SMLOUVA O DODÁVCE A IMPLEMENTACI SYSTÉMU MANAGEMENTU BEZPEČNOSTI INFORMACÍ A POSKYTOVÁNÍ SLUŽEB

(ev. č. Objednatele: SOD/2024/021/Po)

Dnešního dne následující smluvní strany:

Objednatel:	**Nemocnice Znojmo, příspěvková organizace**
se sídlem:	MUDr. Jana Janského 2675/11, 669 02 Znojmo
zastoupen:	MUDr. Miroslavem Kavkou, MBA, FICS, ředitelem
IČO:	00092584
DIČ:	CZ00092584
Bankovní spojení:	[redacted]
Číslo účtu:	
Kontaktní osoba:	[redacted]

(dále jen „***Objednatel***")

a

Poskytovatel: Euro Enterprise Development s.r.o.

se sídlem:	Říční 456/10, Malá Strana (Praha 1), 118 00 Praha
IČO:	27773728
DIČ:	CZ27773728
bankovní spojení:	[redacted]
zastoupena:	Ing. Romanem Kratochvílem, jednatelem

zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, sp. zn. C331126

Kontaktní osoba: Ing. Roman Kratochvíl, jednatel

(dále jen „***Poskytovatel***")

(Objednatel a Poskytovatel dále jednotlivě též jen „***Smluvní strana***" nebo společně „***Smluvní strany***")

uzavírají v souladu s § 1746 odst. 2 zák. č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „***OZ***") s přihlédnutím k § 2586 a násl. OZ tuto

Smlouvu o dodávce a implementaci systému managementu bezpečnosti informací a poskytování služeb (dále jen „*Smlouva*")

1. ÚVODNÍ USTANOVENÍ

1.1. Smlouva se mezi výše uvedenými Smluvními stranami uzavírá na základě výsledku otevřeného zadávacího řízení na veřejnou zakázku s názvem *„Zajištění kybernetické bezpečnosti Nemocnice Znojmo"*, (dále jen *„**Veřejná zakázka**"*), zadávanou dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen *„**ZZVZ**"*). Jednotlivá ujednání Smlouvy tak budou vykládána v souladu se zadávacími podmínkami Veřejné zakázky uvedenými v zadávací dokumentaci včetně jejich příloh a v souladu s nabídkou Poskytovatele podanou na Veřejnou zakázku.

1.2. Smluvní strany prohlašují, že osoby podepisující Smlouvu jsou k tomuto jednání oprávněny.

1.3. Poskytovatel prohlašuje, že se seznámil se zadávací dokumentací Veřejné zakázky, včetně všech jejích příloh (dále jen *„**Zadávací dokumentace**"*), že ji považuje za dostatečný podklad pro plnění Veřejné zakázky, a to zejména v rozsahu nezbytném pro plnění předmětu Smlouvy, přičemž mu nejsou známy žádné nejasnosti či pochybnosti, které by znemožňovaly řádné plnění jeho závazku dle Smlouvy.

1.4. Poskytovatel dále prohlašuje, že se detailně seznámil s rozsahem a povahou předmětu plnění Smlouvy, že jsou mu známy veškeré relevantní technické, kvalitativní a jiné podmínky nezbytné pro realizaci předmětu plnění Smlouvy, a že disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci předmětu plnění Smlouvy za dohodnuté smluvní ceny uvedené ve Smlouvě, a to rovněž ve vazbě na jím prokázanou kvalifikaci pro plnění Veřejné zakázky a informace doložené za účelem hodnocení nabídky dle kritérií hodnocení „Kvalifikace (certifikace) realizačního týmu" a „Zkušenosti vybraných členů realizačního týmu".

1.5. Poskytovatel bere na vědomí, že Objednatel byl v souladu s § 22a zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících předpisů, ve znění pozdějších předpisů (dále jen *„**ZKB**"*), určen jako správce a provozovatel informačního systému základní služby, a proto se Poskytovatel uzavřením Smlouvy stane jeho významným dodavatelem dle § 2 písm. n) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen *„**VKB**"*). Plnění předmětu Smlouvy, a to ve všech jeho fázích a ve všech jeho částech musí splňovat veškeré podmínky dle ZKB a VKB. Poskytovatel se zavazuje informovat o těchto skutečnostech všechny své poddodavatele

a další osoby, s jejichž pomocí či jejichž prostřednictvím bude Poskytovatel plnit předmět Smlouvy.

1.6. Poskytovatel je při plnění předmětu Smlouvy povinen dodržovat Bezpečnostní požadavky v oblasti kybernetické bezpečnosti, které jsou uvedeny v příloze č. 6 Smlouvy.

1.7. Jestliže ve vztahu k plnění podle Smlouvy vznikne v souvislosti se zaváděním nebo aktualizací sytému řízení bezpečnosti informací nebo v souvislosti se zaváděním, prováděním nebo aktualizací bezpečnostních opatření podle ZKB a jeho prováděcích předpisů potřeba uzavřít dodatek k této Smlouvě nebo zvláštní smlouvu, zavazuje se Poskytovatel poskytnout Objednateli veškerou součinnost nezbytnou k formulaci obsahu takového dodatku, resp. smlouvy. Poskytovatel se pro tento případ rovněž zavazuje poskytnout součinnost směřující k uzavření takového dodatku, resp. smlouvy v souladu se ZZVZ.

1.8. Poskytovatel dále prohlašuje, že jím poskytované plnění odpovídá všem požadavkům vyplývajícím z platných právních předpisů, které se na plnění vztahují.

1.9. Objednatel předpokládá možnost kofinancování implementace předmětu plnění Veřejné zakázky z Integrovaného operačního programu (dále jen „***IROP***"), přičemž Poskytovatel je povinen postupovat tak, aby kofinancování z IROP nebylo ohroženo.

1.10. Pojmy s velkými počátečními písmeny definované ve Smlouvě budou mít význam, jenž je jim ve Smlouvě, včetně jejích příloh a dodatků, připisován. Pro vyloučení jakýchkoliv pochybností se Smluvní strany dále dohodly, že:

1.10.1. v případě jakékoliv nejistoty ohledně výkladu ustanovení Smlouvy budou tato ustanovení vykládána tak, aby v co nejširší míře zohledňovala účel Veřejné zakázky vyjádřený Zadávací dokumentací;

1.10.2. Poskytovatel je vázán svou nabídkou předloženou Objednateli v rámci zadávacího řízení Veřejné zakázky, která se pro úpravu vzájemných vztahů vyplývajících ze Smlouvy použije subsidiárně.

1.11. Není-li výslovně ve Smlouvě u lhůt či dob uvedeno, že příslušné dny jsou pracovní, jedná se o dny kalendářní.

2. ÚČEL SMLOUVY

2.1. Základním účelem, k jehož dosažení se Smlouva uzavírá, je zvýšení kybernetické bezpečnosti a celkové úrovně zabezpečení u Objednatele.

2.2. Konkrétně je účelem Smlouvy zásadní posílení ochrany informačních a komunikačních systémů Objednatele před kybernetickými útoky a únikem potencionálně vysoce citlivých dat. Realizace projektu je zaměřena na zavedení mechanismů, které výrazným způsobem zvýší bezpečnost síťové infrastruktury a jednotlivých informačních systémů Objednatele a celkově přispěje ke zvýšení úrovně kybernetické bezpečnosti.

3. PŘEDMĚT SMLOUVY

3.1. Předmětem Smlouvy je závazek Poskytovatele za podmínek Smlouvou dále stanovených poskytnout Objednateli plnění spočívající v zajištění komplexní dodávky a implementace systému managementu bezpečnosti informací, tedy řešení Systému kybernetické bezpečnosti (dále také jako „***SKB***") odpovídajícího požadavkům na funkcionality, výkonnost a dostupnost definovaných zejm. v příloze č. 1 Smlouvy, a dále zajištění veškerých dalších služeb a činností pro Objednatele specifikovaných ve Smlouvě (dále souhrnně jen „***Plnění***"). Plnění předmětu Smlouvy je rozděleno do těchto základních fází:

- Fáze 0 (analytická fáze)
- Fáze 1 (implementační fáze);
- Fáze 2 (provozní fáze a fáze rozvoje).

3.2. Fáze 0 – (analytická fáze) zahrnuje následující činnosti Poskytovatele:

3.2.1. vytvoření samostatného cílového konceptu pro každou aktivitu dle odst. 3.3.2 Smlouvy, přičemž každý cílový projekt bude projednán s Objednatelem v souladu s postupem dle přílohy č. 1 Smlouvy a bude obsahovat harmonogram plnění příslušné aktivity; vzorová šablona cílového konceptu tvoří přílohu č. 7 Smlouvy;

Výstupy: Cílové koncepty pro každou aktivitu dle odst. 3.3.2. v rozsahu dle přílohy č. 1 Smlouvy.

(dále jen „***Fáze 0***")

3.3. Fáze 1 – (implementační fáze) zahrnuje zejména následující činnosti Poskytovatele:

3.3.1. tvorba bezpečnostních politik, bezpečnostní dokumentace, analýzy rizik a dalších výstupů dle přílohy č. 1 Smlouvy (kapitola Analytické práce v oblasti bezpečnosti přílohy č. 1 Smlouvy; řádek 12 přílohy č. 5 Smlouvy – Ceník);

3.3.2. dodávka, implementace a integrace SKB do prostředí Objednatele, který tvoří následující aktivity:

- zavedení síťové analýzy (řádek 13 přílohy č. 5 Smlouvy – Ceník),
- realizace perimetrového a centrálních firewallů a Sandbox (řádek 14 přílohy č.

5 Smlouvy – Ceník),

- vybudování public key infrastructure (řádek 15 přílohy č. 5 Smlouvy – Ceník),
- implementace systému pro správu privilegovaných účtů (řádek 16 přílohy č. 5 Smlouvy – Ceník),
- modernizace síťové infrastruktury a WiFi (řádek 17 přílohy č. 5 Smlouvy – Ceník),
- e-mailová brána (řádek 18 přílohy č. 5 Smlouvy – Ceník),
- implementace sytému pro zálohování dat (řádek 19 přílohy č. 5 Smlouvy – Ceník),
- implementace nástroje pro zabezpečení zdravotnických zařízení (řádek 20 přílohy č. 5 Smlouvy – Ceník),

3.3.3. seznámení s obsluhou pro administrátory u příslušných aktivit (částí SKB),

3.3.4. testování u příslušných aktivit (částí SKB), a

3.3.5. zajištění přípravy nasazení a vlastní nasazení příslušné části SKB do produkčního provozu,

vše v rozsahu specifikace uvedené v příloze č. 1 Smlouvy a cílových konceptů. Pokud bude potřeba zajištění licencí pro implementaci/testování SKB či jeho části v rámci této fáze, budou tyto licence součástí nabídky Poskytovatele – blíže viz příloha č. 1 Smlouvy.

Výstupy: Analýza rizik, Bezpečnostní dokumentace, Funkční SKB odpovídající specifikaci řešení a veškerým požadavkům Objednatele, veškerá související uživatelská a technická dokumentace k SKB, včetně požadovaných licencí k SKB a protokoly o Poskytovatelem provedených, úspěšně zakončených testech SKB a o seznámení s obsluhou určených pracovníků Objednatele v rozsahu dle přílohy č. 1 Smlouvy a cílových konceptů.

(dále jen „***Fáze 1***")

3.4. Fáze 2 (provozní fáze a fáze rozvoje) zahrnuje následující činnosti Poskytovatele:

3.4.1. poskytování technické podpory, zahrnující služby maintenance licencí a podpory (full maintenance, SLA) SKB (společně dále jen „***Služby podpory***"); Služby podpory musí být poskytovány tak, že bude zajištěna kvalitní údržba SKB po dobu trvání Smlouvy s aktualizací veškeré uživatelské a technické dokumentace k SKB minimálně jedenkrát ročně a ke dni ukončení Smlouvy, Poskytovatel je povinen v rámci Služeb podpory aplikovat průběžné legislativní změny, aby SKB odpovídal aktuálně účinným právním předpisům; Poskytovatel se zavazuje sledovat změny ZKB a prováděcích právních předpisů alespoň jednou za kalendářní měsíc, přičemž

v případě změn, které by mohly ovlivnit funkčnost SKB, se zavazuje informovat Objednatele do 14 dnů od zjištění relevantní legislativní změny a nejpozději do 30 dnů od informování Objednatele tyto změny implementovat do SKB, není-li v konkrétním případě dohodnuto jinak; cena za sledování změn ZKB a prováděcích právních předpisů a jejich implementaci je zahrnuta v ceně SLA, a

3.4.2. poskytování služeb rozvoje SKB dle požadavků Objednatele (dále jen „***Služby rozvoje***"); za Služby rozvoje jsou považovány všechny služby, které nejsou součástí Služeb podpory či jiných služeb dle technické specifikace uvedené v příloze č. 1 Smlouvy. Služby rozvoje budou objednávány dle potřeb Objednatele v souladu s odst. 6.3 Smlouvy, přičemž Objednatel není povinen odebrat jakýkoliv objem Služeb rozvoje. Maximální objem Služeb rozvoje činí 180 člověkodnů (MD) za každých 5 let poskytování Služeb rozvoje.

(dále jen „***Fáze 2***").

3.5. Poskytovatel se zavazuje poskytovat Plnění v souladu s platnými právními předpisy, jakož i v souladu se všemi relevantními normami obsahujícími technické specifikace a technická řešení, technické a technologické postupy nebo jiná určující kritéria k zajištění, že materiály, výrobky, postupy a služby vyhovují předmětu Smlouvy a veškerým podmínkám uvedeným v Zadávací dokumentaci.

3.6. Poskytovatel prohlašuje, že předmět plnění dle Smlouvy není plněním nemožným, a že Smlouvu uzavírá po pečlivém zvážení všech možných důsledků. Poskytovatel dále prohlašuje, že se seznámil s předmětem plnění dle Smlouvy, a že Plnění může být poskytnuto způsobem a v termínech stanovených ve Smlouvě.

3.7. Objednatel se zavazuje zaplatit Poskytovateli za řádně poskytnuté Plnění v souladu se všemi podmínkami Smlouvy sjednanou cenu dle Smlouvy.

4. LHŮTA A MÍSTO PLNĚNÍ

4.1. Poskytovatel se zavazuje poskytovat Plnění v souladu s harmonogramem v následujících krocích (fázích):

Fáze	Zahájení Fáze	Ukončení (splnění) Fáze
Fáze 0 (cílové koncepty)	dnem nabytí účinnosti Smlouvy;	do 2 měsíců od účinnosti Smlouvy
Fáze 1 (veškeré aktivity dle řádku 12	dnem nabytí účinnosti Smlouvy;	do 31. 10. 2025

až 20 přílohy č. 5 Smlouvy - Ceník)		
Fáze 2 (Služby podpory odpovídající full maintenance)	po předání a převzetí příslušné dílčí části plnění dle Fáze 1	po dobu neurčitou od předání a převzetí příslušné dílčí části plnění dle Fáze 1
Fáze 2 (Služby podpory odpovídající SLA a Služby rozvoje)	po dokončení (akceptaci) Fáze 1	po dobu neurčitou od akceptace Fáze 1

4.2. Místem plnění je sídlo Objednatele, není-li mezi Smluvními stranami výslovně dohodnuto jinak. Přípravné a programovací práce je Poskytovatel oprávněn realizovat na svém vlastním technickém vybavení, což však nezakládá jakýkoliv nárok Poskytovatele na navýšení ceny Plnění v souvislosti s převodem na cílovou infrastrukturu Objednatele.

4.3. Pokud to povaha plnění dle Smlouvy umožňuje, je Poskytovatel oprávněn poskytovat plnění dle Smlouvy také vzdáleným přístupem. Bezpečnostní požadavky jsou uvedeny v příloze č. 6 Smlouvy.

4.4. Veškeré písemné výstupy, které je podle Smlouvy Poskytovatel povinen vytvořit a/nebo které při plnění Smlouvy vzniknou, budou Poskytovatelem Objednateli předány v sídle Objednatele, nebude-li mezi Smluvními stranami v konkrétním případě dohodnuto jinak.

5. CENA PLNĚNÍ A PLATEBNÍ PODMÍNKY

5.1. Cena za poskytování Plnění je sjednána dohodou Smluvních stran následovně:

5.1.1 Cena za poskytnutí části Plnění odpovídající Fázi 1 dle Smlouvy činí 68 242 900 Kč bez DPH, tj. 82 573 909 Kč včetně DPH ve výši 21 %; cena za poskytnutí Plnění dle Fáze 0 (cílové koncepty pro příslušné aktivity) je zahrnuta v ceně za Plnění dle Fáze 1; platební milníky Fáze 1 jsou uvedeny v odst. 5.6 Smlouvy;

5.1.2 Cena za poskytování části Fáze 2 odpovídající Službám podpory vč. full maintenance a SLA činí 3 750 610 Kč bez DPH za 1 rok poskytovaného plnění dle Smlouvy, tj. 4 538 238,10 Kč včetně DPH ve výši 21 %.

5.1.3 Cena za poskytování části Fáze 2 odpovídající Službám rozvoje činí 15 000 Kč bez DPH za 1 MD poskytovaného plnění dle Smlouvy, tj. 18 150 Kč včetně DPH ve výši 21 %.

Podrobný rozpad ceny za jednotlivé části Plnění je uveden v příloze č. 5 Smlouvy – Ceník. Jednotlivé položky v příloze č. 5 Smlouvy jsou dále rozděleny na projekt 1 a projekt 2, neboť Plnění dle této Smlouvy je kofinancováno ze dvou projektů IROP.

5.2. Součástí cen uvedených v tomto článku Smlouvy jsou i služby a dodávky nezbytné pro řádné a úplné poskytování předmětu Plnění. Poskytovatel nese veškeré náklady nutně nebo účelně vynaložené při plnění závazků ze Smlouvy včetně správních poplatků a nákladů souvisejících (zejména daně, pojištění, veškeré dopravní náklady, včetně nákladů souvisejících s provedením všech zkoušek a testů prokazujících dodržení předepsané kvality a parametrů předmětu Plnění dle Smlouvy, jakož nákladů souvisejících se zajištěním dalších podkladů, předpisů apod.).

5.3. Veškeré ceny uvedené v tomto článku Smlouvy jsou ceny v korunách českých (CZK). Stane-li se v průběhu trvání Smlouvy Česká republika členem Evropské měnové unie a bude-li v závazně stanoven koeficient pro přepočet CZK na EUR, budou ceny sjednané v CZK přepočteny do EUR na základě odpovídajícího koeficientu sjednaného v mezinárodních úmluvách, kterými bude Česká republika vázána, jakož i v souladu s případnou tomu odpovídající vnitrostátní právní úpravou České republiky.

5.4. Veškeré ceny uvedené v tomto článku Smlouvy jsou cenami maximálními, nejvýše přípustnými, nepřekročitelnými a jsou platné a konstantní po celou dobu platnosti Smlouvy, není-li uvedeno jinak. Cenu Plnění je možné změnit v případě změny výše sazby DPH v důsledku změny právních předpisů. V případě změny sazby DPH je Poskytovatel povinen k ceně bez DPH účtovat DPH v platné výši. Smluvní strany se dohodly, že v případě změny ceny v důsledku změny sazby DPH není nutno ke Smlouvě uzavírat dodatek. Poskytovatel odpovídá za to, že sazba daně z přidané hodnoty je stanovena v souladu s platnými právními předpisy.

5.5. Cenu Služeb podpory a Služeb rozvoje dle odst. 5.1.2 a 5.1.3 Smlouvy lze od 1. 1. 2028 upravit z důvodu inflace ponížené o 5 procentních bodů za podmínek dále uvedených:

5.5.1. Inflací se rozumí Průměrná roční míra inflace, kterou udává každým kalendářním rokem Český statistický úřad za rok předcházející vyjádřená v procentech.

5.5.2. Počínaje rokem 2028 a dále do budoucna je Poskytovatel oprávněn zvýšit cenu Služeb podpory a Služeb rozvoje nejčastěji jednou ročně z důvodů inflace, a to o tolik procent, kolik procent činila Průměrná roční míra inflace za rok bezprostředně předcházející ponížená o 5 procentních bodů; součástí (např. přílohou) daňového dokladu dle odst. 5.6 Smlouvy bude vymezení údajů o inflaci

dle Smlouvy, přičemž Objednatel je oprávněn tuto fakturu před uplynutím lhůty splatnosti vrátit, pokud inflace nebude vyjádřena správně (vrácením vadné faktury Poskytovateli přestává běžet původní lhůta splatnosti, nová lhůta splatnosti běží ode dne vystavení nové faktury).

5.5.3. Cena Služeb podpory nebo Služeb rozvoje upravená z důvodu inflace poníženě o 5 procentních bodů se považuje za sjednanou cenu, která nevyžaduje uzavření dodatku ke Smlouvě. Pokud inflace za příslušný rok nepřekročí 5 %, nebude cena Služeb podpory a Služeb rozvoje upravena.

5.6. Ceny dle Smlouvy budou hrazeny na základě daňových dokladů vystavených Poskytovatelem (dále jen „***Faktura***" či „***Faktury***") následovně:

- Právo fakturovat cenu za poskytnutí části Plnění dle Fáze 1 Smlouvy (zahrnuje též cenu za Fázi 0) vzniká Poskytovateli po předání / akceptaci odpovídajícího dílčího plnění v rámci Fáze 1 následovně:

Platební milník	**Podmínka pro vznik oprávnění vystavit Fakturu**	**Cena za daný platební milník (odkaz na přílohu č. 5 Smlouvy)**
Implementace (aktivita „Analytické práce v oblasti bezpečnosti")	Podepsaný akceptační protokol dle čl. 6 Smlouvy	Buňka D12
Dodání HW, SW vč. záruky na 2 roky (aktivita „Zavedení síťové analýzy")	Podepsaný předávací protokol dle čl. 6 Smlouvy	Buňka E13
Implementace (aktivita „Zavedení síťové analýzy")	Podepsaný akceptační protokol dle čl. 6Smlouvy	Buňka D13
Dodání HW, SW vč. záruky na 2 roky (aktivita „Realizace perimetrového a centrálních firewallů a Sandbox")	Podepsaný předávací protokol dle čl. 6 Smlouvy	Buňka E14
Implementace (aktivita „Realizace perimetrového a centrálních firewallů a Sandbox")	Podepsaný akceptační protokol dle čl. 6 Smlouvy	Buňka D14
Dodání HW, SW vč. záruky na 2 roky (aktivita „Vybudování public key infrastructure")	Podepsaný předávací protokol dle čl. 6 Smlouvy	Buňka E15
Implementace (aktivita „Vybudování public key infrastructure")	Podepsaný akceptační protokol dle čl. 6Smlouvy	Buňka D15

Dodání HW, SW vč. záruky na 2 roky (aktivita „implementace systému pro správu privilegovaných účtů")	Podepsaný předávací protokol dle čl. 6 Smlouvy	Buňka E16
Implementace (aktivita „implementace systému pro správu privilegovaných účtů")	Podepsaný akceptační protokol dle čl. 6Smlouvy	Buňka D16
Dodání HW, SW vč. záruky na 2 roky (aktivita „modernizace síťové infrastruktury a WiFi")	Podepsaný předávací protokol dle čl. 6 Smlouvy	Buňka E17
Implementace (aktivita „modernizace síťové infrastruktury a WiFi")	Podepsaný akceptační protokol dle čl. 6Smlouvy	Buňka D17
Dodání HW, SW vč. záruky na 2 roky (aktivita „e-mailová brána")	Podepsaný předávací protokol dle čl. 6 Smlouvy	Buňka E18
Implementace (aktivita „e-mailová brána")	Podepsaný akceptační protokol dle čl. 6Smlouvy	Buňka D18
Dodání HW, SW vč. záruky na 2 roky (aktivita „implementace sytému pro zálohování dat")	Podepsaný předávací protokol dle čl. 6 Smlouvy	Buňka E19
Implementace (aktivita „implementace sytému pro zálohování dat")	Podepsaný akceptační protokol dle čl. 6Smlouvy	Buňka D19
Dodání HW, SW vč. záruky na 2 roky (aktivita „implementace nástroje pro zabezpečení zdravotnických zařízení")	Podepsaný předávací protokol dle čl. 6 Smlouvy	Buňka E20
Implementace (aktivita „implementace nástroje pro zabezpečení zdravotnických zařízení")	Podepsaný akceptační protokol dle čl. 6Smlouvy	Buňka D20

- Je-li Poskytovatel dle odst. 4.1. této Smlouvy povinen dokončit Fázi 1 nejpozději do 31. 10. 2025, je zároveň povinen vystavit všechny faktury za příslušné aktivity Fáze 1 nejpozději do 1. 11. 2025.
- cena za poskytování části Fáze 2 odpovídající full maintenance dle Služeb podpory bude Objednatelem uhrazena ročně vždy před zahájením příslušného roku, v němž budou Služby podpory (full maintenance) poskytovány, přičemž Poskytovatel je oprávněn příslušnou Fakturu vystavit nejdříve 3 (slovy: tři) pracovní dny před zahájením příslušného roku, v němž budou Služby podpory (full maintenance) poskytovány; s ohledem na nemožnost přesného určení

počátku zahájení poskytování Služeb podpory (full maintenance) Smluvní strany uvádí, že nezapočne-li poskytování Služeb podpory (full maintenance) prvního dne kalendářního roku, pak první Faktura za poskytování Služeb podpory (full maintenance) bude vystavena na období od zahájení Služeb podpory (full maintenance) do konce kalendářního roku, v němž poskytování Služeb podpory (full maintenance) započalo, a to ve výši poměrné části ceny odpovídající tomuto období poskytování Služeb podpory (full maintenance); dokud nebudou převzaty veškeré aktivity dle Fáze 1, bude fakturována vždy poměrná část ceny full maintenance dle Služeb podpory pro každou aktivitu dle přílohy č. 5 Smlouvy (Ceník).

- Cena za poskytování části Fáze 2 odpovídající SLA dle Služeb podpory bude Objednatelem hrazena čtvrtletně vždy po ukončení posledního měsíce příslušného kalendářního čtvrtletí (leden až březen, duben až červen, červenec až září, říjen až prosinec), v němž budou Služby podpory (SLA) poskytovány, přičemž Poskytovatel je oprávněn příslušnou Fakturu vystavit nejdříve 2 pracovní dny po ukončení příslušného kvartálu, v němž budou Služby podpory (SLA) poskytovány; s ohledem na nemožnost přesného určení počátku zahájení poskytování Služeb podpory (SLA) Smluvní strany uvádí, že nezapočne-li poskytování Služeb podpory prvního dne kalendářního čtvrtletí, pak první Faktura za poskytování Služeb podpory bude vystavena na období od zahájení Služeb podpory (SLA) do konce příslušného čtvrtletí, v němž poskytování Služeb podpory započalo, a to ve výši poměrné části ceny odpovídající tomuto období poskytování Služeb podpory;
- cena za poskytování části Fáze 2 odpovídající Službám rozvoje bude Objednatelem hrazena za skutečně poskytnuté Služby rozvoje na základě sazby za MD podle počtu řádně poskytnutých MD plnění Služeb rozvoje v souladu se Smlouvu čtvrtletně vždy po ukončení posledního měsíce příslušného kalendářního čtvrtletí (leden až březen, duben až červen, červenec až září, říjen až prosinec, v němž budou Služby rozvoje poskytovány, přičemž Poskytovatel je oprávněn příslušnou Fakturu vystavit nejdříve 2 pracovní dny po ukončení příslušného čtvrtletí, v němž budou Služby podpory poskytovány.

