost dodavatele k předání systému případnému dalšímu dodavateli. |

| Tabulka 42: **Vysvětlení standardizace a udržitelnosti architektury projektu** |
|---|
| Předmět projektu bude dodržovat všechny požadavky aktuálně platné legislativy. Počítáno je také s úpravami v případě legislativních změn (update součástí smlouvy o provozu a podpoře). Dále je počítáno s využitím nejlepších praktik (best practices) v oblasti kybernetické bezpečnosti a úzká spolupráce s příslušnými autoritami, jako je například NÚKIB. Pro zajištění udržitelnosti kybernetické bezpečnosti budou prováděny pravidelné kontroly, viz byznys vrstva. |

## 2.3. Kontrola shody architektury řešení projektu s požadavky Národního architektonického plánu

| Tabulka 43: **Kontrola shody architektury řešení projektu se vzory sdílených služeb eGovernmentu** | | | |
|---|---|---|---|
| **Název architektonického vzoru eGovernmentu** | **Byl dodržen vzor?** | **Č. žádosti o výjimku** | **Podrobný popis způsobu a míry dodržení vzorů návrhem řešení projektu** |
| **Centrální místo služeb** | | | |

| Tabulka 43: **Kontrola shody architektury řešení projektu se vzory sdílených služeb eGovernmentu** | | | | |
|---|---|---|---|---|
| **Název architektonického vzoru eGovernmentu** | | **Byl dodržen vzor?** | **Č. žádosti o výjimku** | **Podrobný popis způsobu a míry dodržení vzorů návrhem řešení projektu** |
| | Publikujete aplikační služby řešené tímto projektem do CMS druhé generace? | Nerelevantní | | Předmětem projektu je zvýšení kybernetické bezpečnosti. Neexistují aplikační služby, které bychom chtěli publikovat prostřednictvím CMS. |
| | Přistupujete ke službám jiných ISVS prostřednictvím CMS druhé generace? | Nerelevantní | | Projekt primárně řeší kybernetickou bezpečnost sítě města, ale do CMS přistupujeme a využíváme jej pro napojení na ISZR. |
| | Jakým způsobem přistupujete do CMS druhé generace? | KIVS | | Prostřednictvím krajské sítě. |
| | Využíváte vlastní připojení do veřejného internetu? | Ne | | |
| **Univerzální kontaktní místo** | | | | |
| | Publikujete na CzechPOINT všechny své samoobslužné služby tak, aby mohly být přístupné i asistovaně? | Nerelevantní | | Projekt řeší kybernetickou bezpečnost, nikoliv poskytování služeb klientům. |
| | Jste na centrálu CzechPOINT připojeni skrze systém CMS? | Nerelevantní | | |
| **Rozšířený backoffice úředníka** | | | | |
| | Máte služby CzechPOINT@office integrovány do svých systémů? | Nerelevantní | | |
| | Budou všechny interní aplikace dostupné z intranetu úřadu/resortu? | Nerelevantní | | |
| | Bude využito principu Single Sign-On? | Ano | | Již využíváme. |
| **ÚEP včetně eFakturace** | | | | |
| | Máte zajištěno předvyplňování formulářů ÚEP všemi státu známými údaji subjektu? | Nerelevantní | | Projekt řeší kybernetickou bezpečnost. Nezabývá se poskytováním služeb klientům. |
| | Máte zajištěn příjem a zpracování elektronických faktur? | Nerelevantní | | |
| **Elektronický systém spisové služby** | | | | |
| | Je realizace propojení systému se spisovou službou vytvořena dle rozhraní definovaného v kapitole 9 Národního standardu? | Nerelevantní | | |

