Název projektu: **Bezpečná infrastruktura města Znojma**

Registrační číslo projektu: **CZ.31.2.0/0.0/0.0/23_093/0008612**

Reforma/investice: **Investice 5: Navýšení investic do kybernetické bezpečnosti**

Milník/cíl: **Informační systémy, jejichž kybernetická bezpečnost byla posílena v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti (T248)**

Produktový rozpad

Rozpad projektu na hlavní produkty

I. Hlavní produkt	
ZÁKLADNÍ INFORMACE	
Název produktu:	**Posílené IS v rámci zabezpečení kyberbezpečnosti**
Počet posílených IS:	*17*
Názvy posílených IS:	• 8369 Scarabeus • 8297 Portál občana • 7227 Mapserver • 7226 Stavební úřad • 7223 Přestupky • 7221 Personalistika • 7138 YAMACO • 4933 MP Manager • 757 FLUXPAM5 • 684 Evidence myslivosti – EMY • 683 Evidence správních řízení – ESPI • 682 Ochrana ovzduší • 681 VITA • 613 HeleTax • 612 Evidence odpadů – EVI • 611 Editor vodoprávní evidence – eVPE • 497 GINIS
Předpokládané zahájení realizace produktu (dd. mm. rrrr):	1.11.2023

Předpokládané ukončení realizace produktu (dd. mm. rrrr):	31.5.2026
Celkové výdaje produktu bez DPH (Kč):	23 577 320 Kč
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor produkt navazuje:	Seznam informačních systémů vybraných v souladu s požadavky zákona č. 181/2014 Sb. o kybernetické bezpečnosti, jejichž kybernetická bezpečnost bude posílena.
Popis produktu:	
Předmětem realizace celého projektu je modernizace a rozšíření stávajícího HW a SW vybavení městského úřadu ve Znojmě. Projekt bude mít kladný vliv na zvýšení efektivnosti a dynamičnosti poskytovaných služeb v rámci agendy úřadu. Dojde k doplnění informačního systému o nové dílčí subsystémy k vytvoření celistvé softwarové platformy pro zajištění komplexní kybernetické bezpečnosti úřadu. Realizace projektu bude mít přímý vliv na fungování 17 informačních systémů: • 8369 Scarabeus • 8297 Portál občana • 7227 Mapserver • 7226 Stavební úřad • 7223 Přestupky • 7221 Personalistika • 7138 YAMACO • 4933 MP Manager • 757 FLUXPAM5 • 684 Evidence myslivosti – EMY • 683 Evidence správních řízení – ESPI • 682 Ochrana ovzduší • 681 VITA • 613 HeleTax • 612 Evidence odpadů – EVI • 611 Editor vodoprávní evidence – eVPE • 497 GINIS	
Způsob prokázání dokončení produktu:	**Dokument (seznam IS)**

II. Hlavní produkt	
ZÁKLADNÍ INFORMACE	
Název produktu:	**Zajištění finálního nezávislého auditu ověřujícího naplnění kybernetických požadavků**
Předpokládané zahájení realizace produktu (dd. mm. rrrr):	18.9.2025
Předpokládané ukončení realizace produktu (dd. mm. rrrr):	31.5.2026
Celkové výdaje produktu bez DPH (Kč):	230 000 Kč
Vazba na VZ:	3. Audit kybernetické bezpečnosti
Uveďte, na jaký monitorovací indikátor produkt navazuje:	Dokument potvrzující úspěšné testování a ověření souladu s požadavky na kybernetickou bezpečnost.
Popis produktu:	
Audit kybernetické bezpečnosti bude mít na konci realizace projektu za cíl posoudit a hodnotit úroveň bezpečnosti zavedených informačních technologií a kybernetických prostředí v organizaci. Cílem tohoto procesu bude ověřit, zda jsou implementovaná bezpečnostní opatření dostatečná k ochraně aktiv, dat a systémů před kybernetickými hrozbami. Audit kybernetické bezpečnosti bude proveden externím certifikovaným subjektem (nezávislým auditem nebo certifikačním orgánem).	
Způsob prokázání dokončení produktu:	**Dokument (výsledky auditu)**