5.7. Kopie příslušných akceptačních protokolů (příp. předávacích protokolů v případě HW a SW) podepsaných pověřenými zástupci obou Smluvních stran jsou povinnou náležitostí každé Faktury vystavené Poskytovatelem za poskytnutí Plnění (či jeho části) dle Smlouvy. V případě, že Plnění není akceptováno některým z uvedených způsobů, Poskytovatel není oprávněn vystavit příslušnou Fakturu, není-li výslovně uvedeno jinak.

5.8. Faktury musí obsahovat evidenční číslo Smlouvy a veškeré údaje vyžadované právními předpisy, zejména zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění

pozdějších předpisů, a § 435 OZ, obecné náležitosti účetních dokladů a současně požadavky poskytovatele dotace alespoň v rozsahu čísla projektu (rozlišení projektu 1 (CZ.06.01.01/00/22_004/0000076) a projektu 2 (CZ.06.01.01/00/22_004/0000077) dle přílohy č. 5 Smlouvy – Ceník) a rozlišení uznatelných a neuznatelných nákladů (dle pokynu Objednatele).

5.9. Splatnost Faktur je stanovena do 30 (třiceti) dnů ode dne doručení Faktury Objednateli. Cena za poskytnutí Plnění či jeho části se považuje za uhrazenou okamžikem odepsání fakturované ceny z bankovního účtu Objednatele ve prospěch účtu Poskytovatele. Uvedený bankovní účet musí být zveřejněn správcem daně způsobem umožňujícím dálkový přístup. V případě, že účet tímto způsobem zveřejněn nebude, je Objednatel oprávněn uhradit Poskytovateli cenu na úrovni bez DPH, DPH Objednatel poukáže správci daně. Stane-li se Poskytovatel nespolehlivým plátcem ve smyslu § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, je povinen neprodleně o tomto písemně informovat Objednatele.

5.10. Nebude-li jakákoliv Faktura obsahovat některou povinnou nebo dohodnutou náležitost nebo bude-li chybně vyúčtována cena nebo DPH, je Objednatel oprávněn tuto fakturu před uplynutím lhůty splatnosti bez zaplacení vrátit Poskytovateli k provedení opravy s vyznačením důvodu vrácení. Poskytovatel provede opravu vystavením nové faktury. Vrácením vadné faktury Poskytovateli přestává běžet původní lhůta splatnosti. Nová lhůta splatnosti běží ode dne vystavení nové faktury.

5.11. Objednatel neposkytuje Poskytovateli na cenu předmětu Plnění jakékoliv zálohy.

5.12. Poskytovatel není oprávněn započíst jakékoliv pohledávky proti nárokům Objednatele. Pohledávky a nároky Poskytovatele vzniklé v souvislosti se Smlouvou nesmějí být postoupeny třetím osobám, zastaveny, nebo s nimi jinak disponováno. Jakýkoliv právní úkon učiněný Poskytovatelem v rozporu s tímto ustanovením Smlouvy bude považován za příčící se dobrým mravům.

6. PŘEDÁVÁNÍ A PŘEVZETÍ PLNĚNÍ

6.1. Jednotlivé dílčí části Fáze 1 – odpovídající platebním milníkům dle odst. 5.6 Smlouvy odrážka první budou Poskytovatelem předávány a Objednatelem převzaty postupně na základě předávacích protokolů v případě HW/SW a v případě zbývajících aktivit na základě dále popsaného akceptačního řízení s tím, že nejpozději 7 dní před termínem ukončení této fáze dle odst. 4.1. Smlouvy Poskytovatel předá Objednateli poslední výstupy z Fáze 1:

6.1.1. Účelem akceptačního řízení je ověřit, zda předaná dokumentace a příslušná část SKB odpovídá schváleným funkčním a technickým specifikacím a všem Objednatelem požadovaným parametrům (výkonnostním, provozním, bezpečnostní apod.), zejména technické specifikaci uvedené v Příloze č. 1 Smlouvy a cílovému konceptu pro tuto aktivitu. V rámci akceptačního řízení se bude předaná část SKB ověřovat a testovat podle vzájemně odsouhlasených testovacích plánů, které vypracuje Poskytovatel, resp. odsouhlasených akceptačních kritérií, které navrhne Poskytovatel jakožto součást výstupů Fáze 0.

6.1.2. Poskytovatel vyzve Objednatele k zahájení akceptačního řízení pro příslušné plnění dle Fáze 1 a předá takové plnění Objednateli na základě předávacího protokolu postupně, jakmile jej bude mít dokončeno, avšak poslední výstupy nejpozději 7 dní před termínem ukončení této fáze Smlouvy. Současně platí, že akceptační řízení může probíhat nejvýše pro 3 dílčí části (aktivity) Fáze 1 souběžně.

6.1.3. Řízení o akceptaci příslušné aktivity dle Fáze 1 je zahájeno dnem skutečného předání takového plnění a je ukončeno podpisem příslušného akceptačního protokolu Objednatelem (dále jen „***Akceptační protokol***"), který bude obsahovat minimálně:

- popis části Plnění, které bylo předmětem akceptace;
- záznam průběhu akceptačního řízení;
- seznam akceptačních testů se záznamem jejich výsledků;
- seznam zjištěných vad s jejich klasifikací dle kategorií;
- výsledek akceptačního řízení.

S posledním výstupem dle Fáze 1 bude vyhotoven rovněž konečný akceptační protokol pro celou Fázi 1, ve kterém bude minimálně popis Plnění, seznam zjištěných a dosud neodstraněných vad s jejich klasifikací a výsledek konečného akceptačního řízení pro Fázi 1.

6.1.4. Není-li výslovně ujednáno jinak, akceptační řízení za každou aktivitu dle Fáze 1 (odst. 3.3.1 a 3.3.2. Smlouvy) lze zahájit pouze na základě předání všech požadovaných plnění pro příslušnou část Fáze 1 dle Smlouvy. Objednatel provede oponentní řízení převzatého plnění a nejméně 3 dny před ukončením akceptačního řízení, které se koná v dohodnutém termínu, sdělí Poskytovateli výhrady k předanému plnění s vyznačením jejich závažností. V akceptačním řízení budou projednány výhrady Objednatele a stanovena výsledná závažnost připomínek vad a nedodělků, včetně termínů jejich odstranění, přičemž Objednatel vezme do úvahy stanovisko Poskytovatele. Výsledky tohoto řízení

budou uvedeny do Akceptačního protokolu.

6.1.5. Kategorizace vad předávaného plnění dle Smlouvy při akceptačním řízení, není-li ve výstupech Fáze 0 či Fáze 1 stanoveno jinak:

- Vada kategorie A

  Popis vady: Vážné vady s nejvyšší prioritou, které mají kritický dopad do funkčnosti SKB nebo jeho části a dále vady, které znemožňují užívání SKB nebo jeho části Objednatelem nebo způsobují vážné provozní problémy.

- Vada kategorie B

  Popis vady: Vada, která svým charakterem nespadá do kategorie A. Znamená vážné vady způsobující zhoršení výkonnosti a funkčnosti SKB nebo jeho části. SKB nebo jeho část má omezení nebo je částečně nefunkční. Jedná se o odstranitelné vady, které způsobují problémy při užívání a provozování SKB nebo jeho části Objednatelem, ale umožňují provoz.

- Vada kategorie C

  Popis vady: Vada, která svým charakterem nespadá do kategorie A nebo kategorie B. Znamená snadno odstranitelné vady s minimálním dopadem na funkcionality či funkčnost SKB nebo jeho části.

6.1.6. Výsledkem akceptačních řízení příslušné aktivity dle Fáze 1 nebo konečné akceptace celé Fáze 1 mohou být dva stavy:

6.1.6.1. **Akceptováno**. V případě, že Objednatel v průběhu akceptačního řízení nenalezne v předaném plnění dle Smlouvy žádné vady ani nedodělky (dle kategorizace vad stanovené Smlouvou, resp. výstupy Fáze 0), nebo budou v průběhu akceptačního řízení shledány v předaném plnění Objednatelem akceptovatelné vady nebo nedodělky kategorie C, avšak přes uvedené bude předvedena způsobilost Plnění sloužit svému účelu, uvede Objednatel do Akceptačního protokolu, že předané plnění bylo akceptováno a akceptační protokol potvrdí svým podpisem. V případě vad nebo nedodělků kategorie A nebo B nebude Objednatel plnění ve Fázi 1 akceptovat, nedohodnou-li se Smluvní strany jinak. Podpis Akceptačního protokolu Objednatelem s výsledkem „Akceptováno" nezbavuje Poskytovatele povinnosti odstranit případné vady a nedodělky (tj. výhrady Objednatele) uvedené v příslušném Akceptačním protokolu, a to ve lhůtách v akceptačním protokolu uvedených (nedohodnou-li se Smluvní strany jinak, resp. nebude-li ve výstupech Fáze 0

stanoveno jinak, maximální lhůta na odstranění jakékoliv vady/nedodělku kategorie C nepřesáhne 15 dnů; vše od doručení Akceptačního protokolu se stavem „Akceptováno" v listinné či elektronické podobě Poskytovateli). Po odstranění všech případných vad a nedodělků podepíší Smluvní strany doklad prokazující odstranění všech případných vad a nedodělků.

6.1.6.2. **Neakceptováno.** V případě, že budou v průběhu akceptačního řízení v předaném plnění dle Smlouvy Objednatelem shledány zásadní vady a nedodělky a nebude předvedena způsobilost Plnění sloužit svému účelu, není předané plnění akceptováno a není rovněž považováno za poskytnuté v souladu se Smlouvou. V Akceptačním protokolu bude Objednatelem uvedeno, že předané plnění nebylo akceptováno, včetně popisu zjištěných vad/nedostatků a Objednatel doručí Akceptační protokol Poskytovateli, který napraví tyto vady/nedostatky a předloží plnění k nové akceptaci. Tento proces se bude opakovat, dokud nebude možné ze strany Objednatele v Akceptačním protokolu zaznamenat výsledek „**Akceptováno**", a to v lhůtě dle čl. 4. odst. 4.1. Smlouvy.

6.1.7. Kategorizaci vad předávaného plnění ve smyslu odst. 6.1.5 Smlouvy stanovuje při akceptačním řízení výhradně Objednatel. V případě změny, částečného řešení nebo vyřešení vady Objednatel může kategorii vady změnit dle závažnosti jejích dopadů.

6.1.8. Předání/převzetí příslušné aktivity dle Fáze 1 je možné pouze na základě akceptačního řízení s výsledkem „Akceptováno", přičemž podpis příslušného Akceptačního protokolu Objednatelem pro příslušná dokončená plnění Fáze 1 je podmínkou pro vznik oprávnění Poskytovatele vystavit Fakturu za poskytnutí části Plnění odpovídající příslušné aktivitě dle Fáze 1, která představuje platební milník (s výjimkou platebních milníků pro HW/SW, u kterých postačuje předávací protokol bez akceptačního řízení). Tato skutečnost nezbavuje Poskytovatele jeho povinnosti odstranit případné vady zjištěné v rámci akceptačního řízení způsobem uvedeným v odst. 6.1.6.1 Smlouvy.

6.2. Nebude-li stanoveno jinak, Služby podpory v rámci Fáze 2 budou Objednatelem přebírány na základě akceptace v rámci akceptačních schůzek, které se budou konat na základě výzvy Poskytovatele. Poskytovatel je povinen předat Objednateli doklady prokazující skutečný rozsah a kvalitu poskytovaného plnění. Před akceptací bude Objednatelem ověřeno, zda plnění bylo dodáno řádně dle příslušných ustanovení Smlouvy a pokud ano, je Objednatel povinen podepsat příslušný Akceptační protokol, jehož přílohou budou příslušné doklady o poskytovaném plnění.

6.3. Proces zadávání a akceptace části Fáze 2 odpovídající Službám rozvoje.

6.3.1. Objednatel je oprávněn čerpat kapacity Poskytovatele na poskytování Služeb rozvoje v člověkodnech (MD), a to podle potřeb Objednatele na základě objednávek. Objednatel je oprávněn v rámci objednávky a požadavků na Služby rozvoje, a to zejména u větších/rozsáhlejších požadavků dle vlastního uvážení Objednatele, požadovat před zahájením poskytování takových Služeb rozvoje, předložení rámcové analýzy Poskytovatele týkající se příslušné objednávky a požadavků na Služby rozvoje. V takovém případě je Poskytovatel povinen do 10 dní od doručení požadavku Objednatele zpracovat na vlastní náklady a předat Objednateli rámcovou analýzu příslušného požadavku Objednatele na Služby rozvoje obsahující mj. rekapitulaci a analýzu požadavku Objednatele, koncepční návrh jeho řešení, včetně možných alternativ, kalkulaci pracnosti realizace takového požadavku Objednatele a předpokládaný harmonogram realizace takového požadavku. Objednatel je oprávněn ve lhůtě 5 dnů od doručení příslušné rámcové analýzy písemně předložit Poskytovateli své připomínky. V takovém případě je Poskytovatel povinen upravit příslušnou rámcovou analýzu v souladu s připomínkami Objednatele (zejména pokud nesplňují požadavky na ně stanovené Objednatelem) a předá Objednateli nejpozději do 5 dní po doručení připomínek Objednatele konečnou verzi příslušné rámcové analýzy. Poskytování příslušných služeb, na které si Objednatel vyžádal předložení rámcové analýzy, je Poskytovatel oprávněn zahájit pouze v případě, že Objednatel schválí příslušnou rámcovou analýzu Poskytovatele, případně jím upravenou na základě připomínek Objednatele, přičemž Objednatelem schválené podmínky v rámcové analýze jsou pro Poskytovatele závazné. Před provedením či potvrzením objednávky je Objednatel také oprávněn provést vlastní průzkum trhu ve vztahu ke konkrétně požadovanému plnění (Službám rozvoje), a to ve vazbě na ověření adekvátnosti a výhodnosti podmínek provedení Služeb rozvoje Poskytovatelem.

6.3.2. Příslušné plnění části Fáze 2 odpovídající Službám rozvoje dle Smlouvy bude Objednatelem přebíráno na základě akceptace v rámci akceptačních schůzek. Objednatel musí být ke schůzce písemně pozván nejpozději do 3 pracovních dnů před termínem příslušné akceptační schůzky s tím, že nejpozději v této lhůtě je Poskytovatel rovněž povinen předat Objednateli doklady Poskytovatele prokazující skutečný rozsah a kvalitu poskytovaného plnění, včetně počtu odpracovaných člověkohodin.

6.3.3. Před akceptací bude Objednatelem ověřeno, zda plnění příslušné části Fáze 2 odpovídající Službám rozvoje bylo dodáno řádně dle příslušných ustanovení Smlouvy a příslušných objednávek a pokud ano, je Objednatel povinen podepsat

příslušný Akceptační protokol, jehož přílohou budou příslušné doklady o poskytovaném plnění.

7. DALŠÍ PRÁVA A POVINNOSTI SMLUVNÍCH STRAN

7.1. Poskytovatel je povinen:

7.1.1 poskytovat řádně a včas Plnění podle Smlouvy bez faktických a právních vad;

7.1.2 postupovat při Plnění předmětu Smlouvy s odbornou péčí, podle nejlepších znalostí a schopností, sledovat a chránit oprávněné zájmy Objednatele a postupovat v souladu s jeho pokyny a interními předpisy souvisejícími s předmětem plnění Smlouvy (či jeho dílčí části), které Objednatel Poskytovateli poskytne, nebo s pokyny jím pověřených osob;

7.1.3 bez zbytečného odkladu oznámit Objednateli veškeré skutečnosti, které mohou mít vliv na povahu nebo na podmínky poskytování plnění dle Smlouvy. Zejména je povinen neprodleně písemně oznámit Objednateli změny svého majetkoprávního postavení, jako je např. přeměna společnosti, vstup do likvidace, úpadek či prohlášení konkurzu;

7.1.4 informovat bezodkladně Objednatele o jakýchkoliv zjištěných překážkách plnění, byť by za ně Poskytovatel neodpovídal, o vznesených požadavcích orgánů státního dozoru a o uplatněných nárocích třetích osob, které by mohly plnění dle Smlouvy ovlivnit;

7.1.5 poskytnout Objednateli veškerou nezbytnou součinnost k naplnění účelu Smlouvy;

7.1.6 na žádost Objednatele spolupracovat či poskytnout součinnost dalším dodavatelům Objednatele; zejména je Poskytovatel povinen poskytovat nezbytnou součinnost dodavateli, který bude dodávat a implementovat skener zranitelností a hardeningové politiky, log management a ochranu koncových stanic v prostředí Objednatele;

7.1.7 provádět svoje činnosti tak, aby nebyl v nadbytečném rozsahu omezen provoz dotčených pracovišť Objednatele;

7.1.8 dodržovat provozní řád v místě plnění a provádět svoje činnosti tak, aby nebyl v nadbytečném rozsahu omezen provoz na pracovištích Objednatele. Poskytovatel zajistí, aby všechny osoby, které se na jeho straně podílí na plnění předmětu Smlouvy, a které budou přítomny v prostorách Objednatele,

dodržovaly všechny bezpečnostní a provozní předpisy tak, jak s nimi byly seznámeny Objednatelem;

7.1.9 informovat Objednatele na jeho žádost o průběhu plnění předmětu Smlouvy a akceptovat jeho pokyny a připomínky k plnění předmětu Smlouvy;

7.1.10 použít veškeré podklady předané mu Objednatelem pouze pro účely Smlouvy a zabezpečit jejich řádné vrácení Objednateli, bude-li to objektivně možné vzhledem k jejich povaze a způsobu použití;

7.1.11 Poskytovatel je povinen uchovávat veškerou dokumentaci související s realizací plnění dle Smlouvy včetně účetních dokladů v souladu s příslušnými Obecnými pravidly IROP minimálně do konce roku 2035. Pokud je v právních předpisech stanovena lhůta delší, musí ji Poskytovatel použít;

7.1.12 Poskytovatel je povinen v souladu s příslušnými Obecnými pravidly IROP minimálně do konce roku 2035 poskytovat požadované informace a dokumentaci související s realizací plnění dle Smlouvy zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci plnění dle Smlouvy v rámci projektu kofinancovaného z IROP a poskytnout jim při provádění kontroly součinnost.

7.2. Objednatel se zavazuje poskytnout Poskytovateli součinnost potřebnou k řádné realizaci předmětu Smlouvy, kterou je po něm Poskytovatel jako osoba, která disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci předmětu plnění Smlouvy, oprávněna požadovat.

7.3. Objednatel je v souvislosti s plněním předmětu Smlouvy oprávněn zejména udělovat Poskytovateli závazné pokyny pro výkon všech činností, ke kterým se Poskytovatel na základě Smlouvy zavázal; tyto pokyny jsou závazné, není tím však dotčena odpovědnost Poskytovatele za včasné upozornění Objednatele na jejich nevhodnou povahu.

7.4. Objednatel má právo přesvědčit se kdykoliv v průběhu realizace plnění Smlouvy o stavu realizace plnění a Poskytovatel mu k tomuto musí vytvořit přiměřené podmínky, případné náklady nese Poskytovatel.

7.5. Pokud se Smluvní strany nedohodnou jinak, součinnost zaměstnanců Objednatele dle Smlouvy bude poskytována pouze v pracovní době (od 7:00 do 15:30). Případné další požadavky na součinnost a podmínky součinnosti budou upraveny v příslušném cílovém konceptu.

7.6. Objednatel požaduje, aby Poskytovatel a jeho případní poddodavatelé realizovali předmět Smlouvy v souladu s úmluvami Mezinárodní organizace práce (ILO) přijatými Českou republikou a právními předpisy. Poskytovatel a jeho případní poddodavatelé se zavazují dodržovat minimálně následující základní pracovní standardy:

7.6.1. Úmluva č. 100 o stejném odměňování pracujících mužů a žen za práci stejné hodnoty,
7.6.2. Úmluva č. 111 o diskriminaci (zaměstnání a povolání),
7.6.3. Úmluva č. 138 o nejnižším věku pro vstup do zaměstnání,
7.6.4. Úmluva č. 155 o bezpečnosti a zdraví pracovníků a o pracovním prostředí.

7.7. Poskytovatel a jeho případní poddodavatelé jsou povinni dodržovat rovněž povinnosti týkající se základních lidských práv, včetně dodržování Všeobecné deklarace lidských práv a evropské Úmluvy o ochraně lidských práv a základních svobod.

7.8. Poskytovatel a jeho případní poddodavatelé jsou odpovědní za zajištění, aby všichni zaměstnanci pracující při realizaci předmětu Smlouvy měli oprávnění k výkonu práce v České republice dle zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a že jejich pracovněprávní vztah bude v souladu se zákonem č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, a prováděcími právními předpisy.

7.9. Poskytovatel a jeho případní poddodavatelé jsou povinni zajistit rovnost a spravedlivé a důstojné zacházení se všemi svými zaměstnanci, včetně spravedlivého a rovného odměňování za práci.

7.10. V případě, že Poskytovatel nebo jeho případní poddodavatelé poruší některou z výše uvedených povinností týkajících se dodržování výše uvedených základních pracovních standardů, mezinárodních úmluv a právních předpisů týkajících se zaměstnanců, je Poskytovatel či jeho poddodavatel povinen tyto nedostatky bezodkladně napravit a dokončit realizaci předmětu Smlouvy v souladu s těmito základními pracovními standardy, mezinárodními úmluvami a právními předpisy. Veškeré náklady vzniklé Poskytovateli či jeho poddodavateli a související s dodržováním povinností definovaných v tomto odstavci Smlouvy nese Poskytovatel, resp. jeho poddodavatel.

7.11. Objednatel je v přiměřené míře oprávněn v průběhu realizace předmětu Smlouvy kontrolovat dodržování výše uvedených základních pracovních standardů, mezinárodních úmluv a právních předpisů.

Sankce vůči Rusku a Bělorusku

7.12. Poskytovatel odpovídá za to, že platby poskytované Objednatelem dle této Smlouvy nebudou přímo nebo nepřímo ani jen zčásti poskytnuty osobám, vůči kterým platí tzv.

individuální finanční sankce ve smyslu čl. 2 odst. 2 Nařízení Rady (EU) č. 208/2014 ze dne 5. 3. 2014 o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině a Nařízení Rady (ES) č. 765/2006 ze dne 18. 5. 2006 o omezujících opatřeních vůči prezidentu Lukašenkovi a některým představitelům Běloruska a které jsou uvedeny na tzv. sankčních seznamech (dle příloh č. 1 obou nařízení); bude-li kterékoliv z nařízení v budoucnu nahrazeno jinou legislativou obdobného významu, uvedená povinnost se uplatní obdobně.

7.13. Poskytovatel odpovídá za to, že po dobu trvání Smlouvy nejsou naplněny podmínky uvedené v nařízení Rady (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, tedy zejména, že Poskytovatel není:

- ruským státním příslušníkem, fyzickou nebo právnickou osobou se sídlem v Rusku,
- právnickou osobou, která je z více než 50 % přímo či nepřímo vlastněna některou z osob dle předešlé odrážky, nebo
- fyzickou nebo právnickou osobou, která jedná jménem nebo na pokyn některé z osob uvedených v předešlých odrážkách.

Poskytovatel odpovídá za to, že po dobu trvání Smlouvy žádná z výše uvedených podmínek není naplněna ani u jeho poddodavatele (nebo jiné osoby prokazující za Poskytovatele kvalifikaci), který se bude na plnění této Smlouvy podílet z více jak 10 % hodnoty Plnění.

7.14. Poskytovatel je povinen Objednatele bezodkladně informovat o jakýchkoliv skutečnostech, které mohou mít vliv na odpovědnost Poskytovatele dle odst. 7.12 nebo 7.13. tohoto článku Smlouvy. Poskytovatel je současně povinen kdykoliv poskytnout Objednateli bezodkladnou součinnost pro případné ověření pravdivosti informací dle odst. 7.12. nebo 7.13. tohoto článku Smlouvy.

7.15. Dojde-li k porušení pravidel dle odst. 7.12. nebo 7.13. tohoto článku Smlouvy, je Objednatel oprávněn odstoupit od této Smlouvy; odstoupení se však nedotýká povinností Poskytovatele vyplývajících ze záruky za jakost, odpovědnosti za vady, povinnosti zaplatit smluvní pokutu, povinnosti nahradit škodu a povinnosti zachovat důvěrnost informací souvisejících s plněním dle této Smlouvy.

7.16. Dojde-li k porušení pravidel dle odst. 7.12. nebo 7.13. tohoto článku Smlouvy, je Poskytovatel povinen zaplatit Objednateli smluvní pokutu ve výši 250.000 Kč, a to za každý jednotlivý případ porušení.

8. PODDODAVATELÉ, REALIZAČNÍ TÝM, OPRÁVNĚNÉ OSOBY

8.1. Poddodavatelé

8.1.1 Poskytovatel se zavazuje plnění předmětu Smlouvy provést sám, nebo s využitím poddodavatelů, uvedených spolu s rozsahem jejich plnění v příloze č. 2 Smlouvy. Poskytovatel je povinen písemně informovat Objednatele o všech svých poddodavatelích (včetně jejich identifikačních a kontaktních údajů a o tom, které služby pro něj v rámci předmětu plnění každý se poddodavatelů poskytuje) a o jejich změně, a to ve smyslu ust. § 105 odst. 3 ZZVZ; Poskytovatel je povinen své poddodavatele smluvně zavázat tak, aby plnili veškeré povinnosti Poskytovatele uvedené v této smlouvě, ve stejném rozsahu jako je zavázán sám Poskytovatel. Poskytovatel je povinen kdykoliv na vyžádání Objednatele předložit smlouvu uzavřenou mezi ním a poddodavatelem, ze které vyplývá tento závazek.

8.1.2 Poskytovatel je oprávněn změnit poddodavatele, pomocí něhož prokázal část splnění kvalifikace v rámci zadávacího řízení Veřejné zakázky, a/nebo jehož zkušenosti / certifikace byly předmětem hodnocení v rámci hodnocení nabídek, jen s předchozím písemným souhlasem Objednatele, přičemž nový poddodavatel musí disponovat minimálně stejnou kvalifikací a zkušeností / certifikací pro účely hodnocení, které původní poddodavatel prokázal za Poskytovatele.

8.1.3 Zadání provedení části plnění dle Smlouvy poddodavateli Poskytovatelem nezbavuje Poskytovatele jeho výlučné odpovědnosti za řádné provedení plnění dle Smlouvy vůči Objednateli. Poskytovatel odpovídá Objednateli za plnění předmětu Smlouvy, které svěřil poddodavateli, ve stejném rozsahu, jako by jej poskytoval sám.