| Tabulka 43: **Kontrola shody architektury řešení projektu se vzory sdílených služeb eGovernmentu** | | | |
|---|---|---|---|
| **Název architektonického vzoru eGovernmentu** | **Byl dodržen vzor?** | **Č. žádosti o výjimku** | **Podrobný popis způsobu a míry dodržení vzorů návrhem řešení projektu** |
| **Informační systém datových schránek** | | | |
| Je prováděno automatické vytěžování přijatých formulářů do informačního systému? | Nerelevantní | | |
| Jakým způsobem je předmět projektu napojen na ISDS? | Přímo pomocí webových služeb | | |
| **Propojený datový fond** | | | |
| Jste ke službám PPDF připojeni skrze CMS? | Nerelevantní | | Není předmětem tohoto projektu. |
| Využíváte pro překlad identity mezi agendami služby ISZR? | Nerelevantní | | Není předmětem tohoto projektu. |
| Využíváte pouze údaje, které máte explicitně uvedeny v daném zákoně? | Nerelevantní | | Není předmětem tohoto projektu. |
| Odebíráte na údaje PPDF notifikace skrze služby ISZR? | Nerelevantní | | Není předmětem tohoto projektu. |
| Je veškerá výměna údajů mezi ISVS realizována pomocí referenčního rozhraní (ISZR, eGSB/ISSS)? | Nerelevantní | | Není předmětem tohoto projektu. |
| **Elektronická identita** | | | |
| Využíváte služeb Národního bodu pro identifikaci a autentizaci? | Nerelevantní | | Elektronická identita není v rámci projektu řešena. Projekt řeší kybernetickou bezpečnost. |
| Používáte pro překlad identifikátoru identity do své agendy (BSI na AIFO) služeb ISZR? | Nerelevantní | | Není předmětem tohoto projektu. |
| Využíváte při obsazení identifikované a autentizované osoby do role úředníka systém JIP/KAAS? | Nerelevantní | | Není předmětem tohoto projektu. |

# 3. DALŠÍ ÚDAJE O PROJEKTU

## 3.1. Majetkoprávní vztahy projektu

| Tabulka 44: Majetkoprávní vztahy<br>Podmínka | Odpověď | Poznámka (důvod) |
|---|---|---|
| **Budou vám udělena výhradní práva k užívání k dodávanému produktu?** | Ne | Ano k speciálně upraveným modulům, ne k běžně prodávaným částem. |
| **Budou vám udělena nevýhradní práva k užívání k dodávanému produktu?** | Ano | Ne k speciálně upraveným modulům, ano k běžně prodávaným částem. |
| **Budou práva k autorskému dílu nějak omezena (IČO, konkrétní uživatel, převoditelnost a další šíření, úpravy produktu, parametry…)?** | Ne | Licence budou nastaveny tak, aby byly využitelní v rámci celé městské korporace – tj. město, organizace (různá IČO). |
| **Budete mít přístup ke zdrojovému kódu pro čtení?** | Ne | U běžných částí se jedná o obchodní tajemství, které není možné získat.<br>U upravených částí speciálně na míru městu ano. |
| **Bude vám či třetímu subjektu umožněno provádět údržbu, měnit produkt, upravovat jej či rozšiřovat bez souhlasu dodavatele?** | Ne | Další subjekty mohou bez licenčních omezení využívat rozhraní, ale běžně prodávané moduly takto upravovat nelze. |
| **Budete mít přístup k aktuální technické dokumentaci produktu?** | Ano | Smluvním ujednáním. |
| **Obsahuje budoucí smlouva ujednání o vyloučení odpovědnosti za výpadky fungování?** | Ano | Smluvním ujednáním. |
| **Budou externí nákupy veřejně soutěženy?** | Ano | Předpokládáme nadlimitní veřejnou zakázku. |
| **Bude celé nebo část řešení publikováno nebo bude využívat Open Source?** | Ano | Ne pro bezpečnostní SW nebo infrastrukturní SW, či spisové služby. Ano v případě centralizace komunikace. |

## 3.2. Finanční připravenost projektu

| Tabulka 45: Finanční připravenost<br>Druh financování | Odpověď | Popis zajištění, získání financování |
|---|---|---|
| **Financování pomocí ESIF1** | Ano | Výzvy programu IROP 03<br>Veškeré investiční výdaje projektu plánujeme podpořit z tohoto zdroje.<br>70% investičních prostředků, jedné se o přechodový region. |
| **Financování z vlastních zdrojů** | **Ano** | **Spolufinancování a předfinancování.**<br>15 % investice |

[1] Evropské strukturální a investiční fondy

| Tabulka 45: Finanční připravenost | | |
|---|---|---|
| **Druh financování** | **Odpověď** | **Popis zajištění, získání financování** |
| | | 100 % provozní náklady, školení, aktualizace dokumentace, bezpečnostní dohled. |
| **Financování pomocí jiných externích zdrojů** | Ne | Podle podmínek státní rozpočet pro přechodový region dává 15%. |