III. Hlavní produkt	
ZÁKLADNÍ INFORMACE	
Název produktu:	**Administrativa projektu**
Předpokládané zahájení realizace produktu (dd. mm. rrrr):	1.9.2023
Předpokládané ukončení realizace produktu (dd. mm. rrrr):	16.8.2025
Celkové výdaje produktu bez DPH (Kč):	100 000 Kč
Vazba na VZ:	-
Uveďte, na jaký monitorovací indikátor produkt navazuje:	-

Popis produktu:	
Činnosti nepřímo související s projektem podle podmínek výzvy – administrativní náklady pořizované formou služby – zpracování žádosti o dotaci, organizace veřejné zakázky.	
Způsob prokázání dokončení produktu:	AKCEPTAČNÍ PROTOKOL

IV. Hlavní produkt	
ZÁKLADNÍ INFORMACE	
Název produktu:	**Ostatní aktivity a služby spojené s realizací projektu**
Předpokládané zahájení realizace produktu (dd. mm. rrrr):	17.8.2025
Předpokládané ukončení realizace produktu (dd. mm. rrrr):	31.5.2026
Celkové výdaje produktu bez DPH (Kč):	880 000 Kč
Vazba na VZ:	1. Analýza rizik
Uveďte, na jaký monitorovací indikátor produkt navazuje:	-
Popis produktu:	
Díky analýze rizik kyberbezpečnosti budou identifikovány, hodnoceny a řízeny potenciální hrozby a zranitelnosti informačních systémů města a celého kyberprostředí s cílem minimalizovat nebo eliminovat možné škody. Tato analýza je klíčovým prvkem efektivní kyberbezpečnostní strategie. Součástí projektu je také administrativní zajištění realizace projektu – pracovníci na DPP po dobu fyzické realizace projektu.	
Způsob prokázání dokončení produktu:	AKCEPTAČNÍ PROTOKOL

Rozpad hlavních produktů na podprodukty

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 1	
Název podproduktu:	**IS Scarabeus**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení,

	- autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning).

	Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix.

	Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti.

	Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky. Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni

	virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy. Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,65 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 2	
Název podproduktu:	**IS Portál občana**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb,

	- vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows.

	Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy.

	Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix).

	NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI) Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky. Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy.

<table>
<tr><td></td><td>Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1.

Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky.

Předpokládá se pořízení následujícího vybavení:
• 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28
• 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28
• 4 ks - SAN Switch (24 x 32Gb SFP28)
• 4 ks - virtualizační server
• 2 ks - sdílené diskové úložiště
• 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat</td></tr>
<tr><td colspan="2">Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (zaškrtnout, ke kterým § se technická opatření vztahují):
<table>
<tr><td>§ 3</td><td>§ 16</td><td>§ 18</td><td>§ 19</td><td>§ 20</td><td>§ 21</td><td>§ 22</td><td>§ 23</td><td>§ 24</td><td>§ 25</td><td>§ 26</td><td>§ 27</td></tr>
<tr><td>☐</td><td>☐</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☐</td><td>☒</td><td>☒</td><td>☐</td><td>☐</td><td>☒</td></tr>
</table></td></tr>
<tr><td>Předpokládané období realizace podproduktu
od – do (dd. mm. rrrr):</td><td>1.11.2023 – 31.5.2026</td></tr>
<tr><td>Celkové výdaje podproduktu bez DPH (Kč):</td><td>1 471 323,65 KČ</td></tr>
<tr><td>Vazba na VZ:</td><td>2. Zajištění kybernetické bezpečnosti MěÚ Znojmo
4. Dodávka antimalware zabezpečení</td></tr>
<tr><td>Uveďte, na jaký monitorovací indikátor podprodukt navazuje:</td><td>Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.</td></tr>
<tr><td>Způsob prokázání dokončení podproduktu:</td><td>Akceptační protokol</td></tr>
</table>

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 3	
Název podproduktu:	**IS Mapserver**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele

	Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows.

	Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy.

	Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix).

	NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI) Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky. Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy.

<table>
<tr><td></td><td>Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1.

Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky.

Předpokládá se pořízení následujícího vybavení:
• 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28
• 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28
• 4 ks - SAN Switch (24 x 32Gb SFP28)
• 4 ks - virtualizační server
• 2 ks - sdílené diskové úložiště
• 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat</td></tr>
<tr><td colspan="2">Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (zaškrtnout, ke kterým § se technická opatření vztahují):
<table>
<tr><td>§ 3</td><td>§ 16</td><td>§ 18</td><td>§ 19</td><td>§ 20</td><td>§ 21</td><td>§ 22</td><td>§ 23</td><td>§ 24</td><td>§ 25</td><td>§ 26</td><td>§ 27</td></tr>
<tr><td>☐</td><td>☐</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☐</td><td>☒</td><td>☒</td><td>☐</td><td>☐</td><td>☒</td></tr>
</table></td></tr>
<tr><td>Předpokládané období realizace podproduktu
od – do (dd. mm. rrrr):</td><td>1.11.2023 – 31.5.2026</td></tr>
<tr><td>Celkové výdaje podproduktu bez DPH (Kč):</td><td>1 471 323,65 KČ</td></tr>
<tr><td>Vazba na VZ:</td><td>2. Zajištění kybernetické bezpečnosti MěÚ Znojmo
4. Dodávka antimalware zabezpečení</td></tr>
<tr><td>Uveďte, na jaký monitorovací indikátor podprodukt navazuje:</td><td>Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.</td></tr>
<tr><td>Způsob prokázání dokončení podproduktu:</td><td>Akceptační protokol</td></tr>
</table>

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 4	
Název podproduktu:	**IS Stavební úřad**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele

	Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows.

	Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy.

	Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix).

	NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI) Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky. Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy.

<table>
<tr><td></td><td>Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1.

Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky.

Předpokládá se pořízení následujícího vybavení:
• 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28
• 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28
• 4 ks - SAN Switch (24 x 32Gb SFP28)
• 4 ks - virtualizační server
• 2 ks - sdílené diskové úložiště
• 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat</td></tr>
<tr><td colspan="2">Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (zaškrtnout, ke kterým § se technická opatření vztahují):
<table>
<tr><td>§ 3</td><td>§ 16</td><td>§ 18</td><td>§ 19</td><td>§ 20</td><td>§ 21</td><td>§ 22</td><td>§ 23</td><td>§ 24</td><td>§ 25</td><td>§ 26</td><td>§ 27</td></tr>
<tr><td>☐</td><td>☐</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☐</td><td>☒</td><td>☒</td><td>☐</td><td>☐</td><td>☒</td></tr>
</table></td></tr>
<tr><td>Předpokládané období realizace podproduktu
od – do (dd. mm. rrrr):</td><td>1.11.2023 – 31.5.2026</td></tr>
<tr><td>Celkové výdaje podproduktu bez DPH (Kč):</td><td>1 471 323,65 KČ</td></tr>
<tr><td>Vazba na VZ:</td><td>2. Zajištění kybernetické bezpečnosti MěÚ Znojmo
4. Dodávka antimalware zabezpečení</td></tr>
<tr><td>Uveďte, na jaký monitorovací indikátor podprodukt navazuje:</td><td>Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.</td></tr>
<tr><td>Způsob prokázání dokončení podproduktu:</td><td>Akceptační protokol</td></tr>
</table>

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 5	
Název podproduktu:	**IS Přestupky**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele

	Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows.

	Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy.

	Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix).

	NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI) Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky. Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy.

	Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,65 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 6	
Název podproduktu:	**IS Personalistika**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele

	Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows.

	Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy.

	Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix).

	NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI) Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento" režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky. Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy.

<table>
<tr><td></td><td>Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1.

Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky.

Předpokládá se pořízení následujícího vybavení:
• 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28
• 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28
• 4 ks - SAN Switch (24 x 32Gb SFP28)
• 4 ks - virtualizační server
• 2 ks - sdílené diskové úložiště
• 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat</td></tr>
<tr><td colspan="2">Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (zaškrtnout, ke kterým § se technická opatření vztahují):
<table>
<tr><td>§ 3</td><td>§ 16</td><td>§ 18</td><td>§ 19</td><td>§ 20</td><td>§ 21</td><td>§ 22</td><td>§ 23</td><td>§ 24</td><td>§ 25</td><td>§ 26</td><td>§ 27</td></tr>
<tr><td>☐</td><td>☐</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☐</td><td>☒</td><td>☒</td><td>☐</td><td>☐</td><td>☒</td></tr>
</table></td></tr>
<tr><td>Předpokládané období realizace podproduktu
od – do (dd. mm. rrrr):</td><td>1.11.2023 – 31.5.2026</td></tr>
<tr><td>Celkové výdaje podproduktu bez DPH (Kč):</td><td>1 471 323,65 KČ</td></tr>
<tr><td>Vazba na VZ:</td><td>2. Zajištění kybernetické bezpečnosti MěÚ Znojmo
4. Dodávka antimalware zabezpečení</td></tr>
<tr><td>Uveďte, na jaký monitorovací indikátor podprodukt navazuje:</td><td>Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.</td></tr>
<tr><td>Způsob prokázání dokončení podproduktu:</td><td>Akceptační protokol</td></tr>
</table>

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 7	
Název podproduktu:	**IS YAMACO**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele

	Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows.

	Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy.

	Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix).

	NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI) Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento" režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky. Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy.

<table>
<tr><td></td><td>Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1.

Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky.

Předpokládá se pořízení následujícího vybavení:
• 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28
• 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28
• 4 ks - SAN Switch (24 x 32Gb SFP28)
• 4 ks - virtualizační server
• 2 ks - sdílené diskové úložiště
• 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat</td></tr>
<tr><td colspan="2">Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (zaškrtnout, ke kterým § se technická opatření vztahují):
<table>
<tr><td>§ 3</td><td>§ 16</td><td>§ 18</td><td>§ 19</td><td>§ 20</td><td>§ 21</td><td>§ 22</td><td>§ 23</td><td>§ 24</td><td>§ 25</td><td>§ 26</td><td>§ 27</td></tr>
<tr><td>☐</td><td>☐</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☐</td><td>☒</td><td>☒</td><td>☐</td><td>☐</td><td>☒</td></tr>
</table></td></tr>
<tr><td>Předpokládané období realizace podproduktu
od – do (dd. mm. rrrr):</td><td>1.11.2023 – 31.5.2026</td></tr>
<tr><td>Celkové výdaje podproduktu bez DPH (Kč):</td><td>1 471 323,65 KČ</td></tr>
<tr><td>Vazba na VZ:</td><td>2. Zajištění kybernetické bezpečnosti MěÚ Znojmo
4. Dodávka antimalware zabezpečení</td></tr>
<tr><td>Uveďte, na jaký monitorovací indikátor podprodukt navazuje:</td><td>Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.</td></tr>
<tr><td>Způsob prokázání dokončení podproduktu:</td><td>Akceptační protokol</td></tr>
</table>

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 8	
Název podproduktu:	**IS MP Manager**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele

	Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows.

	Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy.

	Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix).

	NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI) Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky. Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy.

	Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,65 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 9	
Název podproduktu:	**IS FLUXPAM5**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele

	Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows.

	Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy.

	Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix).

	NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI) Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky. Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy.

	Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,65 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 10	
Název podproduktu:	**IS Evidence myslivosti – EMY**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele

	Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows.

	Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy.

	Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix).

	NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI) Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento" režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky. Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy.

	Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,65 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 11	
Název podproduktu:	**IS Evidence správních řízení – ESPI**
Stav podproduktu:	Realizován
Popis technických opatření, která budou posilovat IS:	**OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook.

	Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa

	Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix).

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☐	☐	☐	☒	☐	☒	☒	☐	☐	☐

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.12.2024**
Celkové výdaje podproduktu bez DPH (Kč):	**36 141,65 KČ**

Vazba na VZ:	4. Dodávka antimalware zabezpečení	
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.	
Způsob prokázání dokončení podproduktu:		**Akceptační protokol**

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 12	
Název podproduktu:	**IS Ochrana ovzduší**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce.

	Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS.

	Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí

	Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace).

	Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k

<table>
<tr><td></td><td>jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky.

Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy.

Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1.

Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky.

Předpokládá se pořízení následujícího vybavení:
• 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28
• 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28
• 4 ks - SAN Switch (24 x 32Gb SFP28)
• 4 ks - virtualizační server
• 2 ks - sdílené diskové úložiště
• 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat</td></tr>
<tr><td colspan="2">Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (zaškrtnout, ke kterým § se technická opatření vztahují):
<table>
<tr><td>§ 3</td><td>§ 16</td><td>§ 18</td><td>§ 19</td><td>§ 20</td><td>§ 21</td><td>§ 22</td><td>§ 23</td><td>§ 24</td><td>§ 25</td><td>§ 26</td><td>§ 27</td></tr>
<tr><td>☐</td><td>☐</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☐</td><td>☒</td><td>☒</td><td>☐</td><td>☐</td><td>☒</td></tr>
</table></td></tr>
<tr><td>Předpokládané období realizace podproduktu
od – do (dd. mm. rrrr):</td><td>1.11.2023 – 31.5.2026</td></tr>
<tr><td>Celkové výdaje podproduktu bez DPH (Kč):</td><td>1 471 323,65 KČ</td></tr>
<tr><td>Vazba na VZ:</td><td>2. Zajištění kybernetické bezpečnosti MěÚ Znojmo</td></tr>
</table>

	4. Dodávka antimalware zabezpečení	
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.	
Způsob prokázání dokončení podproduktu:		**Akceptační protokol**

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 13	
Název podproduktu:	**IS VITA**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce.

	Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS.

	Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí

	Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace).

	Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k

<table>
<tr><td></td><td>jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky.

Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy.

Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1.

Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky.

Předpokládá se pořízení následujícího vybavení:
• 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28
• 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28
• 4 ks - SAN Switch (24 x 32Gb SFP28)
• 4 ks - virtualizační server
• 2 ks - sdílené diskové úložiště
• 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat</td></tr>
<tr><td colspan="2">Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (zaškrtnout, ke kterým § se technická opatření vztahují):
<table>
<tr><td>§ 3</td><td>§ 16</td><td>§ 18</td><td>§ 19</td><td>§ 20</td><td>§ 21</td><td>§ 22</td><td>§ 23</td><td>§ 24</td><td>§ 25</td><td>§ 26</td><td>§ 27</td></tr>
<tr><td>☐</td><td>☐</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☐</td><td>☒</td><td>☒</td><td>☐</td><td>☐</td><td>☒</td></tr>
</table></td></tr>
<tr><td>Předpokládané období realizace podproduktu
od – do (dd. mm. rrrr):</td><td>1.11.2023 – 31.5.2026</td></tr>
<tr><td>Celkové výdaje podproduktu bez DPH (Kč):</td><td>1 471 323,65 KČ</td></tr>
<tr><td>Vazba na VZ:</td><td>2. Zajištění kybernetické bezpečnosti MěÚ Znojmo</td></tr>
</table>

	4. Dodávka antimalware zabezpečení	
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.	
Způsob prokázání dokončení podproduktu:		**Akceptační protokol**

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 14	
Název podproduktu:	**IS HeleTax**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce.

	Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS.

	Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí

	Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace).

	Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k

<table>
<tr><td></td><td>jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky.

Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy.

Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1.

Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky.

Předpokládá se pořízení následujícího vybavení:
• 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28
• 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28
• 4 ks - SAN Switch (24 x 32Gb SFP28)
• 4 ks - virtualizační server
• 2 ks - sdílené diskové úložiště
• 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat</td></tr>
<tr><td colspan="2">Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (zaškrtnout, ke kterým § se technická opatření vztahují):
<table>
<tr><td>§ 3</td><td>§ 16</td><td>§ 18</td><td>§ 19</td><td>§ 20</td><td>§ 21</td><td>§ 22</td><td>§ 23</td><td>§ 24</td><td>§ 25</td><td>§ 26</td><td>§ 27</td></tr>
<tr><td>☐</td><td>☐</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☐</td><td>☒</td><td>☒</td><td>☐</td><td>☐</td><td>☒</td></tr>
</table></td></tr>
<tr><td>Předpokládané období realizace podproduktu
od – do (dd. mm. rrrr):</td><td>1.11.2023 – 31.5.2026</td></tr>
<tr><td>Celkové výdaje podproduktu bez DPH (Kč):</td><td>1 471 323,65 KČ</td></tr>
<tr><td>Vazba na VZ:</td><td>2. Zajištění kybernetické bezpečnosti MěÚ Znojmo</td></tr>
</table>

	4. Dodávka antimalware zabezpečení	
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.	
Způsob prokázání dokončení podproduktu:		**Akceptační protokol**

Podprodukty v rámci I. hlavního produktu **- Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 15	
Název podproduktu:	**IS Evidence odpadů – EVI**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce.

	Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS.

	Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí

	Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace).

	Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k

<table>
<tr><td></td><td>jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky.

Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy.

Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1.

Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky.

Předpokládá se pořízení následujícího vybavení:
• 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28
• 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28
• 4 ks - SAN Switch (24 x 32Gb SFP28)
• 4 ks - virtualizační server
• 2 ks - sdílené diskové úložiště
• 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat</td></tr>
<tr><td colspan="2">Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (zaškrtnout, ke kterým § se technická opatření vztahují):
<table>
<tr><td>§ 3</td><td>§ 16</td><td>§ 18</td><td>§ 19</td><td>§ 20</td><td>§ 21</td><td>§ 22</td><td>§ 23</td><td>§ 24</td><td>§ 25</td><td>§ 26</td><td>§ 27</td></tr>
<tr><td>☐</td><td>☐</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☐</td><td>☒</td><td>☒</td><td>☐</td><td>☐</td><td>☒</td></tr>
</table></td></tr>
<tr><td>Předpokládané období realizace podproduktu
od – do (dd. mm. rrrr):</td><td>1.11.2023 – 31.5.2026</td></tr>
<tr><td>Celkové výdaje podproduktu bez DPH (Kč):</td><td>1 471 323,65 KČ</td></tr>
<tr><td>Vazba na VZ:</td><td>2. Zajištění kybernetické bezpečnosti MěÚ Znojmo</td></tr>
</table>

	4. Dodávka antimalware zabezpečení	
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.	
Způsob prokázání dokončení podproduktu:		**Akceptační protokol**

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 16	
Název podproduktu:	**IS Editor vodoprávní evidence – eVPE**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce.

	Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS.

	Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí

	Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace).

	Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k

	jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky. Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy. Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,65 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo

	4. Dodávka antimalware zabezpečení	
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.	
Způsob prokázání dokončení podproduktu:		**Akceptační protokol**

Podprodukty v rámci I. hlavního produktu **- Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 17	
Název podproduktu:	**IS GINIS**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce.

	Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS.

	Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí

	Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace).

	Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k

	jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky. Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy. Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,6 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo

	4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

Podprodukty v rámci III. hlavního produktu – Administrace projektu	
PODPRODUKT Č. 1	
Název podproduktu:	**ŽÁDOST O DOTACI VČETNĚ VŠECH POVINNÝCH PŘÍLOH**
Stav podproduktu:	Ukončen
Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1. 9. 2023 – 31. 12. 2023**
Celkové výdaje podproduktu bez DPH (Kč):	**70 000 KČ**
Vazba na VZ:	-
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	-
Popis podproduktu:	
Administrativa spojená s přípravou a podáním žádosti o podporu. Součástí poskytnuté služby je zpracování žádosti o podporu v systému ISKP14+, zpracování projektové žádosti, zajištění souhlasného stanoviska OHA.	
Vazba na jiné podprodukty:	
Zpracování žádosti o podporu a získání finančních prostředků na zajištění realizace má zásadní vliv na všechny ostatní realizované aktivity (podprodukty) projektu.	
Způsob prokázání dokončení podproduktu:	AKCEPTAČNÍ PROTOKOL

Podprodukty v rámci III. hlavního produktu - Administrace projektu	
PODPRODUKT Č. 2	
Název podproduktu:	**ORGANIZACE VEŘEJNÉ ZAKÁZKY**

Stav podproduktu:	Plánován
Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**15.5.2025 – 16.8.2025**
Celkové výdaje podproduktu bez DPH (Kč):	**30 000 KČ**
Vazba na VZ:	-
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	-
Popis podproduktu:	
Zajištění administrace otevřeného nadlimitního řízení na hlavní součásti realizace projektu – veřejná zakázka s názvem - Zajištění kybernetické bezpečnosti Znojmo.	
Vazba na jiné podprodukty:	
Zajištění administrace veřejné zakázky bude mít zásadní vliv na podprodukty, které mají být v rámci zakázky „Zajištění kybernetické bezpečnosti MěÚ Znojmo“ realizovány.	
Způsob prokázání dokončení podproduktu:	AKCEPTAČNÍ PROTOKOL

Podprodukty v rámci IV. hlavního produktu – Ostatní aktivity a služby spojené s realizací projektu	
PODPRODUKT Č. 1	
Název podproduktu:	**ANALÝZA RIZIK**
Stav podproduktu:	Plánován
Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**17.8.2025 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**460 000 KČ**
Vazba na VZ:	**1. Analýza rizik**
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	-

Popis podproduktu:	
Díky analýze rizik kyberbezpečnosti budou identifikovány, hodnoceny a řízeny potenciální hrozby a zranitelnosti informačních systémů města a celého kyberprostředí s cílem minimalizovat nebo eliminovat možné škody. Tato analýza je klíčovým prvkem efektivní kyberbezpečnostní strategie. Dokumentace bude pravidelně aktualizována. Opatřením dojde k naplnění § 3 vyhlášky o kybernetické bezpečnosti.	
Vazba na jiné podprodukty:	
Analýza rizik se bude prolínat všemi dalšími aktivitami realizovanými v rámci tohoto projektu – hodnocení realizovaných aktivit.	
Způsob prokázání dokončení podproduktu:	AKCEPTAČNÍ PROTOKOL

Podprodukty v rámci IV. hlavního produktu – Ostatní aktivity a služby spojené s realizací projektu	
PODPRODUKT Č. 2	
Název podproduktu:	**MZDOVÉ NÁKLADY**
Stav podproduktu:	Plánován
Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**17.8.2025 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**420 000 KČ**
Vazba na VZ:	-
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	-
Popis podproduktu:	
Zajištění kapacity interních pracovníků při přípravě a realizaci projektu.	
Vazba na jiné podprodukty:	
Zajištění administrativy a dohledu ze strany pracovníků bude mít přímý vliv na realizaci veřejné zakázky na dodávku jednotlivých komponent projektu a na samotné dodání a implementaci.	

Způsob prokázání dokončení podproduktu:	AKCEPTAČNÍ PROTOKOL