8.2. Realizační tým

8.2.1 Poskytovatel určuje k plnění předmětu Smlouvy realizační tým. Jmenné složení realizačního týmu je uvedeno v příloze č. 3 Smlouvy (dále jen „***Realizační tým***"). Poskytovatel se zavazuje zachovávat po celou dobu plnění předmětu Smlouvy profesionální složení Realizačního týmu v souladu s požadavky stanovenými ve Smlouvě.

8.2.2 Poskytovatel se zavazuje zabezpečovat plnění předmětu Smlouvy prostřednictvím osob, jejichž prostřednictvím prokázal v rámci zadávacího řízení na Veřejnou zakázku splnění kvalifikačních požadavků (technické kvalifikace) a které využil pro účely hodnocení své nabídky v zadávacím řízení. V případě změny těchto osob (členů Realizačního týmu) je Poskytovatel povinen vyžádat si předchozí písemný souhlas Objednatele, tento souhlas je oprávněna vydat

oprávněná osoba Objednatele ve věcech smluvních. Nová osoba Poskytovatele musí splňovat příslušné požadavky na kvalifikaci stanovené v Zadávací dokumentaci, resp. mít alespoň takové zkušenosti a certifikace, které byly relevantní pro účely hodnocení nabídek dle kritérií hodnocení „Kvalifikace (certifikace) realizačního týmu" a „Zkušenosti vybraných členů realizačního týmu", což je Poskytovatel povinen Objednateli doložit odpovídajícími dokumenty.

8.2.3 Objednatel si vyhrazuje právo na odmítnutí významných změn ve složení Realizačního týmu v době plnění Smlouvy. Současně si Objednatel vyhrazuje právo požádat o výměnu člena Realizačního týmu pro opakovanou nespokojenost s kvalitou jím odváděné práce nebo pro nedostatečnou komunikaci s Objednatelem. Veškeré případné náklady související s výměnou člena Realizačního týmu nese výlučně Poskytovatel.

8.3. Oprávněné osoby

8.3.1 Každá ze Smluvních stran dále jmenuje oprávněné osoby, které budou vystupovat jako zástupci Smluvních stran. Oprávněné osoby zastupují Smluvní stranu ve smluvních a technických záležitostech souvisejících s plněním předmětu Smlouvy, zejména podávají a přijímají informace o průběhu plnění Smlouvy a dále:

- osoby oprávněné ve věcech smluvních jsou oprávněny vést s druhou Smluvní stranou jednání obchodního charakteru, jednat v rámci akceptačních procedur při předávání a převzetí Plnění dle čl. 6 Smlouvy, zejména podepisovat příslušné akceptační či jiné protokoly dle Smlouvy.
- osoby oprávněné ve věcech technických jsou oprávněny vést jednání technického charakteru, poskytovat stanoviska v technických otázkách a jednat jménem Smluvních stran v rámci reklamace vad a při uplatňování záruky podle čl. 10 Smlouvy.

8.3.2 Oprávněné osoby budou oprávněny činit rozhodnutí závazná pro Smluvní strany ve vztahu ke Smlouvě v rámci své pravomoci. Oprávněné osoby, nejsou-li statutárními orgány, však nejsou oprávněny provádět změny ani zrušení Smlouvy, nebude-li jim udělena speciální plná moc.

8.3.3 Oprávněnými osobami za Objednatele jsou:

i) ve věcech smluvních: [redacted]

ii) ve věcech technických: [redacted]

8.3.4 Oprávněnými osobami za Poskytovatele jsou:

(i) ve věcech smluvních: [redacted]

(ii) ve věcech technických: [redacted]

8.3.5 Každá ze Smluvních stran má právo změnit jí jmenované oprávněné osoby, musí však o každé změně vyrozumět písemně druhou Smluvní stranu. Změna oprávněných osob je vůči druhé Smluvní straně účinná okamžikem, kdy o ní byla písemně vyrozuměna.

9. VLASTNICKÉ PRÁVO, NEBEZPEČÍ ŠKODY NA VĚCI A PRÁVO UŽITÍ

9.1. Poskytovatel prohlašuje, že vlastnické právo a nebezpečí škody na věci ke všem hmotným součástem plnění předmětu Smlouvy předaným Poskytovatelem Objednateli v souvislosti s plněním předmětu Smlouvy přechází na Objednatele dnem jejich předání Objednateli.

9.2. Vzhledem k tomu, že součástí Plnění dle Smlouvy je i plnění, které může naplňovat znaky autorského díla ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „**AZ**"), je k těmto součástem Plnění poskytována licence za podmínek sjednaných dále v tomto článku Smlouvy.

9.2.1 Objednatel je oprávněn veškeré součásti Plnění Poskytovatele považované za autorské dílo ve smyslu AZ (dále jen „***Autorské dílo***") užívat dle níže uvedených podmínek.

9.2.2 Objednatel je oprávněn Autorské dílo užívat dle níže uvedených licenčních podmínek (dále jen „***Licence***"), a to od okamžiku účinnosti poskytnutí Licence, přičemž Poskytovatel poskytuje Objednateli Licenci s účinností, která nastává okamžikem předání Plnění či jeho části, jehož je Autorské dílo součástí.

9.2.3 Licence je udělena jako nevýhradní, neomezeně přenositelná k užití Autorského díla Objednatelem k jakémukoliv účelu a v rozsahu, v jakém uzná za nezbytné, vhodné či přiměřené. Pro vyloučení všech pochybností to znamená, že:

- Licence je udělena jako neodvolatelná;
- Licence je dále udělena na dobu určitou, a to po celou dobu trvání majetkových práv autorských k Autorskému dílu, bez omezení územního rozsahu;
- jde-li o licenci k SW, je SW dodán jako opakovaně aktivovatelný, bez nutnosti jakékoli další úhrady;

- jde-li o licenci k SW, je Objednatel v případě potřeby oprávněn sám a bezplatně provádět modifikaci konfigurace SW v plném rozsahu a jsou mu zpřístupněny všechny dostupné funkcionality;
- v případě SW, který je součástí Plnění, se Licence vztahuje ve stejném rozsahu i na případné další verze tohoto SW upraveného na základě Smlouvy;
- Objednatel je bez potřeby jakéhokoliv dalšího svolení Poskytovatele oprávněn udělit třetí osobě podlicenci k užití Autorského díla nebo svoje oprávnění k jejímu užití třetí osobě postoupit;
- Licenci není Objednatel povinen využít, a to ani zčásti;
- Licence umožňující Objednateli SKB uživatelsky upravovat, pokud nebude nutné zasahovat do zdrojového kódu (tj. např. úprava formulářů, modifikace dle konkrétní činnosti/procesu apod.)

9.2.4 Současně Poskytovatel uděluje Objednateli souhlas ode dne účinnosti poskytnuté Licence dle Smlouvy provádět jakékoliv modifikace, úpravy, změny Autorského díla a dle svého uvážení do něj zasahovat, zapracovávat jej do dalších autorských děl, zařazovat jej do děl souborných či do databází apod., a to i prostřednictvím třetích osob;

9.2.5 V souvislosti s poskytnutou Licencí je Poskytovatel povinen, s výjimkami uvedenými v odst. 9.3 Smlouvy a 9.4 Smlouvy, nejpozději ke dni ukončení akceptace Plnění či jeho části předat Objednateli zdrojový kód každé jednotlivé části Autorského díla, která je počítačovým programem, a která je Objednateli poskytována na základě Plnění dle Smlouvy jako customizované plnění, aby s ním mohl Objednatel libovolně nakládat. Pro účely této Smlouvy se customizovaným plněním rozumí veškerá řešení vč. jejich úpravy dle požadavků Objednatele. Zdrojový kód musí být spustitelný v prostředí Objednatele a zaručovat možnost ověření, že je kompletní a ve správné verzi, tzn. umožňující kompilaci, instalaci, spuštění a ověření funkcionality, a to včetně podrobné dokumentace zdrojového kódu. Zdrojový kód bude Objednateli Poskytovatelem předán na nepřepisovatelném technickém nosiči dat s viditelně označeným názvem „Zdrojový kód" a označením počítačového programu či její části a jeho verze a dne předání zdrojového kódu. O předání technického nosiče dat bude oběma Smluvními stranami sepsán a podepsán písemný předávací protokol.

9.3. Je-li součástí Plnění tzv. proprietární software (dále jen „***Proprietární software***"), u kterého Poskytovatel nemůže poskytnout Objednateli oprávnění dle odst. 9.2.1 až 9.2.5

Smlouvy nebo to po něm nelze spravedlivě požadovat, postačí, aby Objednatel nabyl k takovému software nevýhradní oprávnění užít jej jakýmkoli způsobem nejméně po dobu trvání Smlouvy, bez územního omezení a v množstevním rozsahu, který je nezbytný pro pokrytí potřeb Objednatele ke dni uzavření Smlouvy. Smluvní strany výslovně uvádějí, že součástí takového nevýhradního oprávnění není právo provádět jakékoliv modifikace, úpravy či změny Proprietárního software či dle svého uvážení do něj zasahovat, zapracovávat ho do dalších autorských děl, zařazovat ho do děl souborných či do databází apod., a to i prostřednictvím třetích osob, ani se u Proprietárního software nevyžaduje poskytnutí zdrojových kódů k takovému software.

9.4. Je-li součástí Plnění tzv. open source software, u kterého Poskytovatel nemůže poskytnout Objednateli oprávnění dle odst. 9.2.1 až 9.2.5 Smlouvy nebo dle odst. 9.3 Smlouvy nebo to po něm nelze spravedlivě požadovat, je Poskytovatel povinen zajistit, aby se jednalo o open source software, který je veřejnosti poskytován zdarma, včetně zdrojových kódů, úplné původní uživatelské, provozní a administrátorské dokumentace a práva takový software měnit a zároveň možnost užití takového software Objednatelem k účelu sjednanému Smlouvou dle podmínek smlouvy.

9.5. Udělení veškerých práv uvedených v tomto článku Smlouvy nelze ze strany Poskytovatele vypovědět a na jejich udělení nemá vliv ukončení účinnosti Smlouvy.

9.6. Poskytovatel prohlašuje, že veškeré jím dodané plnění podle Smlouvy bude prosté právních vad a zavazuje se odškodnit v plné výši Objednatele v případě, že třetí osoba úspěšně uplatní autorskoprávní nebo jiný nárok plynoucí z právní vady poskytnutého plnění dle Smlouvy. V případě, že by nárok třetí osoby vzniklý v souvislosti s plněním Poskytovatele podle Smlouvy, bez ohledu na jeho oprávněnost, vedl k dočasnému či trvalému soudnímu zákazu či omezení užívání SKB či jeho části, zavazuje se Poskytovatel zajistit náhradní řešení a minimalizovat dopady takovéto situace, a to bez dopadu na cenu plnění sjednanou podle Smlouvy, přičemž současně nebudou dotčeny ani nároky Objednatele na náhradu škody.

9.7. S nositeli chráněných práv duševního vlastnictví vzniklých v souvislosti s realizací Plnění dle Smlouvy je Poskytovatel povinen vždy smluvně zajistit možnost nakládání s těmito právy Objednatelem v rozsahu definovaném tímto článkem Smlouvy.

9.8. Poskytovatel podpisem Smlouvy výslovně prohlašuje, že odměna za veškerá oprávnění poskytnutá Objednateli dle tohoto článku Smlouvy je již zahrnuta v ceně za poskytování Plnění dle Smlouvy.

9.9. Poskytovatel je povinen Objednateli uhradit jakékoli majetkové a nemajetkové újmy, vzniklé v důsledku toho, že Objednatel nemohl předmět Plnění Smlouvy užívat řádně a

nerušeně. Jestliže se jakékoliv prohlášení Poskytovatele v tomto článku ukáže nepravdivým nebo Poskytovatel poruší jinou povinnost dle tohoto článku Smlouvy, jde o podstatné porušení Smlouvy a Poskytovatel je povinen uhradit Objednateli smluvní pokutu ve výši 50.000,- Kč za každé jednotlivé porušení povinnosti. Zaplacením smluvní pokuty není nijak dotčeno ani omezeno právo Objednatele na náhradu škody, kterou lze vymáhat vedle smluvní pokuty v plné výši.

9.10. Poskytovatel poskytne Objednateli na jeho písemnou žádost veškerou nezbytně nutnou součinnost pro změnu poskytovatele, a to před ukončením této Smlouvy nebo její části, tj. v průběhu výpovědní doby i po jejím ukončení, případně bezodkladně po obdržení písemné žádosti Objednatele tak, aby byl zajištěn bezproblémový přechod k novému poskytovateli (dále jen „***Exit plán***"). Nezbytně nutná součinnost v rámci Exit plánu bude zahrnovat zejména:

- aktivní spolupráci Poskytovatele při migraci dat při přechodu k jinému poskytovateli, vč. zajištění exportu v dohodnutém či Objednatelem určeném formátu dat,
- poskytnutí úplné a aktuální provozní dokumentace k Plnění (dokumentace musí zahrnovat kompletní elektronickou kopii veškeré dokumentace, kterou Poskytovatel vytvořil v rámci Plnění s tím, že bude aktualizována tak, aby odrážela stav k datu ukončení Plnění),
- prokazatelné odstranění dat na HW prostředcích Poskytovatele,
- poskytnutí další konzultace Objednateli a případnému novému poskytovateli (nad rámec shora uvedených povinností) spojené zejména s přípravou nového dodavatele na výkon Služeb podpory či Služeb rozvoje; konzultace budou poskytovány na základě písemného vyžádání Objednatele.

Objednatel má právo žádost o součinnost učinit kdykoliv po dobu platnosti a účinnosti této Smlouvy a Poskytovatel je povinen tuto součinnost poskytnout ještě 3 další měsíce po ukončení platnosti této Smlouvy či její části. V souvislosti s poskytnutím součinnosti v rámci Exit plánu nenáleží Poskytovateli odměna za prvních 5 člověkodní (MD), kdy tyto jsou zahrnuty v ceně Plnění. V souvislosti s poskytnutím součinnosti v rámci Exit plánu náleží Poskytovateli odměna za 6. a každý další Objednatelem odsouhlasený člověkoden součinnosti ve výši jednotkové ceny za člověkoden (MD) Služeb rozvoje. Součinnost v rámci Exit plánu bude poskytována nejvýše v rozsahu 20 člověkodní (MD).

10. ODPOVĚDNOST ZA ŠKODU, ODPOVĚDNOST ZA VADY, ZÁRUKA

10.1. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod. Smluvní strany nesou odpovědnost za škodu dle platných a účinných právních předpisů a Smlouvy. Poskytovatel odpovídá za škodu rovněž v případě, že část Plnění poskytuje prostřednictvím poddodavatele.

10.2. Žádná ze stran není odpovědná za škodu vzniklou porušením povinnosti ze Smlouvy, prokáže-li, že mu ve splnění povinnosti ze Smlouvy dočasně nebo trvale zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na jeho vůli. Překážka vzniklá ze škůdcových osobních poměrů nebo vzniklá až v době, kdy byl škůdce s plněním povinnosti ze Smlouvy v prodlení, ani překážka, kterou byl škůdce podle Smlouvy povinen překonat, ho však povinnosti k náhradě nezprostí. Smluvní strany se zavazují upozornit druhou stranu bez zbytečného odkladu na vzniklé překážky bránící řádnému plnění Smlouvy a dále se zavazují k vyvinutí maximálnímu úsilí k jejich odvrácení a překonání.

10.3. Škoda se hradí v penězích, nebo, je-li to možné nebo účelné, uvedením do předešlého stavu podle volby poškozené strany v konkrétním případě.

10.4. Poskytovatel se zavazuje, že po celou dobu účinnosti Smlouvy bude mít sjednánu pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou Poskytovatelem třetí osobě s limitem pojistného plnění minimálně 30.000.000,- Kč. Poskytovatel je povinen předložit kopii pojistné smlouvy na vyžádání Objednateli. V případě, že při činnosti prováděné Poskytovatelem dojde ke způsobení prokazatelné škody Objednateli nebo třetím osobám, která nebude kryta pojištěním sjednaným ve smyslu tohoto odst. Smlouvy, bude Poskytovatel povinen tyto škody uhradit z vlastních prostředků.

10.5. Poskytovatel přebírá závazek a odpovědnost za vady Plnění, jež bude mít Plnění (či jeho dílčí část) v době jeho předání Objednateli a dále za vady, které se na Plnění (či jeho dílčí části) vyskytnou v průběhu záruční doby. Poskytovatel v souvislosti s odpovědností za vady Plnění poskytuje Objednateli níže specifikovanou záruku.

10.6. Nevyplývá-li z příloh Smlouvy jinak, poskytovatel poskytuje Objednateli ve smyslu § 2619 OZ záruku za jakost v délce 24 měsíců na to, že předané Plnění bude mít vlastnosti stanovené Smlouvou a výstupy Fáze 0 (u části plnění odpovídající Službám podpory nebo Službám rozvoje případně i vlastnosti stanovené příslušnou objednávkou), bude bez jakýchkoliv nedodělků či vad. Záruční doba počíná běžet u části Plnění odpovídajícího Fázi 1 ode dne konečné akceptace Fáze 1 Objednatelem (tj. po dokončení kompletní Fáze 1), u části Fáze 2 odpovídající Službám rozvoje vždy ode dne předání a převzetí příslušného plnění.

10.7. Záruční doba neběží po dobu, po kterou Objednatel nemůže užívat Plnění či jeho část pro vady, za které odpovídá Poskytovatel. Veškeré činnosti nutné či související s vyřízením reklamací vad činí Poskytovatel sám na své náklady v součinnosti s Objednatelem a v jeho provozní době tak, aby svými činnostmi neohrozil nebo neomezil činnost Objednatele.

10.8. Není-li mezi Smluvními stranami sjednáno jinak, je Poskytovatel povinen jakékoliv vady Plnění či jeho části, které vzniknou v době trvání záruky odstraňovat na své náklady, a to v souladu s režimem SLA uvedeným v příloze č. 1 – Technické specifikaci.

11. SANKČNÍ UJEDNÁNÍ

11.1. Smluvní pokuty:

i) v případě prodlení Poskytovatele s poskytnutím všech cílových konceptů dle Fáze 0 nebo kompletního plnění dle Fáze 1 v termínu dle odst. 4.1. Smlouvy je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši 50.000,- Kč, a to za každý i započatý den prodlení, čímž není dotčeno oprávnění Objednatele požadovat náhradu škody, přičemž škodu pro Objednatele představuje také ztráta či snížení dotace na předmět plnění Smlouvy;

ii) v případě jakéhokoliv nedodržení lhůt pro odstranění vad či nedodělků předaného (akceptovaného) plnění ve smyslu odst. 6.1.6.1 Smlouvy je Poskytovatel povinen Objednateli uhradit následující smluvní pokuty, není-li ve výstupech Fáze 0 stanoveno jinak:

- vada kategorie C: 1.000,- Kč za každý i započatý den prodlení a jednotlivou vadu;

iii) v případě prodlení Poskytovatele s poskytnutím části Fáze 2 odpovídající Službám rozvoje v termínu dle příslušné objednávky je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši 3.000,- Kč, a to za každý i započatý den prodlení;

iv) v případě porušení povinnosti poskytování Služeb podpory, konkrétně SLA, v požadované kvalitě, tj. dle požadavků uvedených v příloze č. 1 Smlouvy, je Poskytovatel povinen uhradit Objednateli následující smluvní pokuty:

- nedodržení lhůty odezvy u provozního incidentu kategorie kritický: 1.000,- Kč za každých i započatých 60 minut prodlení a jednotlivý incident;
- nedodržení lhůty odezvy u provozního incidentu kategorie závažný: 500,- Kč za každých i započatých 60 minut prodlení a jednotlivý incident;
- nedodržení lhůty odezvy u provozního incidentu kategorie běžný: 1.000,- Kč za každý i započatý den prodlení a jednotlivý incident;

- nedodržení lhůty odezvy u provozního incidentu kategorie minoritní: 500,- Kč za každý i započatý den prodlení a jednotlivý incident;
- nedodržení lhůty vyřešení u provozního incidentu kategorie kritický: 1.000,- Kč za každých i započatých 60 minut prodlení a jednotlivý incident;
- nedodržení lhůty vyřešení u provozního incidentu kategorie závažný: 500,- Kč za každých i započatých 60 minut prodlení a jednotlivý incident;
- nedodržení lhůty vyřešení u provozního incidentu kategorie běžný: 500,- Kč za každý i započatý den prodlení a jednotlivý incident;

v) v případě porušení povinnosti Poskytovatele udržovat v platnosti a účinnosti po celou dobu účinnosti Smlouvy pojistnou smlouvu dle odst. 10.4 Smlouvy je Poskytovatel povinen zaplatit Objednateli smluvní pokutu ve výši 100.000,- Kč za každý i započatý měsíc, v němž nebude mít uzavřenou pojistnou smlouvu se stanovenými parametry;

vi) v případě porušení povinností k ochraně důvěrných informací dle článku 12. Smlouvy je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši 200.000,- Kč za každý jednotlivý případ porušení;

vii) provede-li Poskytovatel změnu v realizačním týmu v rozporu s odst. 8.2.2 Smlouvy anebo neprovede změnu v realizačním týmu v souladu s požadavky Objednatele dle odst. 8.2.3 Smlouvy, má Objednatel právo na smluvní pokutu ve výši 100.000,- Kč za každý jednotlivý případ porušení, a to i opakovaně pokud nedojde k nápravě do 14 dnů od předchozího zjištěného porušení;

viii) provede-li Poskytovatel změnu poddodavatele v rozporu s odst. 8.1.2. Smlouvy anebo nebude-li informovat Objednatele o všech svých poddodavatelích v rozporu s odst. 8.1.1. Smlouvy anebo nezaváže-li smluvně všechny své poddodavatele, aby plnili veškeré povinnosti Poskytovatele uvedené v této Smlouvě ve stejném rozsahu jako je zavázán sám Poskytovatel v rozporu s odst. 8.1.1. Smlouvy, je Poskytovatel povinen zaplatit Objednateli smluvní pokutu ve výši 100.000,- Kč za každý jednotlivý případ porušení, a to i opakovaně pokud nedojde k nápravě do 14 dnů od předchozího zjištěného porušení;

11.2. V případě prodlení kterékoliv Smluvní strany se zaplacením peněžité částky vzniká oprávněné Smluvní straně nárok na úrok z prodlení ve výši jedné setiny procenta (0,01 %) z dlužné částky za každý i započatý den prodlení.

11.3. Zaplacením smluvní pokuty není jakkoliv dotčen nárok Objednatele na náhradu škody včetně případné újmy nemajetkové; nárok na náhradu škody je Objednatel oprávněn

uplatnit vedle smluvní pokuty v plné výši. Zaplacením smluvní pokuty není dotčeno splnění povinnosti, která je prostřednictvím smluvní pokuty utvrzena.

11.4. Smluvní pokuta i úrok z prodlení jsou splatné do třiceti (30) dnů po obdržení jejich vyúčtování.

12. OCHRANA DŮVĚRNÝCH INFORMACÍ A OCHRANA OSOBNÍCH ÚDAJŮ

12.1. Smluvní strany se dohodly, že veškeré informace, které si sdělily v rámci uzavírání a plnění Smlouvy, dále informace, které si sdělí nebo jinak vyplynou i z jejího plnění, stejně jako případné utajované informace ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (dále jen „***Zákon o ochraně utaj. Informací***") jsou důvěrné (dále jen „***Důvěrné informace***"). Smluvní strany sjednávají, že Důvěrnými informacemi jsou veškeré Objednatelem, příp. jeho dodavateli (zejména ve smyslu odst. 7.1.6.), poskytnuté informace, podklady a dokumenty, pokud nejsou běžně dostupné ve veřejných zdrojích.

12.2. Pro ochranu utajovaných informací dle Zákona o ochraně utaj. Informací je Poskytovatel povinen dodržovat tento zákon. Smluvní strany se dohodly, že Důvěrné informace nikomu neprozradí a přijmou taková opatření, která znemožní jejich přístupnost třetím osobám. Ustanovení předchozí věty se nevztahuje na případy, kdy:

12.2.1 Smluvní strany mají povinnost stanovenou právním předpisem, a/nebo

12.2.2 takové informace sdělí osobám, které mají ze zákona stanovenou povinnost mlčenlivosti, a/nebo

12.2.3 se takové informace stanou veřejně známými či dostupnými jinak než porušením povinností vyplývajících z tohoto článku Smlouvy.

12.3. Vyjma výše uvedeného se Poskytovatel zavazuje, že bude chránit a utajovat před třetími osobami skutečnosti tvořící obchodní tajemství, Důvěrné informace a jiné skutečnosti, které mu byly poskytnuty v rámci smluvního vztahu s Objednatelem.

12.4. Pokud je sdělení Důvěrných informací třetí osobě nezbytné pro plnění závazků Poskytovatele vyplývajících mu ze Smlouvy, může Poskytovatel tyto Důvěrné informace poskytnout pouze s předchozím písemným souhlasem Objednatele a za předpokladu, že tato třetí osoba před započetím činnosti písemně potvrdí svůj závazek zachování mlčenlivosti a ochrany Důvěrných informací, jinak je za toto porušení odpovědný v plném rozsahu Poskytovatel.

12.5. V případě uplatnění smluvních pokut a náhrady škody není dotčena hmotná a trestní

odpovědnost fyzických osob, které za Poskytovatele jednaly a závazek mlčenlivosti a ochrany Důvěrných informací nedodržely.

12.6. Závazek k mlčenlivosti a ochrany Důvěrnosti informací je platný bez ohledu na ukončení účinnosti Smlouvy. Poskytovatel je povinen zlikvidovat veškeré Důvěrné či chráněné informace, které se dověděl v průběhu plnění této Smlouvy poté, co bude plnění z této Smlouvy ukončeno, ať už splněním anebo jiným způsobem zániku této Smlouvy.

12.7. Vzhledem k veřejnoprávnímu charakteru Objednatele Poskytovatel výslovně prohlašuje, že je s touto skutečností obeznámen a souhlasí se zveřejněním smluvních podmínek obsažených ve Smlouvě v rozsahu a za podmínek vyplývajících z příslušných právních předpisů.

12.8. V případě, že Smluvní strany zjistí, že při plnění Smlouvy bude docházet ke zpracování osobních údajů, Smluvní strany se zavazují uzavřít smlouvu o zpracování osobních údajů, a to před zahájením samotného zpracování.

13. DOBA TRVÁNÍ SMLOUVY, MOŽNOSTI UKONČENÍ SMLOUVY

13.1. Smlouva je v případě Fáze 2 uzavřena na dobu neurčitou. Smlouva nabývá platnosti dnem jejího podpisu Objednatelem a Poskytovatelem a účinnosti dnem jejího uveřejnění prostřednictvím registru smluv ve smyslu zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) ve znění pozdějších předpisů.