## 3.3. Metodická připravenost projektu

| Tabulka 46: Metodická připravenost | | |
|---|---|---|
| **Metodické zajištění** | **Odpověď** | **Popis** |
| **Řízení pomocí metodiky (uveďte název)** | Ano | Vhodná metodika (IPMA, PRINCE II) |
| **Podpora od projektové kanceláře úřadu/resortu** | Ne | Projekt počítá s externí administrací a dozorem nad implementací. |
| **Podpora od architektonické kanceláře úřadu/resortu** | Ne | Tuto funkci zastávají jednotlivé odbory podle zaměření projektu. |
| **Bude tento formulář součástí zadávací dokumentace projektu?** | Ne | |

## 3.4. Personální náročnost projektu

Tabulka 47: **Vysvětlete personální náročnost projektu, jako odhady dopadu do počtu systemizovaných míst, či kapacitní náročnost realizace projektu dle FTE:**

Projekt nemá dopad do systematizovaných míst mimo IT, bude využita stávající personální kapacita. U projektu předpokládáme snížená náročnosti práce o rutinní úkoly apod. Součástí projektu je také nezbytné zaškolení.

Navýšení naopak předpokládáme u nákladů na správu ICT, kde předpokládáme nákup dalších služeb (kapacit).

Pro podporu projektu bude využita smlouva o podpoře, která zajistí potřebné doplnění personálních kapacit včetně dohledu a service desku. Součástí bude také nákup L2 a L3 podpory včetně pomoci pro vyhodnocení záznamů z provozních systémů pro další zvládání kybernetických incidentů v rámci služby bezpečnostního dohledu, který bude zajišťovat vítěz veřejné zakázky.

Pro doplnění dalších služeb (v rámci naplňování vize) bude nutné bezpodmínečně navýšit personální kapacity. Politické rozhodnutí je očekáváno od nové reprezentace po vyhodnocení reálných zkušeností z provozu portálu občana (zahájení v roce 2023).

## 3.5. Harmonogram projektu

| Tabulka 48: Hrubý harmonogram předloženého projektu | | | | |
|---|---|---|---|---|
| **Fáze / milník** | **Začátek** | **Konec** | **Základní náplň** | **Navazuje na** |
| **Přípravná etapa (PE)** | 01. 05. 2022 | 31. 08. 2022 | Příprava projektu | X |
| **Investiční etapa (IE)** | 01. 09. 2022 | 31. 07. 2024 | Realizace projektu | PE |
| **Provozní etapa (PRE)** | 01. 08. 2024 | 31. 08. 2029 | Provozování projektu | IE |

| Tabulka 49: Související projekty (v rozvojovém programu, portfoliu úřadu) | |
|---|---|
| **Předchozí projekty** | **Popis návaznosti na předchozí projekty** |
| **Vybudování a správa datového centra města** | Vybudovaná infrastruktura a datové služby budou využity pro projekt a tento projekt bude tuto datovou základnu chránit.<br>Existující informační systémy, které bude projekt chránit. |
| **Souběžné projekty** | **Popis návaznosti na souběžné projekty** |
| **Školení zaměstnanců na kybernetickou bezpečnost** | Proškolení zaměstnanců v oblasti kybernetické bezpečnosti. |

| Tabulka 49: Související projekty (v rozvojovém programu, portfoliu úřadu) | |
|---|---|
| **Navazující projekty** | **Popis návaznosti na budoucí projekty** |
| | |

| Tabulka 50: **Vysvětlení dalších údajů o projektu** |
|---|
| Účelem realizace projektu je zvýšení kybernetické bezpečnosti města a nastavení všech relevantních procesů a pravidel s tím souvisejících. Projekt bude řízen standardizovanou projektovou metodikou, modifikovanou s přihlédnutím k jeho velikosti. |

## 3.6. Ekonomické parametry projektu

**Hrubý odhad hodnoty záměru nákupu služeb či investic** (externích výdajů)**, souvisejících s informačními a komunikačními technologiemi** (projektu).