13.2. Smlouva může být ukončena písemnou dohodou Smluvních stran.

13.3. Objednatel je oprávněn od Smlouvy písemně odstoupit z důvodu jejího podstatného porušení Poskytovatelem, přičemž za podstatné porušení Smlouvy se bude považovat:

a) prodlení Poskytovatele s poskytováním Plnění či jeho části ve sjednaných termínech delší než 30 dnů, pokud Poskytovatel nezjedná nápravu ani v dodatečné přiměřené lhůtě, kterou mu k tomu Objednatel poskytne v písemné výzvě ke splnění povinnosti, přičemž tato lhůta nesmí být kratší než 10 dnů od doručení takovéto výzvy;

b) další případy, o kterých tak výslovně stanoví Smlouva.

13.4. Objednatel je rovněž oprávněn odstoupit od Smlouvy v případě, že:

a) v insolvenčním řízení bude zjištěn úpadek Poskytovatele nebo insolvenční návrh bude zamítnut pro nedostatek majetku Poskytovatele v souladu se zněním zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění

pozdějších předpisů. Objednatel je rovněž oprávněn odstoupit od Smlouvy v případě, že Poskytovatel vstoupí do likvidace; nebo

b) provede-li Poskytovatel změnu v realizačním týmu v rozporu s odst. 8.2.2 Smlouvy anebo neprovede změnu v realizačním týmu v souladu s požadavky Objednatele dle odst. 8.2.3 Smlouvy, nebo

c) dojde k významné změně kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými Poskytovatelem k plnění dle této Smlouvy ve smyslu písm. n) přílohy č. 7 VKB, nebo

d) proti Poskytovateli je zahájeno trestní stíhání pro trestný čin podle zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob, ve znění pozdějších předpisů.

13.5. Poskytovatel je oprávněn od Smlouvy písemně odstoupit z důvodu jejího podstatného porušení Objednatelem, za což se považuje prodlení Objednatele s úhradou ceny za plnění předmětu dle Smlouvy o více než 30 dní, pokud Objednatel nezjedná nápravu ani do 30 dnů od doručení písemného oznámení Poskytovatele o takovém prodlení s žádostí o jeho nápravu.

13.6. Odstoupení od Smlouvy ze strany Objednatele nesmí být spojeno s uložením jakékoliv sankce k tíži Objednatele.

13.7. Smluvní strany se dále dohodly, že odstoupení od Smlouvy musí být písemné, jinak je neplatné. Odstoupení je účinné ode dne, kdy bylo doručeno druhé Smluvní straně.

13.8. Objednatel i Poskytovatel jsou oprávněni Smlouvu vypovědět, a to i bez udání důvodu, a Smlouva skončí uplynutím příslušného roku (výročí) poskytování Služeb podpory ve Fázi 2, přičemž toto oprávnění může Objednatel uplatnit až v rámci Fáze 2 dle Smlouvy; Poskytovatel je oprávněn výpověď využít nejdříve po uplynutí 5 let od zahájení Fáze 2 po dokončení (akceptaci) Fáze 1. V případě výpovědi Objednatele musí být písemná výpověď Poskytovateli doručena nejpozději 3 měsíce před uplynutím příslušného roku (výročí) poskytování Služeb podpory ve Fázi 2 dle Smlouvy, v případě výpovědi Poskytovatele musí být písemná výpověď Objednateli doručena nejpozději 6 měsíců před uplynutím příslušného roku (výročí) poskytování Služeb podpory ve Fázi 2 dle Smlouvy, jinak je výpověď neplatná, nedohodnou-li se Smluvní strany jinak.

13.9. Pro případ ukončení Smlouvy je Poskytovatel povinen poskytnout Objednateli součinnost dle ustanovení písm. j) přílohy č. 7 k VKB, v rozsahu nezbytném pro zachování kontinuity provozu.

13.10. Ukončením Smlouvy nejsou dotčena ustanovení o odpovědnosti za škodu, nároky na uplatnění smluvních pokut, ustanovení o ochraně důvěrných informací, jakož i ostatní práva a povinnosti založená Smlouvou, která mají podle zákona nebo Smlouvy trvat i po jejím zrušení.

14. SOUČINNOST A VZÁJEMNÁ KOMUNIKACE

14.1. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků. Smluvní strany jsou povinny informovat druhou Smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění Smlouvy.

14.2. Smluvní strany jsou povinny plnit své závazky vyplývající ze Smlouvy tak, aby nedocházelo k prodlení s plněním jednotlivých termínů a s prodlením splatnosti jednotlivých peněžních závazků.

14.3. Veškerá komunikace mezi smluvními stranami bude probíhat prostřednictvím oprávněných osob uvedených v čl. 8 Smlouvy nebo na jeho základě, pověřených pracovníků nebo statutárních zástupců Smluvních stran.

14.4. Veškerá oznámení, tj. jakákoliv komunikace na základě Smlouvy, bude probíhat v souladu s tímto článkem Smlouvy. Jakékoli oznámení, žádost či jiné sdělení, jež má být učiněno či dáno Smluvní straně dle Smlouvy, bude učiněno či dáno písemně. Kromě jiných způsobů komunikace dohodnutých mezi stranami se za účinné považují osobní doručování, doručování doporučenou poštou, kurýrní službou, datovou schránkou či elektronickou poštou, a to na adresy Smluvních stran uvedené v záhlaví Smlouvy, nebo na takové adresy, které si Smluvní strany vzájemně písemně oznámí.

14.5. Oznámení správně adresovaná se považují za doručená

14.5.1. dnem, o němž tak stanoví zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů (dále jen „***ZDS***"), je-li oznámení zasíláno prostřednictvím datové zprávy do datové schránky ve smyslu ZDS; nebo

14.5.2. dnem fyzického předání oznámení, je-li oznámení zasíláno prostřednictvím kurýra nebo doručováno osobně; nebo

14.5.3. dnem doručení potvrzeným na doručence, je-li oznámení zasíláno doporučenou poštou; nebo

14.5.4. dnem, kdy bude, v případě, že doručení výše uvedeným způsobem nebude z jakéhokoli důvodu možné, oznámení zasláno doporučenou poštou na adresu Smluvní strany, avšak k jeho převzetí z jakéhokoli důvodu nedojde, a to ani ve lhůtě tří (3) pracovních dnů od jeho uložení na příslušné pobočce pošty.

14.6. Informace a materiály, které obsahují osobní údaje či důvěrné informace, budou doručovány buď osobně, nebo zasílány elektronicky prostřednictvím šifrovaného distribučního kanálu určeného Objednatelem.

14.7. V případě, kdy dojde k mimořádné situaci (či bezpečnostnímu incidentu), která může mít vliv na integritu a bezpečnost informací, osobních údajů či jiných dat, které lze považovat za citlivé, jež jsou spravovány Objednatelem, je Poskytovatel povinen o nich informovat Objednatele – osoby oprávněné ve věcech technických.

15. ZÁVĚREČNÁ USTANOVENÍ

15.1. Smluvní strany si podpisem Smlouvy sjednávají (pokud Smlouva nestanoví jinak), že závazky Smlouvou založené budou vykládány výhradně podle obsahu Smlouvy, bez přihlédnutí k jakékoli skutečnosti, která nastala a/nebo byla sdělena, jednou stranou druhé straně před uzavřením Smlouvy. Ujednání odst. 1.1 Smlouvy tímto není dotčeno.

15.2. Smlouva představuje úplnou dohodu Smluvních stran o předmětu Smlouvy a všech náležitostech, které Smluvní strany měly a chtěly ve Smlouvě ujednat, a které považují za důležité pro závaznost Smlouvy. Žádný projev stran učiněný po uzavření Smlouvy nesmí být vykládán v rozporu s výslovnými ustanoveními Smlouvy a nezakládá žádný závazek žádné ze Smluvních stran. Smlouvu je možné měnit pouze písemnou dohodou Smluvních stran ve formě číslovaných dodatků Smlouvy, podepsaných oprávněnými zástupci obou Smluvních stran.

15.3. Smluvní strany se podpisem Smlouvy dohodly, že vylučují aplikaci ustanovení § 557 OZ.

15.4. Smluvní strany si nepřejí, aby nad rámec výslovných ustanovení Smlouvy byla jakákoliv práva a povinnosti dovozovány z dosavadní či budoucí praxe zavedené mezi smluvními stranami či zvyklostí zachovávaných obecně či v odvětví týkajícím se předmětu plnění Smlouvy, ledaže je ve Smlouvě výslovně sjednáno jinak.

15.5. Smluvní strany si sdělily všechny skutkové a právní okolnosti, o nichž k datu podpisu Smlouvy věděly nebo vědět musely, a které jsou relevantní ve vztahu k uzavření Smlouvy.

15.6. Pro vyloučení pochybností Poskytovatel výslovně potvrzuje, že je podnikatelem, uzavírá Smlouvu při svém podnikání, a na Smlouvu se tudíž neuplatní ustanovení § 1793 OZ.

15.7. Poskytovatel na sebe v souladu s ustanovením § 1765 odst. 2 OZ přebírá nebezpečí změny okolností. Tímto však nejsou nikterak dotčena práva Smluvních stran upravená ve Smlouvě.

15.8. Není-li stanoveno jinak, jednacím jazykem mezi Objednatelem a Poskytovatelem bude pro veškerá plnění vyplývající ze Smlouvy výhradně jazyk český, případně slovenský, a to včetně veškeré dokumentace vztahující se k předmětu Smlouvy.

15.9. Stane-li se jakékoli ustanovení Smlouvy neplatným, nezákonným nebo nevynutitelným, netýká se tato neplatnost a nevynutitelnost zbývajících ustanovení Smlouvy. Smluvní strany se tímto zavazují nahradit do 5 pracovních dnů po doručení výzvy druhé Smluvní strany jakékoli takové neplatné, nezákonné nebo nevynutitelné ustanovení ustanovením, které je platné, zákonné a vynutitelné a má stejný nebo alespoň podobný obchodní a právní význam.

15.10. Vztahy Smluvních stran Smlouvou výslovně neupravené se řídí českým právním řádem, zejména OZ. Veškeré případné spory ze Smlouvy budou v prvé řadě řešeny smírem. Pokud smíru nebude dosaženo, všechny spory ze Smlouvy a v souvislosti s ní budou řešeny věcně a místně příslušným soudem v České republice. Smluvní strany se dohodly, že místně příslušným soudem pro řešení případných sporů bude soud příslušný dle místa sídla Objednatele.

15.11. Žádné ustanovení Smlouvy nesmí být vykládáno tak, aby omezovalo oprávnění Objednatele uvedená v Zadávací dokumentaci Veřejné zakázky.

15.12. Smlouva bude uzavřena v elektronické podobě, přičemž každá Smluvní strana obdrží její elektronický originál.

15.13. Pokud Smlouva podléhá uveřejnění v registru smluv dle zákona č. zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), Smluvní strany se dohodly, že Smlouvu zašle k uveřejnění v registru smluv Objednatel. Pokud Poskytovatel považuje některé informace v této Smlouvě či jejích přílohách za své obchodní tajemství, označí tyto části nejpozději při uzavření této Smlouvy, a to včetně podrobného odůvodnění, že tyto informace naplňují veškeré znaky dle § 504 OZ. Pokud Poskytovatel řádně prokáže, že určité informace naplňují znaky obchodního tajemství ve smyslu § 504 OZ, bude Objednatel postupovat v souladu s příslušnými právními předpisy.

15.14. Nedílnou součástí Smlouvy jsou následující přílohy:

- Příloha č. 1 – Technické požadavky na předmět plnění;
- Příloha č. 2 – Seznam poddodavatelů (vč. rozsahu jejich plnění);

- Příloha č. 3 – Realizační tým;
- Příloha č. 4 – Specifikace Proprietárního software
- Příloha č. 5 – Ceník
- Příloha č. 6 – Bezpečnostní požadavky v oblasti kybernetické bezpečnosti
- Příloha č. 7 – Vzorová šablona pro cílový koncept

Smluvní strany shodně prohlašují, že si Smlouvu před jejím podpisem přečetly a že byla uzavřena po podle jejich pravé a svobodné vůle, určitě, vážně a srozumitelně, což stvrzují svými podpisy.

Ve Znojmě dne dle data el. podpisu

za Objednatele:

MUDr. Miroslav Kavka, MBA

Digitálně podepsal MUDr. Miroslav Kavka, MBA
Datum: 2024.10.10 07:15:16 +02'00'

MUDr. Miroslav Kavka, MBA, FICS
ředitel

V Praze dne dle data el. podpisu

za Poskytovatele:

Ing. Roman Kratochvíl

Digitálně podepsal Ing. Roman Kratochvíl
Datum: 2024.09.26 15:10:53 +02'00'

Ing. Roman Kratochvíl
jednatel

Technická specifikace

Popis projektu a společná kritéria

Projekt je koncipován jako ucelené řešení bezpečnosti Zadavatele, nikoliv jako dodávka technologií. Skládá se z následujících provázaných celků:

- Analýza a procesní bezpečnost – definice postupů, procesu, směrnic a dalších opatření pro naplnění bezpečnostních potřeb Zadavatele dle analýzy prostředí a požadované kompatibility s definovanými regulacemi.
- Technologie – souhrn řešení pro jednotlivé oblasti bezpečnosti, jež je tvořena konkrétními produkty s výkonnostními parametry.
- Integrace – způsob kooperace a míra provázanosti technologií tak, aby tvořily funkční celek s maximální přidanou hodnotou pro bezpečnost daného prostředí.
- Automatizace – scénáře pro abstrakci práce s technologiemi formou snadno použitelných předpřipravených akcí pro operátory bez nutnosti manuálního zásahu do konfigurace jednotlivých technologií.

V rámci analýzy bude definována bezpečnostní politika v návaznosti na potřeby zadavatele včetně kvantifikovatelných parametrů typu Recovery Time Objective (RTO), Recovery Point Objective (RPO), přičemž hodnoty těchto parametrů budou definovány v rámci projektu v části Analytické práce v oblasti bezpečnosti a dalších, které vycházejí z vyžadované metodiky. Na základě těchto parametrů musí být nastaveny a integrovány dodané technologie, včetně tvorby automatizačních scénářů tak, aby bylo možné splnit mezní limity těchto parametrů. Požadavky na kapacitu, interoperabilitu se známými technologiemi a otevřenost protokolů vychází z předběžné analýzy prostředí a zohledňuje požadavky na míru integrace a automatizace, která je očekávána v rámci projektu.

Ke každé technologii (aktivitě dle odst. 3.3.2. obchodních podmínek) bude vypracován Cílový koncept (Solution Design dokument), který popíše přesné zapojení do stávající infrastruktury, popis systémové konfigurace a provozní konfigurace, včetně integrací a veškeré interoperability s dalšími technologiemi. Nastavení konfigurace a uvedení do ostrého provozu musí být rozplánováno s ohledem na kapacitní možnosti Zadavatele, případně servisní okna daného prostředí dle dopadů na funkcionalitu. Solution Design musí být vzájemně odsouhlasen.

Konfigurační parametry dané definicí procesů a opatření musí být následně aplikovány na všechny technologie v rámci dodávky projektu a dále na existující technologie, které to dovolují (např. komunikační protokoly včetně úrovně zabezpečení, síla hesla, atp.).

DR (Disaster Recovery) plán jakožto jeden z poptávaných výstupů v rámci analytických prací definuje participaci jednotlivých technologií při obnově primárních procesů organizace a určuje formu a rychlost obnovy chodu technologie. Toto musí být reflektováno v popisu obnov technologií a jejich návazností formou detailní provozní dokumentace. Pro účely DR je dále požadováno, aby měly všechny dotčené

systémy nastaven adekvátní plán zálohování dat a systémové konfigurace, přičemž bude podle připravených scénářů docházet k pravidelným testům obnovy. Podle typu řešení lze využít formu snapshotu ve virtuálním prostředí, automatického provisioning procesu skrze automatizační scripty a šablony, případně rekonfigurace HW zařízení přes OOB (out of band) rozhraní.

Schopnost dané technologie zajistit konzistenci systémové konfigurace a procesovaných dat při zálohování a obnově je společným požadovaným kritériem pro všechny technologie v rámci dodávky.

Všechny technologie využívající certifikáty musí používat Public Key Infrastructure (PKI) definovanou v rámci projektu, přičemž je vyžadován standard TLS 1.2 či vyšší.

Nezávisle na interních mechanizmech dodávaných technologií musí být všechny napojeny na provozní monitoring skrze standardní otevřené protokoly typu SNMP, zasílat logy skrze Syslog, využívat centrální NTP a DNS službu pro sjednocení času a identifikace zařízení. Všechny technologie využívající certifikáty musí používat PKI definovanou v rámci projektu, přičemž je vyžadován standard TLS 1.2 či vyšší.

Všechny nově pořizované technologie projektu musí být pokryty podporou od výrobce po dobu minimálně 60měsíců, a to v režimu NBD 5x9; preferovány jsou trvalé (perpetual) licence, v případě, že trvalá licence není k dispozici, pak subscription s plnou funkcionalitou na dobu minimálně 60 měsíců.

V případě potřeby pořízení dodatečných licencí po dobu nezbytně nutnou pro účely implementace/testování, musí být tyto součástí nabídky dodavatele a řádně naceněny v rámci položkového rozpočtu na separátním řádku jako samostatná položka.

Bezpečnostní brány a ochrana proti zero-day hrozbám

Řešení pro ochranu uživatelského a síťového provozu. Zajištění ochrany pomocí firewall technologie v režimu active-active nebo active-passive s odpovídajícími funkcionalitami a požadavky pro ochranu provozu dle specifikace. Ochranu před zero-day malware zajišťuje dedikovaná HW appliance, jenž je s firewall řešením integrována pro kontrolu webového a e-mailového provozu. Řešení musí být homogenní, tj. všechny komponenty jsou od stejného výrobce a společně tvoří funkční celek požadovaných parametrů, včetně jednotné administrátorské konzole.

Kontrola emailového provozu je zajištěna tak, že filtrační pravidla a bezpečnostní politiky firewallu omezují a kontrolují odpovídající komunikaci, následně zpracuje emailová brána dané požadavky a provede bezpečnostní kontrolu včetně odstranění SPAM obsahu. Relevantní přílohy emailové komunikace jsou poté zaslány na dedikovanou appliance pro kontrolu zero-day hrozeb.

Firewall technologie.

1. Dodávka firewall platformy formou HW appliance, management server formou SW image do virtuálního prostředí.
2. Propustnost nejméně 12Gbps NGFW pro každou firewall HW appliance clusteru.
3. Konektivita každé firewall HW appliance minimálně 2x10G interface.
4. Minimálně 2x napájecí hot-swap zdroj na každou HW firewall appliance.
5. Součástí dodávky je možnost virtualizace firewall řešení na 10 virtuálních instancí a odpovídající licenční pokrytí management serveru pro jejich správu.
6. Licenční set musí obsahovat: IPS, URL filtering, DNS security, Antivirus, ochranu před zero-day zranitelnostmi včetně emulace souborů, a to nezávisle na dedikované Sandbox appliance.
7. Součástí dodávky je SSL VPN licence pro 200 uživatelů.
8. Hodnota BTU menší než 1650 na jednu HW firewall appliance.
9. Podpora VLAN, možnost připojení TRUNK interface.
10. Dodávka včetně příslušenství pro montáž do racku.
11. Výrobce technologie musí být hodnocen v reportu Gartner Network Firewall jako Leader nejméně ve třech kalendářních letech z posledních čtyř kalendářních let (tj. byl hodnocen jako Leader alespoň třikrát v období 2020-2023).
12. Použitá platforma musí splňovat kritéria kontinuální bezpečnosti, tj. počet zranitelností pro OS/firmware a další komponenty využité v architektuře, nesmí min. ve dvou kalendářních letech v období posledních tří kalendářních let překročit (tj. nepřekročil min. dvakrát v období 2021, 2022, 2023) průměr jedné kritické zranitelnosti/rok, a to nezávisle na konkrétní verzi OS/firmware.
13. Výrobcem musí být zajištěna na dodané FW podpora minimálně po dobu plánované životnosti 6 let od data dodání.
14. FW musí podporovat licenční model nezávislý na počtu ochraňovaných koncových systémů a uživatelů.
15. FW musí podporovat režim HA v módu Active-Active nebo Active-Standby složený ze dvou a více zařízení.
16. V obou typech HA musejí být veškeré informace o probíhajícím provozu synchronizovány, aby při výpadku jednoho z boxů nedošlo ke ztrátě informací NAT a k přerušení aktivních spojení provozu typu TCP i UDP procházejícího přes FW.
17. FW musí plně podporovat IPv4 i IPv6.

18. FW musí podporovat site-to-site VPN pomocí protokolu IPSec.
19. FW musí podporovat nativní nástroj pro odchycení provozu.
20. FW musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu.
21. FW musí podporovat identifikaci aplikací napříč všemi porty/protokoly.
22. FW musí podporovat identifikaci aplikací na nestandardních portech.
23. FW musí podporovat vytváření bezpečnostních pravidel na základě uživatelských identit.
24. FW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na koncové zařízení nebo doménový kontrolér.
25. FW management musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem.

Sandbox technologie

Sandbox appliance zpracovává dokumenty poskytnuté firewall řešením a není zapojena inline v cestě datového toku infrastruktury. Appliance musí provádět kontrolu připojených datových uložišť na přítomnost malware v obsažených souborech.

1. Minimální propustnost 1200 souborů za hodinu.
2. Licence potřebné pro kontrolu Windows systémů v počtu odpovídajícím maximálnímu počtu virtuálních instancí dané appliance musí být součástí dodávky.
3. Minimálně 2x napájecí hot-swap zdroj.
4. Všechny dokumenty musí být emulovány výhradně lokálně.
5. Hodnota BTU menší než 1650.
6. Podpora ICAP protokolu.
7. Možnost využití otevřeného API pro kontrolu zaslaných dokumentů.
8. Dodávka včetně příslušenství pro montáž do racku.

Integrace

Řešení musí podporovat dynamické seznamy objektů z komponent, které definují virtuální koncová zařízení a uživatele, nejméně z prostředí Microsoft AD a VMware tak, aby tyto objekty mohly být využity pro tvorbu bezpečnostních politik bez nutnosti manuální rekonfigurace pravidel při změně jednotlivých položek dynamického objektu.

Dále je požadována integrace na Nástroj pro zabezpečení zdravotnických zařízení, a to minimálně v rozsahu:

- Automatické aktivace IPS signatur na IoT exploity
- Automatické generování firewallové politiky na základě vlastností zařízení
- Detekce připojených zdravotnických zařízení

Výstupy pro logmanagement a další platformy řídící dohled a bezpečnostní korelace musí být ve formátu Syslog.

Automatizační procesy, jež jsou požadovány a budou součástí Solution Designu musí zahrnovat změny bezpečnostní politiky firewall formou změn bez nutnosti manuálního zásahu správce. Řešení musí být takto konfigurovatelné i přes API rozhraní. Minimální množina automatizačních postupů pro firewall:

- Změna filtračních pravidel reflektujících riziko koncového zařízení či síťového segmentu (zablokování, restrikce na administrátorský prostup, povolení do původního stavu),

- konfigurace IPS profilu,
- založení VPN prostupu či jeho zablokování,
- nastavení nového uživatele pro SSL VPN či jeho zrušení,
- schopnost záchytu síťové komunikace ve formě PCAP pro požadované rozhraní,
- odpojení síťových rozhraní či skupin rozhraní při kritickém scénáři

Implementace

Nasazení firewallu předpokládá perimetrovou ochranu infrastruktury Zadavatele včetně všech definovaných ochran uživatelského provozu, oddělení IT a OT infrastruktury, případně využití aplikačních ochran pro další segmenty v rámci interní infrastruktury, a to zejména technologií datových center.

Analytické práce v oblasti kybernetické bezpečnosti

Bezpečnostní dokumentace

Zadavatel požaduje v této části kompletní dodávku bezpečnostní politiky a bezpečnostní dokumentace. Očekává se po formální stránce plná shoda se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), včetně všech prováděcích vyhlášek, resp. s právní úpravou, která uvedený právní rámec v době plnění nahradí a zajištění shody s přílohou č. 5 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti.

Před vytvářením bezpečnostní dokumentace bude provedeno zmapování současného stavu a sběr informací o zaběhlých procesech a pravidlech nemocnice tak, aby bylo možné vytvořit harmonogram tvorby bezpečnostní dokumentace. Při tvorbě bezpečnostní dokumentace musí být brány v potaz již existující dokumenty nemocnice.

Pro všechny výstupy je požadována vysoká připravenost na novou legislativu NIS2. V případě, že v průběhu plnění smlouvy o dílo před dokončením a akceptací této aktivity bude platná a účinná nová legislativa NIS2, požaduje se plná shoda výstupů této části s novou legislativou.

Pro naplnění celé řady zákonných požadavků je nutné vytvořit bezpečnostní politiky a další bezpečnostní dokumentaci, minimálně v rozsahu požadavků (viz příloha č. 5 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti):

- Politika systému řízení bezpečnosti informací
- Politika řízení aktiv
- Politika organizační bezpečnosti
- Politika řízení dodavatelů
- Politika bezpečnosti lidských zdrojů
- Politika řízení provozu a komunikací
- Politika řízení přístupu
- Politika bezpečného chování uživatelů
- Politika zálohování a obnovy a dlouhodobého ukládání
- Politika bezpečného předávání a výměny informací
- Politika řízení technických zranitelností
- Politika bezpečného používání mobilních zařízení
- Politika akvizice, vývoje a údržby
- Politika ochrany osobních údajů
- Politika fyzické bezpečnosti
- Politika bezpečnosti komunikační sítě
- Politika ochrany před škodlivým kódem
- Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí
- Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí
- Politika bezpečného používání kryptografické ochrany
- Politika řízení změn
- Politika zvládání kybernetických bezpečnostních incidentů
- Politika řízení kontinuity činností

- Zpráva z auditu kybernetické bezpečnosti
- Zpráva z přezkoumání systému řízení bezpečnosti informací
- Metodika pro identifikaci a hodnocení aktiv a pro hodnocení rizik
- Zpráva o hodnocení aktiv a rizik
- Prohlášení o aplikovatelnosti
- Plán zvládání rizik
- Plán rozvoje bezpečnostního povědomí
- Evidence změn
- Hlášené kontaktní údaje
- Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků
- Další doporučená dokumentace (doporučí dodavatel dle best practise)

Analýza rizik

Nezbytnou součástí plnění je provedení identifikace a hodnocení aktiv a rizik v souladu s požadavky § 4 řízení aktiv a § 5 řízení rizik vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti.

Řízení kontinuity činností

Součástí dodávky je také provedení analýzy dopadů (BIA – Business Impact Analysis), na kterou navazuje tvorba plánů kontinuity (BCP) a plánů obnovy (DRP) v souladu s § 15 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (Řízení kontinuity činností).

Zavedení síťové behaviorální analýzy

Předmětem této části je systém pro analýzu síťového provozu a bezpečnostní monitoring, který okamžitě identifikuje bezpečnostní rizika a události a který splňuje požadavky uvedené níže.