**Plán předpokládané ekonomické náročnosti projektu založené na metodologii pětiletých celkových nákladů vlastnictví** (tzv. Total Costs of Ownership) **- účelové členění nákladů projektu.**

| Tabulka 51: TCO – výpočet je proveden v cenách bez DPH | | | | |
|---|---|---|---|---|
| **Souhrnná položka modelu TCO [Kč] bez DPH** | **① Výdaje na realizaci (výstavbu) projektu** | **② Výdaje na provoz a rozvoj (do konce aktuální smlouvy)** | **③ TCO 5 = ① + (②, přepočtené na 5 let)** | **Vysvětlení k položce** |
| **Počet měsíců trvání fáze** | 28 | 60 | 88 | V první buňce je součet času přípravné a investiční etapy. V druhé buňce je doba udržitelnosti po dobu 5 let. |
| **A. Předběžné analýzy (vč. rizik), tvorba zadání, výběr řešení, výběr dodavatele – náklady nákupního procesu** | 660 000 Kč | | 660 000 Kč | Obsahuje následující položky: Studie proveditelnosti Realizace veřejné zakázky |
| **B. Nákup SW a HW pro projekt (bez SaaS či PaaS)** | 23 801 076 Kč | | 23 801 076 Kč | Veškeré investice z projektu. V těchto položkách je také započteno vše, co je uvedeno bod body C, D, E, F, G, H, X. Tyto položky nelze jednoduše oddělit, protože jsou dodavateli nabízeny jako nedělitelný celek – vyjma penetračního testu. |
| **C. Analýza, finální projekt, vývoj, implementace, školení uživatelů, zkušební provoz a testy, případně i migrace dat a akceptační audit** | 100 000 Kč | | 100 000 Kč | Penetrační test |
| **D. Provoz a podpora řešení HW a SW (bez SaaS či PaaS)** | - Kč | 2 250 000 Kč | 2 250 000 Kč | Provozní náklady včetně navýšení o bezpečnostní dohled, další provozní náklady a aktualizaci bezpečnostní dokumentace. |
| **E. Hardware/Software údržba a průběžné úpravy (bez SaaS či PaaS)** | - Kč | | - Kč | |
| **F. Projekty postupné inovace a zlepšování (plánované)** | - Kč | | - Kč | |
| **G. Projekty upgrade (pokud jsou plánovány)** | - Kč | | - Kč | |

| Tabulka 51: TCO – výpočet je proveden v cenách bez DPH | | | | |
|---|---|---|---|---|
| **Souhrnná položka modelu TCO [Kč] bez DPH** | **① Výdaje na realizaci (výstavbu) projektu** | **② Výdaje na provoz a rozvoj (do konce aktuální smlouvy)** | **③ TCO 5 = ① + (②, přepočtené na 5 let)** | **Vysvětlení k položce** |
| **H. Zvýšené náklady užívání řešení vč. nákladů na přechod z předchozího řešení (pokud se vyskytnou)** | - Kč | | - Kč | |
| **I. Útlum, konzervace a ukončení řešení** | - Kč | | - Kč | |
| **X. Licence, HW, provoz, podpora, údržba, průběžný rozvoj – vše v subskripci (pouze SaaS a PaaS)** | - Kč | | - Kč | |
| **Z. Ostatní nerozlišené režijní náklady** | 1 013 075 Kč | | 1 013 075 Kč | Administrace projektu<br>Publicita stálá pamětní deska |
| **Celkem** | **25 574 151 Kč** | **2 250 000 Kč** | **27 824 151 Kč** | **Cena bez DPH** |

| Tabulka 52: **Popis funkčního celku, který je projektem rozšiřován či upravován (pokud existuje)** | |
|---|---|
| Projekt rozšiřuje architekturu úřadu o aspekt kybernetické bezpečnosti, na který doposud nebyl kladen příliš velký důraz. Popis rozšíření a úprav lze nalézt především na úrovni jednotlivých architektur (viz výše ve formuláři). | |
| **Plánované 5leté externí výdaje celého funkčního** celku (mimo tento projekt) [tis. Kč]**:** | 2 250 000 Kč bez DPH<br>včetně zhotovení dokumentace |

Tabulka 53: **Vysvětlení a komentář k souhrnu výdajů a ekonomické náročnosti projektu**