Součástí dodávky je veškerý potřebný hardware, software, licence a případný drobný a spojovací materiál, včetně implementačních a dokumentačních prací. Zadavatel dodá své vlastní dva SFP+ (10 Gbit) SingleMode moduly do ethernetových switchů pro připojení hardwarového kolektoru/senzoru. Dodavatel dodá analogické dva SFP+ moduly do dodávaného hardwarového kolektoru/senzoru (protikusy), tyto jsou tedy součástí dodávky a musí být kryty stejnou zárukou a podporou jako nabízený kolektor/senzor. Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.

Jednotlivé komponenty řešení (hardware, software, licence) a jejich PN (produktové číselné označení) musí být dostupné přímo v oficiálním ceníku výrobce pro český trh. Podpora ve všech úrovních musí být zajištěna přímo jejich výrobcem, kterého může zadavatel přímo kontaktovat.

Dodávané řešení pro analýzu síťového provozu a bezpečnostní monitoring musí splňovat alespoň následující funkce a parametry:

Licenční pokrytí

Pokud jsou v nabízeném řešení zahrnuty jakékoliv licence, jejich legální používání nesmí být časově omezeno. Nabízené řešení tedy musí být plně funkční i po uplynutí doby placené podpory.

Obecné požadavky

Systém složený z hardwarových zařízení musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby, bezpečnostní rizika a anomální chování a musí o nich v reálném čase vytvářet upozornění.

Dodaný systém musí primárně analyzovat síť na základě zrcadleného síťového provozu ze SPAN portů nebo TAPů (nikoliv jen na základě statistických protokolů typu NetFlow) a zároveň bez potřeby nasazovat agenty na koncové stanice nebo další zařízení v síti.

Systém musí analyzovat obsah datových paketů v reálném čase a detekovat protokol nebo aplikaci na základě obsahu provozu prostřednictvím DPI (Deep Packet Inspection), nikoli pouze čísla portu.

Dodaný systém musí být schopen analyzovat síť také na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších, které budou využity ve specifických segmentech infrastruktury.

Systém musí být plně funkční v offline prostředí objednatele bez využití cloudového prostředí pro sběr, ukládání a zpracování dat. Veškeré konfigurace a reporting jsou k dispozici přímo v systému.

Aktualizace systému musí být možné provádět uživatelsky v offline režimu.

Systém ukládá síťové toky ve formátu, který umožní analýzu síťové komunikace na úrovni jednotlivých toků, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku.

Požadované protokoly pro ukládání aplikačních metadat z jednotlivých transakcí jsou: DHCP, DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAPS, KERBEROS, SNMP, CIFS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, NFS, ARP, SSL/TLS zapouzdření.

Je požadováno vysokorychlostní úložiště pro uchování historie datových toků na dobu minimálně 18 měsíců složené z SSD disků.

Systém musí poskytovat jednotné grafické uživatelské rozhraní pro veškerou práci uživatelů, včetně všech detekcí, analýzy síťových statistik, nastavení systému, konfiguraci alertů, reportů a dashboardů.

Systém musí být schopen vytváření profilů a skupin uživatelů pro omezení funkcionality produktu a viditelnosti uložených dat s podporou minimálně:

- granulárního nastavení přístupu k analytickým i konfiguračním/administrativním komponentám systému s definovanými úrovněmi přístupu (alespoň read, write, execute),
- granulárního nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (alespoň read, write, execute),
- vytváření vlastních filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů,
- vytváření vlastních uživatelských pohledů, reportů, dashboardů apod.

Systém musí být schopen upozorňovat uživatele prostřednictvím minimálně emailu a logu o všech identifikovaných událostech a dále o událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu.

Tyto alerty musí být systém schopen dodávat i ve strojově čitelném formátu pro vyžití v nástrojích typu SIEM a musí obsahovat minimálně kompletní informace o detekované události včetně URL odkazu na danou událost v reportovaném období do grafického rozhraní systému.

Systém musí mít možnost vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu zprávy kybernetických incidentů ideálně dle oblastí jejich vzniků (např.: doména, web, email apod.).

Je požadováno vytváření automatizovaných reportů v českém jazyce.

Architektura řešení

Pro všechny HW komponenty senzor a kolektor je požadován formát 1U nebo 2U server o velikosti 19".

Pro všechny HW komponenty senzor a kolektor je požadován duální zdroj napájení se schopností hot-swap.

Pro všechny HW komponenty senzor a kolektor je požadováno samostatné síťové rozhraní pro vzdálenou správu serveru v případě výpadku systému typu IPMI, IDRAC, ILO apod.

V síti je předpokládáno cca 2000 aktivních zařízení s průměrným denním celkovým průtokem do 2Gbps.

Je požadován 1x HW datový kolektor/sensor o celkové propustnosti minimálně 2Gbps s monitorovacím rozhraním 4x 1GE a 2x10GE.

Na zařízení je požadována dostupná historie dat minimálně 6 měsíců zpětně, uložená na rychlém úložišti typu SSD o velikosti alespoň 10TB. Požadován je minimálně RAID10 nebo RAID6 se schopností hot-swap.

Detekce bezpečnostních událostí

Dodaný systém musí identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti – minimálně:

- změna IP/MAC adresy hosta,
- duplicitní IP/MAC adresa,
- změna VLAN,
- vytvoření nové podsítě,
- připojení nového zařízení,
- použití nebo vznik nové služby,
- nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení,
- přístup nového zařízení ke službě či zařízení
- ověřování platnosti interních certifikátů pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení.

Systém musí uživateli umožnit pomocí těchto detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a na porušení těchto politik reagovat upozorněním.

Systém musí používat matematické metody samostatného učení pro analýzu síťové aktivity, vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace. Systém musí mít schopnost na základě matematického modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování, a to zejména odchylky od modelu normálního chování pro:

- odchylku od modelu pro přenos dat, toků a paketů,
- odchylku od modelu pro počet komunikačních partnerů,
- odchylku od modelu entropie na komunikačních portech,
- odchylku od modelu pro počet síťových toků a využitých síťových služeb,
- odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy).

Samostatné učení je požadováno na všech síťových zařízeních a na nich provozovaných službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 a L4 síťové vrstvy.

Systém musí být schopen detekovat neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod. Zejména musí být identifikovány tyto příznaky potenciálně škodlivého chování:

- průzkumné aktivity v síti,
- detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě,
- detekce repetitivních vzorců chování na síti,
- detekce botnetů a ovládání kompromitované stanice,
- detekce příznaků těžení kryptoměn,
- útoky hrubou silou a enumerace dat,
- rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a DNS tunely.

Systém musí být schopen identifikovat hrozby a reportovat události na základě

- detekční databáze známých hrozeb, tj. malware (trojské koně, viry, červy, rootkity, apod.), známých útoků (exploity) a zranitelností, porušení bezpečnostních pravidel a „best practices" a dalších rizik,
- reputační databáze známých škodlivých IP adres, TLS certifikátů, záznamů DNS a hostname, URL adres a hashů souborů.

Tyto databáze musí být aktualizované minimálně na hodinové bázi.

Uživatel musí být schopen importovat vlastní indikátory kompromitace.

Systém musí využívat tuto detekci pro veškerý monitorovaný provoz (na perimetru i v interní síti mezi všemi segmenty), nikoliv pouze pro omezený segment nebo podmnožinu celkové komunikace.

Databáze detekčních pravidel (signatur) musí být založena na pokročilých regulárních výrazech pro zpracování řetězců, které dokáží provádět inspekci veškeré síťové komunikace od L2 po L7. Systém musí detekovat události na základě vysokého počtu signaturních pravidel (minimálně několik desítek tisíc).

Analýza šifrované komunikace - Vedle samostatného učení musí systém používat další metody pro analýzu šifrované komunikace, minimálně TLS fingerprinting a s ní spojenou detekci známých hrozeb.

Je požadován uživatelsky přívětivý proces vytváření pravidel pro zpřesnění detekce a eliminaci falešně pozitivní detekce, a to na základě minimálně následujících parametrů:

- IP adresa,
- MAC adresa,
- hostname,
- segment sítě / podsíť,
- lokalita – ASN, země, apod.
- směr komunikace – určení klienta, nebo serveru,
- detekovaná událost – kategorie, název apod.
- použité služby, protokolu, portu,
- libovolné kombinaci výše popsaných.

Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii.

Síťová viditelnost

Systém musí být schopen okamžitého (v řádu vteřin) vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka.

Jedná se o možnost okamžitě filtrovat a vyhledávat v plné historii všech uložených dat, tj. bezpečnostních událostí, síťových toků a agregovaných síťových statistikách (tabulky a grafy), a to minimálně:

- podle parametrů IP a MAC adresa, hostname, username (identita uživatele), příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN,
- prostřednictvím full-textového vyhledávání v datech a vyhledávání na základě definice směru (zdroj, cíl) a logických výrazů and, or, not.

Systém musí pro vyhledávání poskytovat již předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení v síti a pro všechny na něm provozované služby, bez nutnosti zpracování surových dat ze síťových logů.

Systém musí být schopen filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách.

Systém musí být schopen ukládat a následně vyhledávat aplikační metadata (vždy dotaz i odpověď všech transakcí v toku) minimálně z následujících protokolů, které jsou nebo mohou být využívány ve vnitřní síti organizace: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP, HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, RDP, ARP, MS-SQL, SIP, Kerberos, SSL/TLS.

Systém umožnuje provádět uživatelsky jednoduché a okamžité vizualizace síťových prostupů mezi zařízeními a podsítěmi. Využitím uživatelského datového filtru lze vizualizační pohledy libovolně modifikovat.

Systém musí být schopen pro každé zařízení získávat, vizualizovat a v jednom grafickém pohledu zobrazovat kontextuální informace:

- jméno uživatele a další jeho parametry z doménového řadiče (MS Active Directory) včetně historie,
- hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu,
- IP geolokace,
- IP reputace, vč. údaje, jestli je IP adresa na blacklistu nebo podezřelá,
- historie použitých MAC adres a výrobce zařízení,
- operační systém a jeho historie na zařízení,
- uživatelem zadané poznámky a informace k zařízení,
- automaticky přiřazené značky/tagy zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy.

Zaznamenávání a ukládání plného provozu - je požadováno nahrávání plného síťového provozu (full packet capture) ve formátu PCAP na všech dodaných zařízeních minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6. Zaznamenávání je možno zapínat automaticky dle detekovaných událostí, nebo uživatelskou aktivací.

Integrace

Systém musí poskytovat hotové nástroje umožňující integraci se softwarem třetích stran bez použití API systému, a to minimálně:

- syslog, CEF a LEEF pro export událostí včetně plné podpory filtrů (exportování pouze požadovaných dat),
- přímé URL odkazy na libovolnou obrazovku grafického uživatelského rozhraní a filtrovaná zobrazení v grafickém uživatelském rozhraní,
- export informací o toku ve formátu IPFIX nebo podobném formátu včetně plné podpory filtrů (exportovat lze pouze požadovaná data),

- integrace se službami identity uživatelů bez nutnosti konfigurace zasílání logů do systému – minimálně Cisco ISE a Microsoft Active Directory,
- integrace s firewally, alespoň Palo Alto, Fortinet a Checkpoint, pro automatické a manuální reakce vyvolané systémem,
- integrace s nástroji pro řízení přístupu k síti minimálně Cisco ISE, pro automatickou a manuální reakci systému.

Implementace

Všechna dodavatelem instalovaná zařízení nebo komponenty musí být dodavatelem profesionálně nainstalovány a zprovozněny a po jejich nasazení řádně dokumentovány a otestovány, vč. prokázání, že tato zařízení plní všechny požadované a výkonnostní parametry. Součástí implementace je i konfigurace aktivních prvků – nastavení SPAN portů atd. Součástí dodávky je administrátorské seznámení s obsluhou u tří zaměstnanců zadavatele v rozsahu nejméně 2 dny.

Vybudování PKI

Je požadováno vybudování interní certifikační autority PKI (Public Key Infrastructure – architektura veřejných klíčů), která bude ve správě Zadavatele. Zaměstnanci se tak budou moci jednoznačně a bezpečně identifikovat například při přístupu do sítě nebo do významných aplikací.

Záměr je doplnit do infrastruktury bezpečnostní vrstvu, vybudovanou na bázi PKI. Implementace PKI by měla doplnit bezpečnostní funkce, jako jsou například zabezpečení komunikace (SSL apod.) nebo autentizace serverů vůči počítačům a uživatelům. Část PKI je určena pro vydávání uživatelských certifikátů na čipové karty a následné zavedení dvoufaktorové autentizace jako náhrady autentizace jménem/heslem.

Pro implementaci PKI je požadována technologie, která je nativně podporována v prostředí Active Directory - certifikační služba na platformě MS Windows Server.

V rámci dodávky bude v prostředí vybudována hierarchie certifikačních autorit. Vybudované certifikační autority budou podřízeny pod jedinou kořenovou CA, a to:

- autorita pro vydávání uživatelských certifikátů,
- autorita pro vydávání certifikátů serverů, počítačů a prvkům infrastruktury.

Všechny vydávající CA budou mít vydán certifikát z kořenové CA, která bude offline a nebude chráněna HW prostředky. K certifikačním autoritám bude existovat provozní i bezpečnostní dokumentace.

Provozní a bezpečnostní koncept PKI zadavatele

Požaduje se zpracování dokumentu cílového konceptu PKI v prostředí zadavatele. V rámci konceptu budou navrženy jednotlivé aspekty PKI:

- hierarchie CA,
- infrastruktura PKI,
- bezpečností perimetry a jejich separace,
- vlastnosti a parametry jednotlivých CA,
- bezpečnostní koncept PKI, role, oprávnění, ochrana aktiv,
- typy vydávaných certifikátů a vlastnosti příslušných šablon certifikátů,
- parametry certifikačních autorit (1 CA kořenová, 1 CA pro vydávání uživatelských certifikátů a 1 CA pro vydávání certifikátů pro počítače, servery, infrastrukturu),
- definice distribučních bodů CRL a certifikátu CA,
- návrh konceptu zálohování CA.

Koncept PKI bude v souladu s bezpečnostními politikami zadavatele. Podle navrženého konceptu PKI budou následně implementovány PKI subsystémy do prostředí zadavatele.

Systém pro správu privilegovaných účtů

Nasazení systému, který zajistí správu privilegovaných účtů a monitoring privilegovaných relací. Tento systém zajistí logování všech relací, logování aktivit administrátorů, možnost dohledání zadaných a vykonávaných příkazů a možnost pozastavit, uzamknout nebo terminovat relaci. Dodávané řešení pro správu privilegovaných uživatelských účtů musí splňovat alespoň následující funkce a parametry.

Licenční pokrytí

Dodávka musí poskytnout licence pro neomezený počet správců (dostupné veškeré funkce řešení) a pro minimálně 200 koncových aktiv.

Součástí licence je i řešení redundance všech komponent a taktéž geo-redundance (alespoň active-passive) s dodatečnou místní redundancí v sekundární geolokaci. Množství licencí lze v budoucnu dále rozšiřovat dle aktuálních potřeb aditivně, tj. bez nutnosti zpětného odkupu původního balíku a jeho náhrady. Zadavatel vyžaduje on-premise řešení a neumožňuje alternativu umístěnou v cloud prostředí. Součástí nabízeného řešení musí být i licence MS CAL, pokud je řešení potřebuje k naplnění jakéhokoliv z uvedených bodů v této definici.

Architektura řešení

Veškeré komponenty řešení musí splňovat nároky na vysoké zabezpečení a automaticky vynucovat tzv. hardening. Úložiště dat, kde jsou uloženy jednotlivé účty, přihlašovací údaje, nahrávky relací a auditní záznamy, je vysoce zabezpečeno dle požadavků. Řešení bude dodáno na dvou virtuálních appliance, které jsou out-of-the-box dodány jako uzavřená platforma, obsahující všechny licence na provoz řešení, existují v produktové řadě výrobce, mají produktové číslo a jsou výrobcem zabezpečeny proti hrozbám hardeningem. Update OS na vyšší verzi musí být realizován výměnou appliance. Úprava systému /instalace aplikací na úrovni operačního systému není možná. Zadavatel požaduje autonomní řízení aktualizací OS a samotného SW pomocí výrobcem dodávaných balíčků skrze administrační rozhraní dodávané výrobcem.

Řešení musí být nasazeno ve vysoké dostupnosti pro zabezpečení High Availability, minimálně v režimu Active-Passive, Disaster Recovery a zálohování řešeno tak, aby citlivá data byla stále vysoce zabezpečená a dostupná pouze vlastníkům dat. Disaster recovery a HA proces je plně automatický.

Systém musí umožňovat až 8 otevřených spojení na jednoho administrátora. Systém musí umožňovat alespoň 250 RDP paralelních spojení a 450 SSH paralelních spojení.

Řešení musí umožňovat bezpečné zálohování dat systému – zálohy musí být šifrované a přístup k zálohovaným datům je umožněn pouze pomocí zabezpečených postupů, které zajišťují integritu zálohovaných dat. Řešení musí poskytovat automatický hardening úložiště dat, který bude nezávislý na zásahu správců systémů a bude minimalizovat možnou lidskou chybu. Řešení musí být v navrhované konfiguraci stabilní a je možné ho ověřit dle odkazovaných referencí.

Řešení musí pokrývat tzv. „break glass" scénáře s postupy, jak jednat v situacích s fatálním dopadem na PAM systém. Součástí dodávky je rámcový popis pro řešení disaster recovery a break-glass scénářů, který bude detailně rozpracován při analýze.

Veškeré komponenty systému musí podporovat SNMP monitoring, tak aby bylo možné monitorovat dostupnost. Požadován je monitoring vytížení CPU, využití disků a paměti.

Řešení musí být dimenzované tak, aby uchovávalo nahrávky relací minimálně po dobu 365 dní.

Obecné požadavky

Řešení poskytuje nástroj pro správu privilegovaných účtů, řízení přístupu k těmto účtům a monitoring veškerých aktivit privilegovaných účtů. Uživatelské přístupy jsou řízeny bezpečnostní politikou, ve které má vybraný uživatel práva přístupu pouze k definovaným účtům a systémům. Účty a systémy, ke kterým nemá práva přístupu, nejsou pro uživatele viditelné.

Systém plně podporuje oddělení přístupových oprávnění. Uživatelé/skupiny uživatelů mají přístup pouze k vybraným účtům, systémům, auditním záznamům, konfiguraci atp. Řešení podporuje minimálně následující role:

- Žadatel
- Schvalovatel
- Auditor
- Administrátor systému

Řešení umožňuje víceúrovňové schvalování správcovských přístupů k cílovým systémům – přístupy lze omezit dle vybraného účtu, nebo na daný časový úsek. Schvalování přístupu lze vynutit odděleně pro přístup k přihlašovacím údajům privilegovaného účtu, nebo pro připojení na koncový systém. O nových žádostech, schválení a zamítnutí budou uživatelé upozorněni emailem, vytvořením ticketu v helpdesk systému, nebo jinou metodou schválenou v rámci Solution Design dokumentu.

Řešení zaručuje vysokou bezpečnost přenášených a uložených informací (confidentiality, integrity, availability). Uložené informace, včetně nahrávek a spravovaný přihlašovacích údajů, jsou uloženy v jedné centrální zabezpečené databázi. Dle požadavků Řešení musí umožňovat omezení práv správce systému tak, aby neměl sám přístup k uloženým přihlašovacím údajům, logům, nebo nahrávkám bez autorizace vlastníků dat. Systém musí být certifikovaný bezpečnostním standardem Common Criteria.

Správa řešení je umožněna pomocí jednotné centrální správy. Přístup k uživatelskému rozhraní je požadován přes webový portál s možností ověření přes LDAP/MS Active Directory a druhým faktorem (minimálně PKI karty, RSA ID, Radius server).

Řešení je možné spravovat a konfigurovat také pomocí Rest API, a to minimálně pro vytváření a editace uživatelů a účtů, nastavení oprávnění, system health monitoring, schvalování požadavků, autentizace, změny přihlašovacích údajů, terminace spojení atp.

Řešení musí umožňovat integraci s ticketovacími nástroji třetích stran – žádost o schválení přístupu, přístup na základě existujícího tiketu, atp.

Řešení nabízí plnou integraci s Microsoft Active Directory na úrovni informací o uživatelích, příslušnosti ke skupinám a informace o emailech. Integrace musí umožňovat mapování rolí v PAM řešení v návaznosti na skupiny v AD.

Nástroj umožňuje vynutit silnou autentizaci uživatelů pro přístup k uloženým údajům i pro bezpečné vzdálené připojení. Silnou autentizací je míněna minimálně možnost kombinace jméno/heslo + druhý faktor (RADIUS, PKI, certifikát, atp ...). Řešení umožňuje integraci s MFA nástroji třetích stran.

Řešení musí splňovat standard FIPS 140-2 a šifrovací algoritmy minimálně na úrovni AES-256 a RSA-2048. Řešení umožňuje společnostem splnit compliance požadavky pro ZKB, GDPR, PCI-DSS, SOX, HIPAA.

Řešení musí poskytovat zabezpečený přístup k veřejným webovým aplikacím pomocí SSO portálu. Pro autentizaci k SSO portálu se použije jméno+heslo a vynucení vícefaktorového ověření. Systém musí podporovat minimálně následující integrace:

- NTLM
- Basic auth
- SAML
- Uživatelské heslo

Management hesel

Řešení umožňuje vyhledávat privilegované účty v operačních systémech Windows, Unix, Linux a Mac OS / LDAP, Active Directory, databázích a síťových zařízeních a přidat je (manuálně i automaticky) do systému řízení přístupu dle bezpečnostní politiky. Dále řešení dokáže určit o jaký typ účtů se jedná (běžný uživatel vs. Administrátor/root). Vyhledávání účtů nevyužívá instalaci agentů na koncová zařízení. Systém umožňuje vyhledávání v on-premise i cloud prostředí.

Řešení umožňuje automatickou výměnu hesel a SSH klíčů privilegovaných účtů po ukončení relace (jednorázové heslo) nebo v pravidelných intervalech dle bezpečnostní politiky. Rotaci hesla/SSH klíče lze vynutit i uživatelem. Hesla a SSH klíče se vyměňují bez nutnosti využití agenta.

Řešení kontroluje v pravidelných intervalech shodu uloženého hesla v systému řízení přístupů a na cílovém bodu. V případě neshody vynutí synchronizaci nebo zašle upozornění správci.

Systém umožňuje vyhledat účty v MS Windows prostředí a jejich návaznost na další služby/aplikace (service17chedulerled tasks, IIS pool, COM+ object, ...). Při přidávání účtů na návaznosti upozorňuje nebo automaticky integruje do systému. Při vynucení změny hesla je heslo propsáno i do návazných služeb.

Systém umožňuje pravidelné vyhledávání účtů, které nejsou řešením spravovány, ale jsou používány pro přístupy na koncové systémy. Systém takové účty dokáže vyhledat, upozornit na jejich použití a případně automaticky zařadit do správy. Řešení zároveň umožňuje detekci nespravovaných účtů a automatické uložení a vynucení změny hesla.

Řešení musí umožňovat možnost úpravy systému password management tak, aby bylo možné integrovat další systémy zadavatele. Úpravy je možné provádět pomocí nástroje dodávaného výrobcem a případně úpravou konfiguračních souborů.

Řízení privilegovaných relací

Nabízené řešení musí obsahovat Privileged Session management minimálně pro RDP a SSH spojení navázaná z administrátorské stanice, bez nutnosti instalace agenta na stanici administrátora.

Správcovský přístup na cílový systém bude zprostředkován pomocí tzv. terminal/proxy serveru prostřednictvím zvoleného komunikačního protokolu, aplikace a příslušného privilegovaného účtu tak, aby koncový uživatel neměl přístup k přihlašovacím údajům. Izolace přístupu je možná až na úroveň aplikace (typu webový prohlížeč s konkrétní URL, MMC konzole s vybraným snap-in, konkrétní aplikace... např. MS SQL Management Studio, WinSCP, atp.), kdy uživatel nemá možnost přistupovat k jiným službám či aplikacím v rámci dané relace. Po ukončení aplikace se uzavře spojení celé relace. Vzdálené připojení k relaci lze navázat jak přes vlastní GUI dodaného řešení, tak i pomocí standardních protokolů RDP a SSH a

standardních klientů typu putty a remote desktop manager. U všech možností připojení ke vzdálené relaci musí být podporováno vynucení silné autentizace (minimálně integrace s LDAP a RADIUS).

Správcovský přístup prostřednictvím SSH protokolu se bude provádět přes SSH Proxy, kde bude uživatel ověřen svými přihlašovacími údaji (je možné spárovat s MS Active Directory) a bude připojen zvoleným privilegovaným účtem na cílový systém bez zadávání hesla a dle bezpečnostní politiky. Pro připojení pomocí SSH Proxy je vyžadována podpora silné autentizace (minimálně integrace s LDAP, RADIUS, či autentizace pomocí SSH klíče).

Vzdálené připojení zajišťuje řešení tak, aby nebylo potřeba dalších licencí třetích stran, např. MS CAL, a tak, aby nebylo potřeba pro tento účel instalovat zvláštní server fyzický ani virtuální.

Řešení musí umožňovat monitoring a nahrávání celé relace a aktivit privilegovaných účtů v komprimovaném video formátu s možností kontextového vyhledávání, bez nutnosti instalace permanentních agentů na koncový systém nebo na stanici administrátora. V nahrávkách je možné zpětně vyhledávat v záznamu ve formě metadat – minimálně u RDP spuštěné aplikace a události, u SSH relací jednotlivé příkazy, u Webových aplikací click na jednotlivé odkazy, u jiných typů relací alespoň stisky kláves. Pro přehrávání nahrávek není potřeba instalace nástrojů třetích stran (flash, java, codec, atp...) a je dostupné z GUI dodávaného řešení.

Řešení nabízí možnost uživatelům s konkrétním oprávněním (Auditor) manuální nahlížení do probíhajících relací a jejich případné pozastavení, zamknutí a terminaci potenciálně nebezpečných RDP a SSH relací s možností jejich následného odemčení.

Řešení nabízí možnost automatického pozastavení, zamknutí a terminaci potenciálně nebezpečných SSH relací a reporting nad těmito potenciálně nebezpečnými relacemi.

Sledování živých relací je také možné pomocí prohlížeče a protokolu HTTPS.

Systém umožňuje autorizovanému personálu centrálně vyhledávat v nahrávkách podle data, uživatele a spuštěného příkazu.

Součástí řešení nebo pomocí integrace na SIEM nebo SOAR, je možnost provádět průběžnou analýzu využívání privilegovaných účtů a následnou detekci potenciálně škodlivého chování – uživatel se připojuje z nestandardní IP, uživatel se připojuje na systémy, na které běžně nemá přístup, uživatel používá privilegovaný přístup v nestandardní časy, atp.

Nahrávky musí být zaznamenávány efektivním způsobem (např. s využitím komprimace, zaznamenávání pouze aktivní relace). Řešení, které zaznamenává celou nahrávku, není z kapacitních důvodů připuštěno. Maximální povolená velikost SSH/RDP nahrávek za 1min. je 20 MiB.

Bezpečný vzdálený přístup

Řešení umožňuje okamžité zavedení nových uživatelů do systému. Správce řešení může přes webové rozhraní vytvořit uživatele, přiřadit mu oprávnění s jakými privilegovanými účty může disponovat a pro jaké časového období. Řešení následně zašle email novému uživateli a umožní mu bezpečné vzdálené připojení k PAM řešení.

Před bezpečným vzdáleným připojením uživatele k řešení PAM je uživatel ověřen pomocí druhého faktoru.

Řešení musí obsahovat nativní TOTP (Time-based one-time password) nástroj pro silnou autentizaci přistupujících uživatelů k řešení. Nástroj musí generovat QR kódy pro rychlé zavedení silného ověření pro uživatele. Souběžně toto nativní řešení musí podporovat autentizační mechanismy, např. typu Microsoft Authenticator, Google Authenticator nebo jiných rovnocenných řešení.

Spojení mezi externím uživatelem a řešením PAM musí být plně šifrované. Není umožněno přímé spojení mezi stanicí uživatele a cílovým systémem – je využit princip tzv. „jump serveru".

Nástroj musí při žádosti o přístup automaticky vyhodnocovat kontextová data založená na konkrétním dni, datu, času a geolokaci žadatele o přístup, ještě před schválením/odmítnutím daného přístupu. Tento proces musí být plně automatický.

Základní řešení PAM nevyžaduje instalaci agenta na stanice uživatelů a na cílové systémy. Uživatelům je umožněno bezpečně přistupovat pomocí webového prohlížeče do řešení PAM.

Audit a reporting

Systém musí umožňovat audit jednotlivých akcí uživatelů s privilegovanými účty – zobrazení hesla, změny uložených údajů, vytvoření relace.

Řešení musí umožňovat vygenerování reportu veškerých aktivit administrátora řešení.

V nabízeném řešení musí být k dispozici minimálně následující předdefinované typy reportů:

- Report uživatelů a jejich oprávnění včetně výpisu účtů, které mají k dispozici,
- Report všech spravovaných účtů včetně přiřazených politik hesel a výčtu uživatelů, kteří mají k danému účtu přístup,
- Report o současných i historických změnách hesel napříč prostředím,
- Report aktivit nad účty (check out/in, přidělení účtu atp.),
- Report softwaru, který je instalovaný na koncových privilegovaných aktivech a otevřené porty na daném aktivu včetně vizuální prezentace.

Řešení musí generovat reporty ve všech z následujících formátů: XML, CSV, PDF, Excel, Word a TIFF.

Řešení umožňuje nastavení přístupu k reportům pouze pro vybrané uživatele.

Pro zabezpečení přístupu k archivovaným relacím systém neumožňuje uživatelům / správcům exportovat nahrávky do jiného video formátu, ani externě nakládat s nahrávkami a mít tak citlivé nahrávky plně pod kontrolou po celou dobu jejich existence.

Auditní záznamy a logy veškerých aktivit v zabezpečeném úložišti jsou chráněné proti změnám a smazání všemi uživateli (včetně všech administrátorských rolí řešení), a to minimálně po dobu 30 dní. Auditní záznamy musí být bezpečně uloženy v zašifrované podobě tak, aby k nim měl přístup pouze oprávněný uživatel.

Řešení umožňuje nahlížení do historie snapshotů a stavu jednotlivých aktiv v síti v návaznosti na automatické skenování. Tyto snapshoty musí reportovat historii změn, a to minimálně privilegovaných účtů, sdílených účtů, servisních účtů, instalovaného SW a otevřených portů.

Systém umožňuje monitoring jednotlivých komponent pomocí RestAPI – integrace se systémy zadavatele a monitoring.

Integrace a Podporované platformy

Výrobce musí poskytovat veřejně seznam integrovaných řešení na úrovni Password Management, Remote Session Management, SIEM, atp.

Nabízený systém musí obsahovat API pro automatizaci a integraci třetích stran a mít jej plně zalicencované. Řešení musí umožnit integraci s nástroji typu Vulnerability Management, nebo RPA pro automatické a bezpečné předávání dat pomocí API rozhraní.

Řešení musí podporovat integraci s nástroji třetích stran pro vynucení vícefaktorové autentizace. Minimálně na úrovní LDAP/S, RADIUS, PKI, RSA.

Systém musí umožňovat integraci s nástroji SIEM pro přenos logovaných auditních záznamů, a to v reálném čase pomocí Syslog.

Systém musí umožňovat integraci s nástroji HSM – uložení šifrovacích klíčů k databázi řešení.

Systém musí nativně podporovat řízení hesel a bezpečné přístupy minimálně na systémech:

- Windows 7, 8, 8.1, 10, Windows Server 2008, 2012, 2016, 2019
- Active Directory,
- HP iLO, Dell DRAC, IBM,
- Windows Services, Windows Scheduled Tasks, IIS Application Pool, Windows Registry COM+,
- VMWare, HyperV, Citrix,
- Red Hat, Suse, Unix, AIX,
- MS SQL, MySQL, PostreSQL, Oracle,
- Fortinet, Checkpoint, Palo Alto, Symantec,
- Cisco, Juniper, F5, HP,
- Amazon Web Services, Office 365, Microsoft Azure Application Keys.

Pro další systémy pak musí disponovat možností definovat password management modul.

Integrace klientských aplikací: Microsoft Management Studio, WinSCP, Putty, VNC. Po integraci budou mít administrátoři dostupné jejich viditelné servery v nativních výše zmíněných aplikacích a při přístupu přes tyto aplikace budou zachovány všechny funkcionality PAM (automatické vydání hesla, nahrávání přístupu, rotace hesel a SSH klíčů).

Rozšiřitelnost řešení

Řešení umožňuje řízení oprávnění uživatelů na koncových systémech (OS platformy Windows, MacOS a UX), tak aby bylo možné granulárně definovat, který příkaz, aplikaci a akci je uživatel schopný spustit a pod jakými oprávněními. Řešení je schopné vynutit autorizaci (zadání důvodu, schvalování) pro každý úkon, který vyžaduje vyšší oprávnění, jako je spuštění aplikace vyžadující vyšší oprávnění, konfigurace systému, editace systémových nastavení atp.

Řešení umožňuje, aby uživatel na koncovém zařízení, ať se jedná o uživatelské pracovní stanice, notebooky nebo servery, mohl pracovat pouze pod standardním neprivilegovaným uživatelským oprávněním.

Veškeré požadavky na vyšší oprávnění jsou řízeny podle bezpečnostní politiky. Oprávnění jsou následně povyšována jednorázově pro vybrané aktivity. Správce řešení může centrálně definovat, jaké aplikace budou spuštěny se standardním oprávněním a které se budou spouštět s vyšším oprávněním. Díky této funkci lze umožnit uživatelům bezproblémovou práci se standardními prostředky a zároveň zajistit maximální bezpečnost systému. Řešení dokáže monitorovat spuštěné aplikace na koncových systémech a na základě monitoringu vytvářet politiky, které aplikace následně systém umožní na koncových bodech spustit a které nikoliv.

Řešení umožňuje spuštění neznámých aplikací na koncových bodech, ale v omezeném režimu (tzn. omezení práv, pod kterými je aplikace spuštěna, omezení přístupu ke korporátním datům, omezení přístupu na internet). Řešení umožňuje detekci a blokování aktivit, které vedou ke zcizení přihlašovacích údajů uživatelů na koncových bodech. Systém poskytuje zabezpečení minimálně na úrovni ochrany Windows credentials (SAM, LSASS, LSA, NTDS.dit atd.), přihlašovacích údajů uložených v cache prohlížečů (IE, Edge, Chrome, Firefox), přihlašovacích údajů uložených v různých nástrojích pro vzdálenou správu (WinSCP, VNC, Putty) a dalších standardních nástrojích (Git, Total Commander).

Řešení poskytuje možnost správy přihlašovacích údajů i pro stanice a servery na OS MS Windows, které nejsou trvale připojeny do korporátní sítě.

Implementace

V rámci implementace je požadováno:

1. Vytvoření dokumentu Solution Design s popisem architektury, jednotlivých komponent, návrhu hromadného rolloutu agentů (bude-li použito), akceptačních testů, pilotního testování.
2. Návrh politiky způsobu řízení privilegovaných účtů. Konzultace se Zadavatelem a finalizace politiky.
3. Instalace centrální správy.
4. Instalace dalších komponent (například skenery nebo další potřebné servery).
5. Konfigurace centrální správy, vytvoření uživatelů a skupin, nastavení SMTP reportingu, vytvoření nebo úprava dashboardů po domluvě s administrátory Zadavatele. Volitelně nastavení SSO.
6. Vytvoření skenovacích úloh (host Discovery a privilegovaných účtů, otestování funkčnosti na pilotním vzorku, vyladění autentizace v rámci privilegovaných skenů).
7. Načítaní všech privilegovaných účtů a zařízení na platformách Windows, Linux, databáze, síťová zařízení, bezpečnostní technologie a automatizace vyhledávání zařízení / účtů a jejich automatické členění do skupin dle sítí a účelu zařízení / účtů.
8. Nastavení skupin a oprávnění uživatelů a administrátorů PAM, nastavení a přiřazení přístupových politik skupinám uživatelů, nastavení politik hesel podle skupin zařízení.
9. Automatizované navázání administrátorských účtů z domény k administraci jednotlivých skupin zařízení.
10. Automatizované navázání osobních administrátorských účtů z domény a ze zařízení běžným účtům administrátorů tak, aby každý administrátor používal jen svůj osobní privilegovaný účet a neviděl v žádném případě jiné osobní administrátorské účty.
11. Přiřazení automaticky vytvářených skupin účtů skupinám uživatelů.
12. Spuštění automatické rotace řízených účtů.
13. Zajištění automatického reportování změny hesel a aktivit s účty.

14. Vytvoření provozní dokumentace – popis běžných operativních aktivit, upgradu agentů a komponent, instalace a odinstalace (manuální i hromadné), troubleshooting.
15. Realizace akceptačních testů.
16. Seznámení s obsluhou pro 2 administrátory řešení v rozsahu 2 dnů.

Síťová infrastruktura a WiFi

Cílem je modernizace počítačové sítě náhradou zastaralých prvků a zvýšení její kapacity doplněním nových prvků. Současně bude pro zvýšení úrovně zabezpečení počítačové sítě implementován systém řízení přístupu k síti NAC na bázi protokolu IEEE 802.1X s napojením na centrální databázi identit Active Directory a systém řízení identit Identity Management. NAC bude implementován jako jednotný pro drátovou i bezdrátovou část sítě a dynamické zařazování koncových zařízení do VLAN na základě ověření, typu zařízení apod.

Core switch/switche – 3 kusy

- L3 modulární nebo 1U switche s podporou stackování
- Minimální počet portů v modulárním switchi/stacku
    - 72x 10 Gbps SFP+
    - 48x 1Gbps 1000BASE-T, podpora L3
- Možnost rozšíření na minimálně dvojnásobek požadovaného počtu portů v rámci modulárního switche / stacku
- Všechny SFP+ porty budou osazeny SM LR 10Gb transceivery (je přípustné použití OEM modulů)
- Redundantní napájecí zdroje
- Vyměnitelné ventilátory – hot swap

Access switche

- 20x 1U switch: min 48x 1Gbps 1000BASE-T bez PoE, alespoň 2x 10Gbps SFP+ uplink
- 10x 1U switch: min 24x 1Gbps 1000BASE-T bez PoE, alespoň 2x 10Gbps SFP+ uplink
- 20x 1U switch: min 48x 1Gbps 1000BASE-T s PoE (min 370W), alespoň 2x 10Gbps SFP+ uplink
- 10x 1U switch: min 24x 1Gbps 1000BASE-T s PoE (min. 370W), alespoň 2x 10Gbps SFP+ uplink
- Minimálně dva SFP+ porty v každém switchi budou osazeny SM LR 10Gb transceivery (je přípustné použití OEM modulů)

Obecné požadavky na switche

- Centrální management switchů – provedení on-premise (HW nebo virtuální appliance – není přípustný cloudový management), trvalá licence pro všechny dodané prvky
- Podpora "jumbo rámců" včetně velikosti 9198 Byte
- Podpora linkové agregace IEEE 802.3ad
- Konfigurovatelné rozkládání LACP zátěže podle L2 a L3
- Protokol pro definici šířených VLAN: MVRP
- Podpora VLAN podle IEEE 802.1Q, minimálně 512 aktivních VLAN
- IEEE 802.1s - Multiple Spanning Tree
- STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
- Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED
- Detekce jednosměrnosti optické linky (např. UDLD)
- NTP pro IPv4 a IPv6 včetně MD5 autentizace
- Statické směrování IPv4 a IPv6
- IGMP v2 a v3
- MLD v1 a v2
- Hardware podpora IPv4 a IPv6 ACL
- ACL definice na základě skupiny fyzických portů

- ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN
- BPDU guard a Root guard
- HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na množství paketů za vteřinu
- ICMPv4 a ICMPv6 rate-limiting per port
- Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port
- Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
- 802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN
- Dynamické zařazování do VLAN
- 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení)
- Port security
- Podpora IPv4 a IPv6 QoS

Emailová brána

Nasazení systému zajišťujícího kontrolu proti spamu, virům a malware u emailů, které projdou přes emailový server (email gateway). Dále budou propuštěny pouze emaily, které budou splňovat nastavená kritéria. Systém na bázi MTA, který zajistí ochranu před spamem, phishingem a známým malware. Kontrola dle reputačních databází odesilatelů, behaviorální a heuristická analýza obsahu, kontrola URL v těle mailu a možnost integrace s blacklisty třetích stran. Systém musí disponovat karanténou včetně uživatelského přístupu. Licenční model dle počtu chráněných uživatelů.

Dodávané řešení musí splňovat alespoň následující funkce a parametry.

Architektura řešení

Emailová bezpečnostní brána musí být nasazena ve dvou lokalitách z důvodu zajištění geografické redundance. Předpokládá se nasazení v režimu MTA, včetně možnosti nasazení v režimu vysoké dostupnosti. Systém musí být poskytnut formou virtuálního zařízení do virtualizovaného prostředí. AntiSpamové řešení bude sloužit jako první ochrana emailové komunikace. Řešení musí být schopno emailové filtrace pro minimálně 1000 uživatelů.

Minimální požadavky

- kontrola na úrovni spojení, hlaviček i těla zprávy,
- kontrola oproti databázi známých SPAM zpráv,
- kontrola oproti reputační databázi odesílajících mailserverů,
- behaviorální a heuristická analýza,
- podpora Bayesova filtru,
- kategorizace URL obsažených v emailu,
- podpora greylistingu,
- podpora integrace s blacklisty třetích stran,
- podpora funkce DMARC,
- možnost konfigurovat akci na základě detekovaného SPAMu:
    - přidání tagu,
    - přidání hlavičky,
    - předání emailu na jiný poštovní server,
    - odmítnutí (reject),
    - zahození (discard),
    - uložení do karantény,
    - přepsání adresy příjemce,
- podpora karantény včetně pohodlného uživatelského přístupu do karantény,
- možnost omezit parametry na úrovni navázaného SMTP spojení, jako např.:
    - počet zpráv za definované časové rozmezí odeslaných jedním klientem,
    - maximální počet spojení navázaných klientem,
    - verifikace uživatelských jmen (SMTP, LDAP),
    - možnost omezit počet zpráv v rámci SMTP relace,
- integrovaná funkce DLP (ochrana úniku citlivých informací),
- výkonnost (musí dostatečně převyšovat tzv. nejhorší scénář pro 1000 uživatelů),
- licenční model nezávislý na počtu chráněných IP adres/uživatelů, případně licenci pokrývající s dostatečným přesahem odhady růstu na následujících 5 let a to minimálně 50% růst,

- plnohodnotný management pomocí web GUI (HTTPs) a CLI (SSH),
- plnohodnotná integrace se síťovým dohledem (podpora SNMP v2c, v3), včetně dostupnosti MIB souboru dodávaného výrobcem.

Systém pro zálohování dat

Nabízené SW řešení musí být přítomné v kvadrantu lídrů za rok 2022 Gartner Magic Quadrant pro řešení zálohování a obnovy datového centra (Enterprise Backup and Recovery Software Solutions).

- Trvalé licence pro zálohování minimálně 100 virtuálních serverů, 20 HW serverů a 50 stanic.
- Software musí podporovat hostitele spravované serverem VMware vCenter Server a samostatné hostitele.
- Software musí podporovat hostitele Hyper-V spravované produktem System Center Virtual Machine Manager, klastrové počítače, samostatné počítače a režim instalace serveru Nano Server.
- Software musí podporovat zálohování všech operačních systémů, které jsou podporovány pro provoz ve virtualizaci VMware nebo Hyper-V.
- Software musí být nezávislý na hardware a musí využívat jakýkoli hardware serveru a úložiště.
- Software musí umožňovat vytváření záloh v plném, syntetickém úplném, přírůstkovém a zpětném přírůstkovém režimu.
- Software musí mít mechanismy deduplikace a komprese, které vedou ke snížení objemu úložného prostoru pro zálohy. Povolení deduplikace a/nebo komprese nesmí omezit žádné funkcionality uvedené ve specifikaci.
- Níže uvedené požadavky na HW pro systém pro zálohování dat jsou minimální

Server pro zálohy – 2kusy

Parametr	**Požadované parametry řešení**
Provedení a vnitřní uspořádání	provedení RACK (hloubka do 85 cm, výška 1U), hot-plug vnitřní komponenty, pro přístup ke všem komponentám serveru není nutné nářadí, zásuvné kolejnice pro instalaci do racku. Čelní displej není podmínkou.
CPU	Systém osazený 1x CPU, který má min. 42000 Benchmark bodů a současně min. 2700 bodů pro Single Thread Rating dle https://cpubm.com/top-cpu/ a.
RAM	Velikost paměti 128GB, optimalizace pro maximální výkon, moduly organizace 2R, server musí podporovat 16 paměťových slotů, 3200Mhz RDIMM.
Datové disky	Minimálně 2 ks hot plug 480GB SSD disk velikosti 2,5". Endurance DWPD (Drive Writes Per Day) minimálně 3,5.
Úložný prostor a rozšíření	Server musí podporovat bez dodatečných nákladů minimálně 8ks 2,5" hot plug disků typu SAS, SATA, server musí akceptovat rotační i SSD disky, včetně jejich kombinace. Možnost rozšíření diskové kapacity o minimálně 2 disky na celkem min. 10 disků.
Diskový řadič	Rozhraní SAS/SATA, 12Gb/s SAS a 6Gbs SATA, PCI Express 3.0x8 link, RAID 0, 1, 5, 6, 10, porty pro připojení minimálně 8 zařízení. Podpora Mixed Mode provozu.
Řadič SAS	Rozhraní SAS, 12Gb/s SAS, PCI Express 3.0x8 link, RAID 0, 1, 5, 6, 10, 2x externí port SAS minimálně. Podpora Mixed Mode provozu.
Síťové rozhraní	1x 2-port 10/25Gbit/s SFP+ /SFP28 adaptér LAN.

FC rozhraní	2x 1-port 32Gbit/s SFP FC HBA adaptér.
Management rozhraní	1x dedikovaný port LAN pro vzdálenou správu. 1x Dedikovaný port USB pro lokální správu. Umístění portu na čelním panelu.
USB rozhraní	Minimálně 4xUSB port 3.X (1xpřední, 1x interní, 2x zadní)
TPM Modul	Osazený TPM Modul
Napájení	2x redundantní, za běhu měnitelné napájecí zdroje o výkonu minimálně 800W. Zdroje musí vyhovovat technické specifikaci Platinum. Musí podporovat vzdálený management s možností zapínat, vypínat a restartovat server.
Management procesor	Management procesor pro vzdálenou správu (virtuální grafická konzole) včetně plné podpory hostitelského OS a vzdálených médií. Licence a technická podpora musí být dostupná po celou dobu záruční podpory serveru.
Kompatibilita (podporované OS)	Microsoft Windows Server 2019, 2022, VMware 7.1, 8.0
OS a licence CAL,	Microsoft Windows Server 2022 Standard
Podpora a servis	60 měsíců servisní podpora v režimu 9x5 NBD – servisní podpora hardware a software třetích stran s odezvou do druhého pracovního dne. Servis musí být prováděn výrobcem serveru, nebo autorizovaným servisním partnerem v ČR.

Diskové pole 1 – 1 kus

Parametr	**Požadované parametry řešení**
Provedení a vnitřní uspořádání	Provedení RACK, max. 4U, plná kompatibilita s nabízeným serverem, společný management pro všechny pole. Hot-plug vnitřní komponenty, pro přístup ke všem komponentám pole není nutné nářadí, zásuvné kolejnice pro instalaci do racku.
Řadiče	Diskové pole s redundantními řadiči pracujícími v režimu active-active podle standartu ALUA. Celková paměť na řadičích musí být min. 24GB.
Výkon na front-end portech	Výkon pole na úrovni front-end portů min. 200 000 IOPS (8k 100% random read) pro SSD Tier.
Front-end konektivita	Pole musí být vybaveno min. 4x 16Gb/s FC rozhraním s možností rozšíření na 8 portů celkem. Pole musí být vybaveno 2x LAN RJ-45 portem pro management (1 na každý kontrolér).
Kapacita pro disky SSD	Minimálně 4 ks 1,92TB Read Intensive SSD, 2,5". Endurance DWPD (Drive Writes Per Day) minimálně 1.
Kapacita pro disky HDD	Minimálně 20 ks 14TB SATA, 7 200 ot/s, 3,5" HDD. Diskové pole musí podporovat poslední generaci SAS disků (12Gb).
Rozšiřitelnost kapacity	Minimálně na 120 disků. Všechny typy disků (SSD, SAS, SATA) musí být možno kombinovat v jedné diskové polici.

Záloha datové cache	Cache paměť musí být zálohována (bateriemi, vysokokapacitními kondenzátory nebo podobnou technologií) po dobu min. 5 let.
Podpora RAID	Odolnost proti výpadku minimálně dvou disků (RAID 6, distribuovaný RAID 6 nebo obdobná technologie
Spare disk	Pole musí umět nastavit spare disky dedikované (pro určitou RAID skupinu) i globální pro celé pole.
Tiering	Podpora automatického přesouvání blokových dat mezi diskovými tiery (tvořené např. 10k SAS a SSD disky).
Počet LUN	Pole by mělo umožnovat vytvoření alespoň 512 logických disků (LUN). Velikost jednoho LUNu min.100TB nebo větší.
Licence SW	Pole podporuje a má plně licencovanou funkcionalitu Thin Provisioning včetně podpory T-10 SCSI UNMAP funkcionality na celou kapacitu pole.
Licence snapshot	Nabízená technologie musí umět vytvářet snapshoty a klony LUNů a musí být možné vytvořit až 512 snapshotů jednoho LUNu na úrovni diskového pole.
Podpora MPIO	Pole podporuje standardy typu MPIO pro připojení LUNů více cestami. Pokud je k tomu zapotřebí specializovaný SW, požaduje se přiložit licence pro neomezený počet server.
Podpora OS	Microsoft Windows Server 2019, Microsoft Windows Server 2022, VMware vSphere 7.X, 8.0
Podpora vCentre	Pole musí být možné spravovat i z vCenter rozhraní (vytváření nových datastore, templates apod).
Podpora VAAI	Pole musí podporovat VAAI primitiva pro VMware integraci.
Redundance a vysoká dostupnost	Pole musí být ve vysoce dostupné konfiguraci a podporovat přidávání a náhradu disků za běhu, mít redundantní řadiče, napájení a větráky.
Upgrade SW a firmware	Veškeré upgrady pole (včetně upgrade FW řadičů i disků, přidávání diskových polic) musí být realizovatelné on-line.
Měření a nastavení výkonu	Nabízené řešení musí podporovat funkce Quality of Service, kde je možné definovat a garantovat minimální a maximální hodnoty IOPs a MB/s zátěže, latence a priority na úrovni jednotlivých disků a jejich skupin.
Podpora a servis	60 měsíců servisní podpora v režimu 24x7 – servisní podpora hardware a software třetích stran s odezvou do druhého pracovního dne. Servis musí být prováděn výrobcem serveru, nebo autorizovaným servisním partnerem v ČR.

Diskové pole 2 – 2kusy

Parametr	**Požadované parametry řešení**
Provedení a vnitřní uspořádání	Provedení RACK, max. 4U, plná kompatibilita s nabízeným serverem, společný management pro všechna pole. Hot-plug vnitřní komponenty, pro přístup ke všem komponentám pole není nutné nářadí, zásuvné kolejnice pro instalaci do racku.
Řadiče	Diskové pole s redundantními řadiči, pracujícími v režimu active-active podle standartu ALUA. Celková paměť na řadičích musí být min. 24GB.
Výkon na front-end portech	Výkon pole na úrovni front-end portů min. 200 000 IOPS (8k 100% random read) na SSD Tier.

Front-end konektivita	Pole musí být vybaveno min. 4x 16Gb/s FC rozhraním s možností rozšíření na 8 portů celkem. Pole musí být vybaveno 2x LAN RJ-45 portem pro management (1 na každý kontrolér).
Počet spare disků	Minimálně 2 ks spare disk
Kapacita pro disky HDD	Minimálně 20 ks 14TB SATA, 7 200 ot/s, 3,5" HDD. Diskové pole musí podporovat poslední generaci SAS disků (12Gb).
Rozšiřitelnost kapacity	Minimálně na 120 disků. Všechny typy disků (SSD, SAS, SATA) musí být možno kombinovat v jedné diskové polici.
Záloha datové cache	Cache paměť musí být zálohována (bateriemi, vysokokapacitními kondenzátory nebo podobnou technologií) po dobu min. 5 let.
Podpora RAID	Odolnost proti výpadku minimálně dvou disků (RAID 6, distribuovaný RAID 6 nebo obdobná technologie
Spare disk	Pole musí umět nastavit spare disky dedikované (pro určitou RAID skupinu) i globální pro celé pole.
Tiering	Podpora automatického přesouvání blokových dat mezi diskovými tiery (tvořené např. 10k SAS a SSD disky).
Počet LUN	Pole by mělo umožnovat vytvoření alespoň 512 logických disků (LUN). Velikost jednoho LUNu min.100TB nebo větší.
Licence SW	Pole podporuje a má plně licencovanou funkcionalitu Thin Provisioning včetně podpory T-10 SCSI UNMAP funkcionality na celou kapacitu pole.
Licence snapshot	Nabízená technologie musí umět vytvářet snapshoty a klony LUNů a musí být možné vytvořit až 512 snapshotů jednoho LUNu na úrovni diskového pole.
Podpora MPIO	Pole podporuje standardy typu MPIO pro připojení LUNů více cestami. Pokud je k tomu zapotřebí specializovaný SW, požaduje se přiložit licence pro neomezený počet server.
Podpora OS	Microsoft Windows Server 2019, Microsoft Windows Server 2022, VMware vSphere 7.X, 8.0
Podpora vCentre	Pole musí být možné spravovat i z vCenter rozhraní (vytváření nových datastore, templates apod).
Podpora VAAI	Pole musí podporovat VAAI primitiva pro VMware integraci.
Redundance a vysoká dostupnost	Pole musí být ve vysoce dostupné konfiguraci a podporovat přidávání a náhradu disků za běhu, mít redundantní řadiče, napájení a větráky.
Upgrade SW a firmware	Veškeré upgrady pole (včetně upgrade FW řadičů i disků, přidávání diskových polic) musí být realizovatelné on-line.
Měření a nastavení výkonu	Nabízené řešení musí podporovat funkce Quality of Service, kde je možné definovat a garantovat minimální a maximální hodnoty IOPs a MB/s zátěže, latence a priority na úrovni jednotlivých disků a jejich skupin.
Podpora a servis	60 měsíců servisní podpora v režimu 24x7 – servisní podpora hardware a software třetích stran s odezvou do druhého pracovního dne. Servis musí být prováděn výrobcem serveru, nebo autorizovaným servisním partnerem v ČR.