**Položkový rozpočet investic (způsobilé náklady)**

| Položka | Cena bez DPH | DPH | Cena vč. DPH |
|---|---|---|---|
| Příprava projektu | 410 000 Kč | 86 100 Kč | 496 100 Kč |
| IDM – správa identit | 5 028 940 Kč | 1 056 077 Kč | 6 085 017 Kč |
| AntiX Ochrana | 2 906 525 Kč | 610 370 Kč | 3 516 895 Kč |
| Zvýšení odolnosti a dostupnosti infrastruktury | 15 865 611 Kč | 3 331 778 Kč | 19 197 389 Kč |
| Penetrační test | 100 000 Kč | 21 000 Kč | 121 000 Kč |
| Dozor nad implementací opatření | 100 000 Kč | 21 000 Kč | 121 000 Kč |
| Příprava a organizace veřejné zakázky, právní služby | 250 000 Kč | 52 500 Kč | 302 500 Kč |
| Administrace projektu, management dotace | 150 000 Kč | 31 500 Kč | 181 500 Kč |
| Publicita stálá pamětní deska | 4 000 Kč | 840 Kč | 4 840 Kč |
| Ostatní náklady spojené s řízením a realizací projektu | 759 075 Kč | 159 406 Kč | 918 481 Kč |
| **Celkové přímé náklady** | **23 901 076 Kč** | **5 019 226 Kč** | **28 920 302 Kč** |
| **Celkové nepřímé náklady** | **1 673 075 Kč** | **351 346 Kč** | **2 024 421 Kč** |
| **Celkové způsobilé náklady** | **25 574 151 Kč** | **5 370 572 Kč** | **30 944 723 Kč** |

**Podpora a služby hrazené jako nezpůsobilý výdaj – výdaje paušální**

| Popis | TP za rok bez DPH | TP za 5 let bez DPH | TP za rok včetně DPH | TP za 5 let včetně DPH |
|---|---|---|---|---|
| Podpora a služby | 450 000 Kč | 2 250 000 Kč | 544 500 Kč | 2 722 500 Kč |
| **Celkem** | **450 000 Kč** | **2 250 000 Kč** | **544 500 Kč** | **2 722 500 Kč** |

Případný nedostatek kapacit bude řešen:

- V případě kybernetického incidentu bude nakoupen L2 a L3 support – jeho poskytování je zajištěno smlouvou s budoucím dodavatelem prvků kybernetické bezpečnosti.
- Další potřeby kapacity jsou vykrývány v rámci operativy v kapacitách pracovních úvazků.

Výkonové výdaje:

- Neočekávané výdaje – např. nutnost řešit havárii nebo kybernetický incident většího rozsahu je plánováno vytvořit fond na úrovni tajemníka úřadu.
- Povinnost podpory je zahrnuta v rámci paušálních výdajů.

| Tabulka 53: **Vysvětlení a komentář k souhrnu výdajů a ekonomické náročnosti projektu** |
|---|
| • Zvláštní objednávky v rámci projektu budou realizovány v případě L3 supportu, kde dodavatel bude garantovat smluvní cenu pod inflační doložkou a podle zkušeností je taková podpora nutná cca 2-3 x za rok. S ohledem na současné ceny odhadujeme náklady na 140 000 Kč bez DPH / rok.<br><br>Podrobná finanční analýza je součástí studie proveditelnosti kapitola 11 Finanční analýza. |

# 4. VYJÁDŘENÍ K BEZPEČNOSTNÍM ASPEKTŮM

| Tabulka 54: **Předkladatel prohlašuje, že předkládaný projekt bude realizován plně v souladu s níže uvedeným prohlášením** |
|---|
| *Text vyplňujte až na případnou výzvu OHA.* |

# 5. UPOZORNĚNÍ A DOPORUČENÍ

| Tabulka 55: **Upozornění a doporučení** |
|---|
| |

# 6. PŘÍLOHY

| Tabulka 56: **Přílohy** | | |
|---|---|---|
| **Typ** | **Číslo a název přílohy** | **Upřesnění přílohy** |
| Jiný | 1 Studie proveditelnosti | Studie proveditelnosti |
| Architektonický model | 2 Model v XML | Otevřený formát export z Archimate. |
| *Zvolte položku.* | | |
| Celkový počet příloh: | 2 | |