Pásková knihovna – 1 kus

Parametr	Požadované parametry řešení
Provedení	Modulární provedení konstrukce, základní modul o velikosti max 3U.
Uchycení	Rack-mount včetně montážního kitu.
Škálovatelnost	Možnost až 6 rozšiřujících modulů 3U pro celkovou kapacitu až 280 kazet.
Počet slotů	Minimálně 40 slotů
Počet zásobníků	Minimálně 2 zásobníky
Počet mail slotů	Mimimálně 5 slotů
Podpora jednotek	Podpora až tří páskových jednotek s poloviční výškou nebo kombinace jedné páskové jednotky s vysokou páskou a jedné páskové jednotky s poloviční výškou v každém modulu.
Napájení	2x redundantní hot-swap napájecí zdroj 80 PLUS Silver. Zdroje napájení musí být připojeny ke dvěma samostatným okruhům.
Čárové kódy	Čtečka čárových kódů
Konektivita	Minimálně 2xSFP+ 8 Gbit/s Fiber Channel Protocol
Management port	2x RJ-45 LAN, 100/1000Mbit/s, 2x USB port
Rychlost přenosu dat	Nativní rychlost přenosu dat minimálně 300 MB/s
Management	Čelní ovládací panel + ovládací tlačítka
Vzdálený management	Webové grafické uživatelské rozhraní; SNMP, e-mailová upozornění.
Počet a typ mechanik	2x LTO8 Ultrium
Nativní kapacita pásky	Minimálně 10 TB
Minimální kapacita	Minimálně 1PB pro plně obsazený modul.
Typ média	Verze LTO-8
Datová kazeta	Minimálně 40 kusů
Čistící kazeta	Minimálně 2 kusy
Podpora backup SW	Veeam Backup and Retention, ARCserve Server, CommVault Simpana, HPE/Micro Focus Data Protector
Hostitelské operační systémy	Microsoft Windows Server 2016, 2019 a 2022; Red Hat Enterprise Linux (RHEL) 6 a 7; SUSE Linux Enterprise Server (SLES) 12.
Záruka	60 měsíců servisní podpora v režimu 9x5 NBD – servisní podpora hardware a software třetích stran s odezvou do druhého pracovního dne. Servis musí být prováděn výrobcem switche nebo autorizovaným servisním partnerem v ČR.

SAN Switch – 2 kusy

Parametr	Požadované parametry řešení
Provedení	SAN switch 24 port v provedení rack mount.
Velikost	1U včetně montážního kitu.
Počet portů	Až 24x 32/16/8Gbit/s SFP+ Porty.
Osazení portů	24x port 16Gb/s SW. Možná výměna SFP za LW moduly
Management port	1x RJ45 1Gb Ethernet pro management, 1x USB port, 1x Serial port
Připojovací kabely	24ks kabelů LC/LC OM4 2f 5m
Přenosový protokol	Protokol datového spoje Fibre Channel SCSI.
Propustnost	Minimálně 768Gbps.
Latence	Maximální latence 900ns
Duplex	Podpora plně duplexního provozu.
ISL Ttunking	Frame-based Trunking až pro 8x 32 Gbit/s porty na 1 ISL trunk; až 256 Gbp Gbit/s pro ISL trunk. . Exchange-based load balancing přes ISLs s DPS včetně Fabric OS
Podpora portů	F_Port, E_Port, M_Port, D_Port (ClearLink Diagnostic Port) on 24 SFP+ port, Access Gateway mode: F_Port and NPIV-enabled N_Port.
Zabezpečení	Metoda ověřování min. RADIUS, Secure Shell v.2 (SSH2), LDAP
Podpora QoS	Podpora pro adaptivní síťové služby, jako je Quality of Service (QoS). Switch musí podporovat omezení datového toku od méně kritických hostitelů v přednastavených šířkách pásma.
Autentikace	FC-SP for host-to-switch and switch-to-switch authentication.
Požadované SW a HW vlastnosti	Licence pro všechny porty switche pro: Full Fabric, Advanced Zoning, Advanced Diagnostic Tools
Management SW	Podpora managementu pro WEB rozhraní, podpora pro CLI
Zónování	Podpora zónování (ardware-enforced zoning, Logical-unit-number (LUN) zoning a read-only zones).
Vzdálený management	SNMP v3, HTTPS, SMI-S, SSH-2.
Záruka	60 měsíců servisní podpora v režimu 9x5 NBD – servisní podpora hardware a software třetích stran s odezvou do druhého pracovního dne. Servis musí být prováděn výrobcem switche nebo autorizovaným servisním partnerem v ČR.

Nástroj pro zabezpečení zdravotnických zařízení

Systém musí provádět pasivní (tj. bez explicitní komunikace směrem ke koncovým zařízením) detekci klinické přístrojové techniky a dalších IoT technologií. Takto vytváří evidenci a díky široké databázi a schopnosti rozpoznání jednotlivých technologií vytváří také kategorizaci do logických celků. Součástí řešení je také vizualizace komunikační matice, rozpoznání zranitelností a možnost alertingu všech odchylek od dané baseline. Systém musí poskytovat informace a reporty o používaní zdravotnické techniky, a to nejen dobu po kterou je zařízení online, ale počet a případně typ zákroku na daném zařízení.

Dodávané řešení zabezpečení zdravotnických zařízení musí splňovat alespoň následující funkce a parametry.

Licenční pokrytí

Systém musí být poskytnut formou virtuálního zařízení do virtualizovaného prostředí. Požadována je licence do prostředí obsahujícího 600 zdravotnických prostředků bez omezení počtu koncových IoT zařízení.

Primární funkcionality systému

Automatický discovery engine – systém eviduje a rozpozná přístrojovou techniku, vytvoří katalog zařízení pro asset management, tj. vytváří pro dané prostředí CMDB, která může být pro následné procesy primární, či podpůrná pro validaci existující CMDB.

Kategorizace zařízení – nalezená zařízení jsou rozčleněna do logických skupin, ke kterým lze následně přistupovat v rámci nastavení dalších systémů jako k objektům, bez nutnosti vytvářet pravidla pro každé zařízení zvlášť. Tento mechanizmus musí zajistit odpovídající škálovatelnost řešení bez nutnosti vykonávat atomické operace nad jednotlivými zařízeními manuálně.

Vyhodnocení zranitelnosti – díky schopnosti rozpoznat aktuální verzi systému/firmware nalezeného zařízení a propojení na databázi zranitelností systém reportuje riziková zařízení. Výrobce systému musí být v alianci s výrobci přístrojové techniky a zohlednit reálné bezpečnostní riziko daných zařízení, nikoliv odhadované riziko na základě generických hodnocení o použitém OS, či SW. Tento postup zajišťuje snížení false positive a tím nutné operativy na adekvátní mez. Systém musí v této souvislosti pracovat se vstupy MDS2 standardu.

Monitoring provozu – vytvoření komunikační mapy pro ověření validity provozu a zejména reporting odchylek od dané baseline. Systém musí být schopen zobrazit také servisní přístupy pro jednotlivá zařízení v rámci mapy komunikační matice. Požadována je nativní integrace se systémem pro správu a monitoring servisních přístupů, tj. možné rozšíření o tuto funkcionalitu od stejného výrobce.

Indikátory kompromitace pro dané prostředí – specifické indikátory kompromitace pro nemocniční prostředí pomohou odhalit potenciální incident v preinfekční i postinfekční fázi díky nativní IDS funkcionalitě, jejíž výstupy jsou součástí management rozhraní a obohacují informační profil jednotlivých zařízení přístrojové techniky.

Integrace se síťovými a bezpečnostními prvky – je požadována automatizace s bezpečnostními prvky tak, aby bezpečnostní politika z pohledu síťových prostupů či potřebné izolace infikovaných zařízení zajistila okamžitou reakci bez nutnosti manuální rekonfigurace správcem řešení. To obsahuje zejména výměnu

informací o objektech v reálném čase a schopnost práce se skupinami zařízení dle navržených bezpečnostních profilů a politik. Konkrétní automatizační scénáře budou definovány v Solution Design dokumentu.

Utilizace přístrojové techniky – vytváření statistiky pro reálnou utilizaci zobrazovacích zařízení a infuzních pump tak, aby mohla být v přehledné formě reportována v manažerském přehledu. Integrací s PACS/DICOM zároveň poskytne statistiky typu zobrazovacích záznamů, včetně statistik segmentů.

Standardizace výstupů bezpečnostních událostí – podpora klasifikace a vizualizace atomických událostí ve frameworku MITRE ATT&CK ICS, tj. včetně rozšíření o ICS kategorie.

Vzhledem k nutnosti automatizovat bezpečnostní procesy pro schopnost okamžité reakce je nutné zajistit interoperabilitu požadovaného systému s dalšími existujícími či plánovanými systémy v rámci infrastruktury. Požadovaný systém v sobě kombinuje bezpečnostní mechanizmy a naplňuje související procesy ISO 27001 standardu (change management, patch management, incident management). Primární oblastí z pohledu síťové architektury je OT, resp. IoT část prostředí, která je v současné době definována separátním IP rozsahem a oddělena na úrovni VLAN segmentů. Dále je požadována podpora pro pxGrid – schopnost pracovat s SGT tagy pro bezpečnostní skupiny.

Integrace a nativní kompatibilita

Integrace je požadována pro následující okruhy řešení. Kompatibilita musí být zajištěna pro všechny relevantní komponenty tohoto projektu, zejména se jedná o části Síťová infrastruktura a WiFi a bezpečnostní brány. Dále je požadována integrace s produkty výrobců, které jsou v infrastruktuře již provozovány:

- VMware vCenter
- DHCP integrace – požaduje se integrace na Microsoft DHCP Server.

Dále řešení musí podporovat integrace na:

- NAC integrace - požaduje se přímá integrace na systém pro řízení přístupu na síti a to minimálně pro technologie: Cisco ISE, Aruba ClearPass Policy Manager, Fortinet FortiNAC.
- Network Management – požaduje se integrace na systémy pro management síťové infrastruktury, a to minimálně pro Cisco Prime a Cisco DNA-C.
- Skener zranitelností a to minimálně Rapid7, Nessus, Tenable sc., Qualys
- Nativní integrace pro vyčítání dat ze SNMP
- Microsoft Active directory
- Zobrazování vytíženosti infuzních pump Alaris

Řešení musí disponovat rozhraním REST API pro integraci s interními systémy zákazníka.

Řešení musí být schopno integrace systémy SIEM, SNMP a CMDB.

Podmínky technické podpory (SLA) a rozvoje řešení

Tento požadavek je součástí Servisu Díla. Dále uvedené požadavky se neuplatní ve vztahu k HW, u kterých je výše v technické specifikaci stanoven speciální požadavek. Dodavatel se zavazuje poskytovat zadavateli služby v režimu 24x7 v minimálním rozsahu:

- telefonická hot-line podpora pro okamžitou komunikaci 24h denně
- diagnostika a odstraňování poruch systému
- profylaxe - preventivní prohlídka systému v rozsahu
- kontrola stavu nainstalovaných updatů a hotfixů
- kontrola a analýza chybových logů systémového SW, stejně tak aplikačního programového vybavení
- kontrola vytíženosti systémových zdrojů
- sběr zpětné vazby od administrátorů systému

Dodavatel se zavazuje zadavateli, že jakékoliv vady plnění Servisu díla či jeho části, budou odstraněny na náklady dodavatele. Dodavatel garantuje zadavateli čas pro odezvu a čas pro vyřešení provozního incidentu, a to pro jednotlivé kategorie provozních incidentů následovně:

Kategorie incident	Lhůta odezvy (IRT)	Lhůta vyřešení (TRT)
Kritický	60 minut	4 hodiny
Závažný	60 minut	8 hodin
Běžný	1 den	3 dny
Minoritní	3 dny	Best effort

Podpora je poskytovaná v českém jazyce ve formě Help-desk podpory a v případě kritického incidentu telefonické podpory. Jednotlivé úkony/akce dle specifikace podpory jsou definovány následovně.

Lhůta odezvy (IRT)

Je definovaná jako časový interval měřený od doby, kdy zadavatel ohlásil incident do Helpdeskové aplikace poskytovatele nebo telefonicky s následným zadáním do Helpdeskové aplikace po dobu, kdy je zpětně kontaktovaný dodavatelem nebo je incident přijat do řešení. Lhůta odezvy může být také označována jako reakční doba.

Doba vyřešení (TRT)

Je definovaná jako časový interval měřený od doby, kdy zadavatel ohlásil incident do Helpdeskové aplikace poskytovatele nebo telefonicky s následným zadáním do Helpdeskové aplikaci po dobu, kdy dodavatel vyřešil popsaný incident.

Priority

Zaručená lhůta odezvy na vzniklé incidenty se dělí dle jejich priority. Priorita je dána kritičností vzniklého incidentu v návaznosti na požadovanou funkčnost produktu:

- Kritický incident – Nefunkčnost způsobená dodanou technologií, Nefunkčnost/nedostupnost řešení
- Závažný incident – Nefunkčnost některé z komponent, která nedovoluje vykonávat požadovanou činnost. Vážné chyby řešení ovlivňující provoz objednatele.
- Běžný incident – Nefunkčnost některé z komponent, která nemá přímý dopad na dostupnost objednatele, vážné konfigurační chyby.
- Minoritní incident – Chyby v konfiguraci, Chyby řešení neovlivňující provoz objednatele, Nefunkčnost komponent minoritního charakteru.

V rámci části služby rozvoje je požadován rozvoj a údržba díla, tedy činnosti, které nejsou součástí SLA podpory. Cena za Služby rozvoje je pro účely porovnatelnosti nabídek vypočtena jako součin Ceny za jeden člověkoden (MD) práce (implementace) bez DPH a předpokládaného Počtu člověkodní rozsahu 180 MD za období 5 let. Předpokládaný počet člověkodní (MD) je stanoven pouze pro účely hodnocení nabídek v zadávacím řízení. Zadavatel není povinen předpokládaný počet člověkodní (MD) služeb rozvoje vyčerpat.

Seznam poddodavatelů vč. rozsahu jejich plnění

Seznam poddodavatelů včetně rozsahu jejich plnění níže čítá tři poddodavatele:

Název poddodavatele	Rozsah plnění
Security Avenegers s.r.o.	Poddodavatel se zavazuje podílet na realizaci služeb specifikovaných v odst. 2.1 Poddodavatelské smlouvy – Obchodních podmínek. Více viz. poddodavatelská smlouvy, jež je součástí nabídky.
Aricoma Systems a.s.	Poddodavatel se zavazuje podílet na realizaci služeb specifikovaných v odst. 2.1 Poddodavatelské smlouvy – Obchodních podmínek. Více viz. poddodavatelská smlouvy, jež je součástí nabídky.
AVENET Distrobution s.r.o.	Poddodavatel se zavazuje podílet na realizaci služeb specifikovaných v odst. 2.1 Poddodavatelské smlouvy – Obchodních podmínek. Více viz. poddodavatelská smlouvy, jež je součástí nabídky.

Součástí dokladů prokazujících splnění kvalifikace je i Poddodavatelská smlouva, z níž je zřejmý závazek poddodavatele nést společnou odpovědnost a nerozdílnou odpovědnost za plnění veřejné zakázky.

Příloha č. 3
Realizační tým

Pozice v projektovém týmu	*Jméno a příjmení člena týmu*	*Agenda člena týmu*
Vedoucí realizačního týmu	[redacted]	Vedení projektového týmu, koordinace projektových aktivit mezi týmem objednatele a dodavatele, pravidelná účast na projektových poradách a statusech.
Bezpečnostní architekt	[redacted]	Návrh bezpečnostní architektury informačních systémů a integrace jejich jednotlivých komponent, dohled nad souladem implementace architektury.
Architekt síťové bezpečnosti	[redacted]	Návrh bezpečnostní architektury sítě a jejich jednotlivých komponent, dohled nad souladem implementace architektury.
Síťový specialista	[redacted]	Implementace jednotlivých prvků a technologií síťové bezpečnosti v souladu s designem sítě stanovené architektem.
Specialista na firewally	[redacted]	Implementace technologie firewallů a jejich následná integrace a konfigurace v souladu s návrhem architekta.
Specialista na ochranu privilegovaného přístupu	[redacted]	Implementace technologie privilegovaného přístupu, následná integrace a konfigurace v souladu s návrhem architekta.

Ing. Roman Kratochvíl

Digitálně podepsal Ing. Roman Kratochvíl
Datum: 2024.09.18 17:08:04 +02'00'

Příloha č. 4

Specifikace Proprietárního software

#	PartNumber	Výrobce	Popis/Název	Typ	Aktivita
1	CPSM-NGSM5	Check Point	Next Generation Security Management Software for 5 gateways (SmartEvent & Compliance 1 year)	SW	P1: Realizace perimetrového a centrálních firewallů a Sandbox
2	CPSB-EVS-5-3Y	Check Point	SmartEvent and SmartReporter blade for 5 gateways (Smart-1 & open server) 3 year subscription	SW	P1: Realizace perimetrového a centrálních firewallů a Sandbox
3	CPSB-EVS-5-1Y	Check Point	SmartEvent and SmartReporter blade for 5 gateways (Smart-1 & open server) 1 year subscription	SW	P1: Realizace perimetrového a centrálních firewallů a Sandbox
4	CPAP-SG9300-SNBT	Check Point	9300 Plus Appliance with SandBlast subscription package for 1 year	HW+SW	P1: Realizace perimetrového a centrálních firewallů a Sandbox
5	CPSB-SNBT-9300-3Y	Check Point	Next Generation Threat Prevention and Sandblast for additional 3 years for 9300 Plus Appliance	SW	P1: Realizace perimetrového a centrálních firewallů a Sandbox
6	CPSB-SNBT-9300-1Y	Check Point	Next Generation Threat Prevention and Sandblast for additional 1 year for 9300 Plus Appliance	SW	P1: Realizace perimetrového a centrálních firewallů a Sandbox
7	CPSB-MOB-200	Check Point	Mobile Access Blade for 200 concurrent connections	SW	P1: Realizace perimetrového a centrálních firewallů a Sandbox
8	CPSB-VS-10	Check Point	10 Virtual Systems package	SW	P1: Realizace perimetrového a centrálních firewallů a Sandbox
9	MA-SC-2k-SW	Grey Cortex	GREYCORTEX Mendel perpetuální SW licence: senzor + kolektor / 2Gbps trvalý průtok / 1800 obohacených toků za vteřinu & 3500 NetFlow za vteřinu / 8000 monitorovaných IP adres / Plná funkcionalita	SW	P1: Zavedení síťové behaviorální analýzy
10	MA-SC-2k-MS1Y	Grey Cortex	Roční SW předplatné pro MA-SC-2k-SW	SW	P1: Zavedení síťové behaviorální analýzy
11	MA-S-1k-SW	Grey Cortex	GREYCORTEX Mendel perpetuální SW licence: senzor / 1Gbps trvalý průtok / 1000 obohacených toků za vteřinu & Plná detekční sada	SW	P1: Zavedení síťové behaviorální analýzy
12	BT-APP-U-VM-SUB-5Y	Beyond Trust	BeyondTrust Appliance U Series-VMSubscription 5 years	SW	P1: Systém pro správu privilegovaných účtů
13	PS-SUB-5Y	Beyond Trust	Password Safe Per Asset Subscription 5 years	SW	P1: Systém pro správu privilegovaných účtů

14	MED-CVI-1500	MediGate	Medigate Essentials 0-1500 IoMT Devices	SW	P2: Nástroj pro zabezpečení zdravotnických zařízení
15	MED-ATD-1500	MediGate	Module: Advanced Anomaly & Threat Detection 0-1500 IoMT Devices	SW	P2: Nástroj pro zabezpečení zdravotnických zařízení
16	MED-CDE-1500	MediGate	Module: Advanced Clinical Device Efficiency 0-1500 IoMT Devices	SW	P2: Nástroj pro zabezpečení zdravotnických zařízení
17	MED-NSM-1500	MediGate	Module: Advanced Network Security Management 0-1500 IoMT Devices	SW	P2: Nástroj pro zabezpečení zdravotnických zařízení
18	MED-VRM-1500	MediGate	Module: Advanced Vulnerability & Risk Management 0-1500 IoMT Devices	SW	P2: Nástroj pro zabezpečení zdravotnických zařízení
19	FortiMail-VM04	FortiNet	FortiMail-VM04, SW virtual appliance	SW	P2: Emailová brána
20	FortiMail-VM04	FortiNet	FortiMail-VM04, Licence, 24x7 Enterprise ATP Bundle Contract 5YR	SW	P2: Emailová brána
21		Veeam	Veeam Data Platform Foundation Universal Perpetual License. Includes Enterprise Plus Edition features. 10 instance pack. 1 year of Production (24/7) Support is included. Public Sector.	SW	P2: Systém pro zálohování dat
22		Veeam	4 additional years of Production (24/7) maintenance prepaid for Veeam Data Platform Foundation Universal Perpetual License. 10 instance pack.	SW	P2: Systém pro zálohování dat

Datum dle data el. podpisu:

Ing.
Roman
Kratochvíl

.....

Doda

Projekt kybernetické bezpečnosti

Zadavatel:	**Nemocnice Znojmo, příspěvková organizace**
Dodavatel:	Euro Enterprise Development s.r.o.
Datum vyplnění:	30.07.2024

Cena za jeden člověkoden práce (implementace) bez DPH: 15 000 Kč

Dílo				
Aktivita	**Počet člověkodní implementace**	**Cena implementace bez DPH**	**Cena HW, SW vč. záruky na 2 roky bez DPH**	**Cena celkem b**
P1: Analytické práce v oblasti bezpečnosti	110	1 650 000,00 Kč	N/A	1 650 00
P1: Zavedení síťové behaviorální analýzy	65	975 000,00 Kč	**4 531 500,00 Kč**	5 506 50
P1: Realizace perimetrového a centrálních firewallů a Sandbox	65	975 000,00 Kč	**12 900 000,00 Kč**	13 875 00
P1: Vybudování PKI	18	270 000,00 Kč	**0,00 Kč**	270 00
P1: Systém pro správu privilegovaných účtů	70	1 050 000,00 Kč	**6 100 000,00 Kč**	7 150 00
P2: Síťová infrastruktura a WiFi	95	1 425 000,00 Kč	**6 404 400,00 Kč**	7 829 40
P2: Emailová brána	38	570 000,00 Kč	**3 720 000,00 Kč**	4 290 00
P2: Systém pro zálohování dat	75	1 125 000,00 Kč	**13 077 000,00 Kč**	14 202 00
P2: Nástroj pro zabezpečení zdravotnických zařízení	110	1 650 000,00 Kč	**11 820 000,00 Kč**	13 470 00
SUMA	**646**	**9 690 000,00 Kč**	**58 552 900,00 Kč**	**68 242 90**

Servis			
Kategorie	**Cena za 1 rok bez DPH**	**Cena za 5 let bez DPH**	**Cena za 5 let s DPH**
Plná údržba řešení (Full maintenance)	50 610,00 Kč	253 050,00 Kč	306 190,50 Kč
Technická podpora dodavatele v režimu 24-7 (SLA)	3 700 000,00 Kč	18 500 000,00 Kč	22 385 000,00 Kč
SUMA	**3 750 610,00 Kč**	**18 753 050,00 Kč**	**22 691 190,50 Kč**

Kategorie	**Počet MD/5 let/ bez DPH**	**Počet MD/5 let/ s DPH**
Služby rozvoje	180	180
SUMA	**2 700 000,00 Kč**	**3 267 000,00 Kč**

Sumarizace	**Cena bez DPH**	**Cena bez DPH**	**Cena bez DPH MAX**	**Cena s DP**
Projekt P1	**28 451 500,00 Kč**	**28 451 500,00 Kč**	**28 500 000,00 Kč**	**34 426 31**
Projekt P2	**39 791 400,00 Kč**	**39 791 400,00 Kč**	**40 000 000,00 Kč**	**48 147 59**
Celková cena díla	**68 242 900,00 Kč**	**68 242 900,00 Kč**	**68 500 000,00 Kč**	**82 573 90**
Celková cena servisu	**21 453 050,00 Kč**	**21 453 050,00 Kč**	**21 500 000,00 Kč**	**25 958 19**
Celková cena	**89 695 950,00 Kč**	**89 695 950,00 Kč**	**90 000 000,00 Kč**	**108 532 09**

#	PartNumber	Výrobce	Popis/Název	Typ	Aktivita	Je
1	CPSM-NGSM5	Check Point	Next Generation Security Management Softwar	SW	P1: Realizace perimetrového a centrálních firewallů a San	
2	CPSB-EVS-5-3Y	Check Point	SmartEvent and SmartReporter blade for 5 gate	SW	P1: Realizace perimetrového a centrálních firewallů a San	
3	CPSB-EVS-5-1Y	Check Point	SmartEvent and SmartReporter blade for 5 gate	SW	P1: Realizace perimetrového a centrálních firewallů a San	
4	CPAP-SBTE2500N-4	Check Point	SandBlast TE2500N-8VM Appliance	HW	P1: Realizace perimetrového a centrálních firewallů a San	
5	CPAP-SG9300-PLU	Check Point	9300 Plus Appliance with SandBlast subscriptio	HW+SW	P1: Realizace perimetrového a centrálních firewallů a San	
6	CPSB-SNBT-9300-3	Check Point	Next Generation Threat Prevention and Sandbla	SW	P1: Realizace perimetrového a centrálních firewallů a San	
7	CPSB-SNBT-9300-1	Check Point	Next Generation Threat Prevention and Sandbla	SW	P1: Realizace perimetrového a centrálních firewallů a San	
8	CPSB-MOB-200	Check Point	Mobile Access Blade for 200 concurrent connec	SW	P1: Realizace perimetrového a centrálních firewallů a San	
9	CPSB-VS-10	Check Point	10 Virtual Systems package	SW	P1: Realizace perimetrového a centrálních firewallů a San	
10	CPCES-CO-STANDA	Check Point	Collaborative Enterprise Support - Standard Ad	HW	P1: Realizace perimetrového a centrálních firewallů a San	
11	CPCES-CO-STANDA	Check Point	Collaborative Enterprise Support - Standard	HW	P1: Realizace perimetrového a centrálních firewallů a San	
12	MA-SC-2k-SW	Grey Cortex	GREYCORTEX Mendel perpetuální SW licence: s	SW	P1: Zavedení síťové behaviorální analýzy	
13	MA-SC-2k-MS1Y	Grey Cortex	Roční SW předplatné pro MA-SC-2k-SW	SW	P1: Zavedení síťové behaviorální analýzy	
14	HW-SC-M	Grey Cortex	HW server All-in-one model M / 4x1GbE & 2x10	HW	P1: Zavedení síťové behaviorální analýzy	
15	HW-E-SS4	Grey Cortex	HW rozšíření – datové úložiště: Dodatečné 2x3.8	HW	P1: Zavedení síťové behaviorální analýzy	
16	MA-S-1k-SW	Grey Cortex	GREYCORTEX Mendel perpetuální SW licence: s	SW	P1: Zavedení síťové behaviorální analýzy	
17	MA-S-1k-MS1Y	Grey Cortex	Roční SW podpora a údržba pro MA-S-1k-SW	Maintenance	P1: Zavedení síťové behaviorální analýzy	
18	HW-S-S	Grey Cortex	HW server Senzor model S / 4x1GbE monitorova	HW	P1: Zavedení síťové behaviorální analýzy	
19	BT-APP-U-VM-SUB	Beyond Trust	BeyondTrust Appliance U Series-VMSubscriptio	SW	P1: Systém pro správu privilegovaných účtů	
20	PS-SUB-5Y	Beyond Trust	Password Safe Per Asset Subscription 5 years	SW	P1: Systém pro správu privilegovaných účtů	
21	MED-CVI-1500	MediGate	Medigate Essentials 0-1500 IoMT Devices	SW	P2: Nástroj pro zabezpečení zdravotnických zařízení	
22	MED-ATD-1500	MediGate	Module: Advanced Anomaly & Threat Detectior	SW	P2: Nástroj pro zabezpečení zdravotnických zařízení	
23	MED-CDE-1500	MediGate	Module: Advanced Clinical DeviceEfficiency 0-15	SW	P2: Nástroj pro zabezpečení zdravotnických zařízení	
24	MED-NSM-1500	MediGate	Module: Advanced Network SecurityManageme	SW	P2: Nástroj pro zabezpečení zdravotnických zařízení	
25	MED-VRM-1500	MediGate	Module: Advanced Vulnerability & Risk Manage	SW	P2: Nástroj pro zabezpečení zdravotnických zařízení	
26	JL663A	Aruba	Aruba 6300M 48G 4SFP56	HW	P2: Síťová infrastruktura a WiFi	
27	JL658A	Aruba	Aruba 6300M 24SFP+ 4SFP56 Swch	HW	P2: Síťová infrastruktura a WiFi	
28	JL676A	Aruba	1U switch: min 48x 1Gbps 1000BASE-T bez PoE,	HW	P2: Síťová infrastruktura a WiFi	
29	JL678A	Aruba	1U switch: min 24x 1Gbps 1000BASE-T bez PoE,	HW	P2: Síťová infrastruktura a WiFi	
30	JL675A	Aruba	1U switch: min 48x 1Gbps 1000BASE-T s PoE (m	HW	P2: Síťová infrastruktura a WiFi	
31	JL677A	Aruba	1U switch: min 24x 1Gbps 1000BASE-T s PoE (m	HW	P2: Síťová infrastruktura a WiFi	
32		Aruba	metalické kabely, montážní příslušenství	HW	P2: Síťová infrastruktura a WiFi	
33		Aruba	optické kabely, 502710773 - Optický patchkabe	HW	P2: Síťová infrastruktura a WiFi	
34		Aruba	OEM transievery, SFP+ transceiver 10GBASE-LR	HW	P2: Síťová infrastruktura a WiFi	
35	FortiMail-VM04	FortiNet	FortiMail-VM04, SW virtual appliance	SW	P2: Emailová brána	
36	FortiMail-VM04	FortiNet	FortiMail-VM04, Licence, 24x7 Enterprise ATP B	SW	P2: Emailová brána	
37		Veeam	Veeam Data Platform Foundation Universal Per	SW	P2: Systém pro zálohování dat	
38		Veeam	4 additional years of Production (24/7) mainten	SW	P2: Systém pro zálohování dat	
39	HPE DL325	HPE	HPE DL325 G10+ v2 8SFF CTO Svr	HW	P2: Systém pro zálohování dat	
40	HPE MSA 2060	HPE	HPE MSA 2060 16Gb FC LFF Storage	HW	P2: Systém pro zálohování dat	
41	HPE MSA 2060	HPE	HPE MSA 2060 16Gb FC LFF Storage	HW	P2: Systém pro zálohování dat	
42	HPE MSL3040	HPE	HPE MSL3040 Scalable Base Module	HW	P2: Systém pro zálohování dat	
43	HPE SN3600B	HPE	HPE SN3600B 24/24 PP+ 24p 16G SW FC Swch	HW	P2: Systém pro zálohování dat	
44	MS WS22 16C	Microsoft	MS WS22 16C Std en/cs/pl/ru/sv SW	HW	P2: Systém pro zálohování dat	
45						
46						

47						
48						
49						
50						
51						
52						
53						
54						
55						
56						
57						
58						
59						
60						
61						
62						
63						
64						
65						
66						
67						
68						
69						
70						
71						
72						
73						
74						
75						
76						
77						
78						
79						
80						
81						
82						
83						
84						
85						
86						
87						
88						
89						
90						
91						
92						
93						
94						
95						
96						
97						

98						
99						
100						
101						
102						
103						
104						
105						
106						
107						
108						
109						
110						
111						
112						
113						
114						
115						
116						
117						
118						
119						
120						
121						
122						
123						
124						
125						
126						
127						
128						
129						
130						
131						
132						
133						
134						
135						
136						
137						
138						
139						
140						
141						
142						
143						
144						
145						
146						
147						
148						

149						
150						
151						
152						
153						
154						
155						
156						
157						
158						
159						
160						
161						
162						
163						
164						
165						
166						
167						
168						
169						
170						
171						
172						
173						
174						
175						
176						
177						
178						
179						
180						
181						
182						
183						
184						
185						
186						
187						
188						
189						
190						
191						
192						
193						
194						
195						
196						
197						
198						

Bezpečnostní požadavky v oblasti kybernetické bezpečnosti

Nemocnice Znojmo (dále jen „Objednatel") od svých Poskytovatelů (dále jen „Poskytovatel") vyžaduje dodržování těchto Bezpečnostních požadavků v oblasti kybernetické bezpečnosti

Poskytovatel bere na vědomí, že Objednatel je provozovatelem základní služby s informačním systémem základní služby v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů.

Provozovatel bere na vědomí, že je pro Objednatele v pozici významného Poskytovatele podle §2 odst. n) vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti a musí při plnění smluvního vztahu (dále jen „Předmět plnění") pro Objednatele dodržovat níže uvedené bezpečnostní požadavky.

1. OBECNÁ PRAVIDLA

1.1. Předmět plnění nesmí být zatížen žádnými faktickými ani právními vadami a musí odpovídat všem technickým požadavkům, technickým a bezpečnostním normám pro daný druh Předmětu plnění, a to jak normám závazným, tak i doporučujícím.

1.2. Zaměstnanci Poskytovatele mohou přistupovat k informačním a komunikačním prostředkům (ICT prostředky) Objednatele výhradně prostřednictvím autentizačních údajů přidělených Objednatelem (např. VPN přístup).

1.3. Poskytovatel se zavazuje dodržovat bezpečnostní opatření a pravidla Objednatele při práci s informacemi a ICT prostředky Objednatele.

1.4. Poskytovatel se zavazuje nakládat s veškerými daty, informacemi a údaji, ke kterým se dostane v rámci Předmětu plnění takovým způsobem, aby nemohlo dojít k jejich ztrátě, vyzrazení, neoprávněné či neodborné manipulaci. Dále se zavazuje používat tato data pouze k danému účelu a neumožnit jejich zpřístupnění nepovolané osobě.

1.5. Poskytovatel se zavazuje dodržovat veškerou platnou legislativu, zejména pak tu v oblasti kybernetické bezpečnosti a ochrany osobních údajů.

2. BEZPEČNOST KOMUNIKACE

2.1. V případě ztráty nebo odcizení hardware, software, dat, informací Objednatele musí Poskytovatel vždy neprodleně nahlásit tuto skutečnost oddělení IT Objednatele, a to i v případě pouhého podezření neoprávněný přístup a manipulaci s daty.

2.2. Při práci na zařízení (například: počítači, notebooku, mobilním telefonu, zdravotnickém prostředku) připojeném do sítě a/nebo k informačním systémům Objednatele musí Poskytovatel dodržovat tyto zásady:

2.2.1. umožnit přístup jen proškolenému zaměstnanci Poskytovatele,

2.2.2. chránit výpočetní techniku a všechna data Objednatele před porušením důvěrnosti, integrity či dostupnosti,

2.2.3. po ukončení práce v síti a/nebo v informačním systému Objednatele provést neprodleně odhlášení uživatele.

2.3. Při práci na serverech Objednatele musí být splněny následující zásady, které se vztahující i na servisní (provozní) smlouvy (s ohledem na specifikace informačních systémů):

2.3.1. server svěřený Poskytovateli do správy musí Poskytovatel pravidelně udržovat a kontrolovat zejména z pohledu bezpečnosti, dostupnosti a integrity dat,

2.3.2. Poskytovatel nesmí měnit jakákoliv oprávnění na serveru nebo informačním a komunikačním systému bez souhlasu oddělení IT,

2.3.3. Poskytovatel nesmí měnit nastavení operačního systému serverů a jeho komponent bez souhlasu oddělení IT,

2.3.4. Poskytovatel musí zajistit bezpečnostní aktualizaci operačního systému a aplikačních částí serverů; bezpečnostní aktualizace kritického charakteru, které mohou ohrozit bezpečnost sítě Objednatele musí aplikovat neprodleně po jejich vydání.

2.4. Při práci v interní sítí Objednatele odpovídají zaměstnanci Poskytovatele, kteří mají přidělen přístup do interní sítě Objednatele, za své činnosti prováděné v rámci této sítě. Zaměstnanci Poskytovatele nesmí, zejména:

2.4.1. zneužívat síťové prostředky pro osobní účely a zatěžovat kapacitu sítě,

2.4.2. šířit či jinak nakládat se škodlivým malwarem,

2.4.3. využívat nástroje sloužící k maskování identity,

2.4.4. provádět bezdůvodné skenování portů či jiných parametrů sítě a síťových zařízení,

2.4.5. provádět jakoukoliv formou monitorování sítě, které může vést k zachycení dat, pokud není Předmětem plnění Smlouvy,

2.4.6. obcházet autentizaci uživatele nebo obcházet zabezpečení jakéhokoliv počítače, sítě nebo uživatelského účtu,

2.4.7. provádět jakékoliv nepracovní aktivity vedoucí k omezování nebo odepírání služeb jiným uživatelům,

2.4.8. užívat jakékoliv programy, skripty nebo příkazy, nebo zasílat zprávy v jakékoliv formě s úmyslem omezit nebo znemožnit poskytování služeb nebo terminálových relací lokálně nebo přes síť, internet nebo intranet,

2.4.9. využívat bezpečnostních mezer nebo vytvářet útoky na komunikaci v počítačových sítích (např. přístup k datům, jichž není zaměstnanec zamýšleným příjemce, přihlašování na server nebo účet zaměstnancem, který není k tomuto přístupu výslovně oprávněn, s výjimkou případů, kdy tyto aktivity jsou součástí řádných pracovních úkolů),

2.4.10. předávat informace o konfiguraci a topologii sítě cizím osobám; tyto informace je oprávněn předat pouze odpovědný zaměstnanec Objednatele, pokud jsou takové informace nutné z hlediska přípravy či Předmětu plnění.

3. KYBERNETICKÉ BEZPEČNOSTNÍ UDÁLOSTI A INCIDENTY

3.1. Poskytovatel musí vyvinout maximální úsilí pro odvracení bezpečnostních hrozeb a kybernetických útoků pro informační a komunikační systémy Objednatele.

3.2. Poskytovatel musí zajistit maximální součinnost při analýze kybernetických bezpečnostních událostí a incidentů Objednatele a následně zavádět vhodná nápravná opatření určené Objednatelem.

3.3. V případě podezření či potvrzení vzniku bezpečnostní hrozby pro informační a komunikační systém Objednatele je Poskytovatel povinen neprodleně písemně (e-mailem) či telefonicky (a následně také písemně) informovat o této skutečnosti vedoucího oddělení IT Objednatele.

4. POŽADAVKY NA DODÁVENÉ INFORAMČNÝ SYSTÉMY

4.1. Informační systém musí být vytvářen tak, aby dostatečně chránil data před porušením důvěrnosti, dostupnosti a integrity.

4.2. Informační systém musí být vytvořen tak, aby byla každá operace uložena v provozním záznamu (logu) s jedinečným identifikátorem uživatele, který tuto operaci vykonal. Musí být zajištěno, aby nemohlo dojít k provádění operací pod cizím identifikátorem uživatele.

4.3. Uživatel informačního systému musí být nucen si heslo pravidelně měnit.

4.4. Informační systém musí být vytvořen tak, aby byl počet neúspěšných pokusů o přihlášení omezen. Po deseti neúspěšných pokusech o přihlášení musí být další zadávání dočasně zablokováno nebo spojení rozpojeno.

4.5. V případě, že je povolen přístup do informačního systému, v němž určuje vstupní heslo administrátor, je povinností autora informačního systému vynutit si změnu tohoto inicializačního hesla.

4.6. Poskytovatel nesmí používat jedno přihlašovací jméno pro několik svých zaměstnanců, každý účet musí být jmenný.

4.7. *V informačních systémech musí být pořizovány auditní záznamy obsahující alespoň:*

4.7.1.*identifikaci uživatele;*

4.7.2.*datum a čas přihlášení a odhlášení;*

4.7.3.*identifikaci místa, odkud se uživatel přihlašoval (pokud je to možné);*

4.7.4.*záznamy o přístupu (úspěšném i neúspěšném), případně o prováděných operacích.*

4.8. Před umožněním přístupu musí být každý uživatel identifikován a autentizován.

4.9. Informační systém by měl po určité době nečinnosti uživatele (doporučeno 15 minut) tohoto uživatele odhlásit.

4.10. Po určitém množství neúspěšných autentizačních pokusů (doporučeno 10) se musí ukončit přihlašovací proces.

4.11. V případě neúspěšné autentizace nesmí informační systém poskytnout uživateli informaci o tom, která část autentizace je chybná.

4.12. Pro každého uživatele informačního systému musí být možné identifikovat, jaká má přístupová práva.

4.13. Pro každý prostředek musí být možné vytvořit seznam uživatelů, kteří mají přístupová práva k tomuto prostředku s rozlišením druhu přístupových práv (čtení, úprava atd.).

4.14. Informační systém musí mít mechanismus pro odejmutí všech přístupových práv konkrétnímu uživateli nebo skupině.

4.15. Data vstupující do informačních systémů musí být kontrolována tak, aby byla zajištěna jejich správnost. V informačních systémech se musí evidovat identifikátor uživatele, který změny provedl. Pro kontrolu dat musí Poskytovatel aplikovat opatření:

4.15.1. vstupní kontrola (neplatné znaky, rozsah, přetečení, kompletnost, souvislost...),

4.15.2. kontrola vnitřního zpracování dat,

4.15.3. kontrola oprávněnosti běhu programů,

4.15.4. kontrola integrity dat,

4.15.5. kontrola obsahu generovaných dat.

4.16. Vývoj software musí probíhat:

4.16.1. legálním softwarem,

4.16.2. autorská a licenční ujednání musí být smluvně řešena před samotným vývojem,

4.16.3. na testovacím prostředí odděleném od prostředí produkčního,

4.16.4. na testovacích datech, která nejsou převzata z provozní databáze; pokud je nutné použít data z provozní databáze, je nutné je anonymizovat,

4.16.5. migrace do provozního prostředí může být provedena až po akceptaci výsledků testů ve vývojovém či testovacím prostředí.

5. PŘEDÁNÍ PŘEDMĚTU PLNĚNÍ

5.1. Je-li informační systém vyvíjen na zakázku, musí splňovat všechny níže uvedené body a jedná-li se o již vyvinutý informační systém, musí být tyto požadavky zohledněny v hlavní smlouvě.

5.2. Dodávka software musí být řádně smluvně zajištěna a průběžně kontrolována a dokumentována. Pokud není stanoveno ve smlouvě jinak, je Poskytovatel povinen software dodat se zdrojovými kódy.

5.3. U veškerého dodávaného programového vybavení musí být zřejmé, zda se jedná o volně šířený software nebo program podléhající licenční a registrační politice. Pracuje-li počítačový program nebo aplikace s daty, musí být specifikováno s jakými daty a musí být provedena jejich kategorizace.

5.4. Ke každé dodávce musí existovat kromě účetních dokladů i předávací protokol podepsaný Poskytovatelem a Objednatelem. Způsob předání závisí na konkrétním hardware a na smlouvě s Poskytovatelem.

5.5. Způsob předání závisí na konkrétní službě a na smluvních podmínkách dohodnutých ve Smlouvě.

5.6. Poskytovatel zajistí monitorování služby tak, aby bylo možné porovnání jejich parametrů, rozsahu a kvality stanovených Smlouvou.

5.7. Nedílnou součástí dodávky Předmětu plnění je projektová a bezpečnostní dokumentace Předmětu plnění. Rozsah a náplň dokumentace musí být specifikován ve smlouvě s Poskytovatelem. Chybějící, neúplná nebo neaktuální dokumentace je důvodem k reklamaci dodávky.

5.8. Pokud má být měněn Předmět plnění, musí Poskytovatel aktualizovat dokumentaci.

5.9. Každý dodávaný prvek Předmětu plnění musí být plně a široce Poskytovatelem otestován, zda splňuje očekávané a smluvně definované parametry, a zda jeho používání nepředstavuje neočekávaná bezpečnostní rizika (penetrační test, práce s daty).

5.10. Každý prvek Předmětu plnění je předán až podpisem písemného předávacího protokolu oprávněnými zástupci smluvních stran.

6. FYZICKÁ BEZPEČNOST

6.1. Na neveřejných pracovištích a prostorách Objednatele (např. datové centrum) není dovolen pohyb cizích osob bez dozoru zaměstnance Objednatele.

6.2. Zaměstnanci Poskytovatele mohou fyzicky přistupovat k ICT prostředkům Objednatele pouze v doprovodu oprávněné osoby Objednatele.

6.3. V případě práce Poskytovatele v prostorách Objednatele nebo v jím využívaných prostorách v datových centrech musí Poskytovatel dále dodržovat tyto zásady:

6.3.1. připojovat vlastní počítač, notebook pouze se souhlasem odpovědné osoby Nemocnice,

6.3.2. v blízkosti ICT prostředků nejíst, nepít a nekouřit.

6.4. Poskytovatel není oprávněn k výměně a odvozu použitých či vadných technologií bez autorizace Objednatele.

7. POSKYTOVÁNÍ INFORMAČNÍ TŘETÍM STRANÁM

7.1. Poskytovatel je povinen dodržovat mlčenlivost o důvěrných informacích Objednatele, které se dozvěděl při dodávce Předmětu plnění, a to i v následujících čtyřech letech po ukončení smluvního vztahu založeného Smlouvou. Důvěrnou informací Objednatele se rozumí informace obchodní, technická, osobní údaje, zdravotnická dokumentace či jiná, která je významná pro Objednatele a/nebo je konkurenčně významná a není v obchodních kruzích běžně dostupná.

7.2. Pokud Poskytovatel přijde do styku s osobními údaji, musí se řídit platnou legislativou na ochranu osobních údajů, především týkající se zpracování a předávání. Je-li zpracovatelem osobních údajů, podepíše zpracovatelskou smlouvu.

7.3. Poskytovatel může šířit informace o Předmětu plnění či o spolupráci s Objednatelem (web, medializace Poskytovatele, publikace, tisk apod.) jen s předchozím písemným souhlasem Objednatele.

8. PORUŠENÍ BEZPEČNOSTNÍ POŽADAVKŮ

8.1. Porušení těchto bezpečnostních požadavků představuje porušení Předmětu plnění. Za porušení těchto bezpečnostních požadavků může být udělena sankce v souladu s čl. 11 Smlouvy.

8.2. Pokud Poskytovatel poruší tyto bezpečnostní požadavky hrubým způsobem nebo opakovaně, je Objednatele oprávněna odstoupit od smluvního vztahu s Poskytovatelem v souladu s čl. 13 Smlouvy.

CÍLOVÝ KONCEPT

PRO SPOLEČNOST:	
DODAVATEL PROJEKTU:	
NÁZEV PROJEKTU:	
PROJEKTOVÝ MANAŽER:	
ID PROJEKTU:	
VERZE:	
DATUM SCHVÁLENÍ:	

VERZOVÁNÍ A PŘEHLED PROVEDENÝCH ZMĚN

Datum	Verze	Zpracoval	Stručný popis změn v dokumentu

OBSAH

1 ÚVOD 5

1.1 Cíl dokumentu 5
1.2 Související dokumenty 5
1.3 Použité pojmy a zkratky 5

2 DEFINICE PROJEKTU 5

2.1 Důvod realizace projektu 5
2.2 Cíl projektu 5
2.3 Výstupy 5
2.4 Bezpečnostní požadavky 5

3 NÁVRH ŘEŠENÍ 6

3.1 Aplikační a datová architektura 6
3.1.1 Aplikační architektura 6
3.1.2 Datová architektura řešení a integrace 6
3.1.3 Přístup uživatele 6
3.2 Technologická architektura 6

4 BEZPEČNOST 7

4.1 Identifikace business hrozeb a zranitelností 7
4.2 Požadavky na dostupnost, důvěrnost a integritu dat 7
4.3 Požadavky na logování událostí a bezpečnostní monitoring 7
4.4 Detekce, prevence a zvládání incidentů 7
4.5 Požadavky na hardening ICT systémů 7

5 REALIZACE A NASTAVENÍ 7

5.1.1 Autentizace a autorizace 7
5.1.2 Migrace dat 8
5.1.3 Životní cyklus 8
5.1.4 Popis release aplikace 8
5.1.5 Útlum nahrazených aplikací 8
5.2 Infrastruktura 8
5.2.1 Sizing prostředí 8
5.2.2 Technologické komponenty 8
5.2.3 Požadavky na nastavení bezpečnostníinfrastruktury 9
5.2.4 Útlum nahrazených systémů 9
5.3 Licence 9
5.3.1 Aplikační licence 9
5.3.2 Infrastrukturní licence 9

6 TESTOVÁNÍ A ŠKOLENÍ 10

6.1 Testovací scénáře 10
6.1.1 Uživatelské aplikační testy 10
6.1.2 Testy infrastruktury 10
6.1.3 Bezpečnostní a penetrační testy 10
6.2 Školení 10

7 PROVOZ SYSTÉMU 10

7.1 Plán zálohování 10
7.2 Plán dohledu 10
7.2.1 Aplikační dohled 10
7.2.2 Infrastrukturní dohled 10
7.3 Strategie obnovy 10
7.4 Patchování, upgrade 10

7.5 Aktualizace prostředí testování, školení 10
7.6 Neprodukční prostředí 10
7.7 Servisní model 10
8 ŘÍZENÍ PROJEKTU 11
8.1 Harmonogram realizace 11
8.2 Analýza rizik projektu 11
8.3 Součinnost 11
8.4 Akceptační kritéria 11
9 OTEVŘENÉ BODY 11
10 PŘÍLOHY 11
10.1 Soulad s interní řídicí dokumentací 11

1 ÚVOD

1.1 CÍL DOKUMENTU

Cílem dokumentu je vytvořit detailní podmínky pro realizaci ICT řešení. Dokument v sobě zahrnuje popis business procesů, detailní funkční, technickou, bezpečností a architektonickou specifikaci včetně akceptačních kritérií.

Dokument je určen primárně těmto osobám:

- Všem členům projektového týmu včetně zástupců objednatele a externích dodavatelů
- Provozním útvarům xxx

1.2 SOUVISEJÍCÍ DOKUMENTY

Technická specifikace nabízeného řešení

1.3 POUŽITÉ POJMY A ZKRATKY

Pojem / Zkratka	Popis

2 DEFINICE PROJEKTU

2.1 DŮVOD REALIZACE PROJEKTU

2.2 CÍL PROJEKTU

2.3 VÝSTUPY

2.4 BEZPEČNOSTNÍ POŽADAVKY

3 NÁVRH ŘEŠENÍ

3.1 APLIKAČNÍ A DATOVÁ ARCHITEKTURA

3.1.1 APLIKAČNÍ ARCHITEKTURA

3.1.1.1 Nastavení systému

3.1.1.2 Zákaznický vývoj

3.1.2 DATOVÁ ARCHITEKTURA ŘEŠENÍ A INTEGRACE

3.1.3 PŘÍSTUP UŽIVATELE

3.2 TECHNOLOGICKÁ ARCHITEKTURA

- Celková technologická architektura
- Použité technologie, verze dle standardu – rekapitulace

Technologické standardy použité v návrhu	Kategorie	Stav

- Roadmapa použitých technologií

Produkt	Aktuální verze	Mainstream Support End Date	Extended Support End Date	Service pack Support End Date

- Mapování aplikace na infrastrukutrní služby

Aplikační služba/funkcionalita	Infrastrukturní služba

Aplikační služba/funkcionalita	Infrastrukturní služba

- Mapování infrastrukturní služby na ICT Zdroje

Infrastrukturní Služba	ICT Zdroj- technologie

- Diagram prostředí a umístění
- Diagram použitých komponent a vazby
- Processing diagram z technologického pohledu
- Diagram implementace
- Komunikační diagram

4 BEZPEČNOST

4.1 IDENTIFIKACE BUSINESS HROZEB A ZRANITELNOSTÍ

4.2 POŽADAVKY NA DOSTUPNOST, DŮVĚRNOST A INTEGRITU DAT

4.3 POŽADAVKY NA LOGOVÁNÍ UDÁLOSTÍ A BEZPEČNOSTNÍ MONITORING

4.4 DETEKCE, PREVENCE A ZVLÁDÁNÍ INCIDENTŮ

4.5 POŽADAVKY NA HARDENING ICT SYSTÉMŮ

5 REALIZACE A NASTAVENÍ

5.1.1 AUTENTIZACE A AUTORIZACE

5.1.1.1 Správa identit, autentizace a SSO

5.1.1.2 Autorizační koncept

5.1.1.3 Vazba na IDM

5.1.2 MIGRACE DAT

5.1.3 ŽIVOTNÍ CYKLUS

5.1.3.1 Archivace

5.1.3.2 Skartace

5.1.4 POPIS RELEASE APLIKACE

5.1.5 ÚTLUM NAHRAZENÝCH APLIKACÍ

5.2 INFRASTRUKTURA

5.2.1 SIZING PROSTŘEDÍ

5.2.2 TECHNOLOGICKÉ KOMPONENTY

5.2.2.1 Servery

Název	Parametry

Server name	Cpus [core]	Memory [GB]	Disk [GB]	OS_arch	OS_type	OS_distribution	OS_version	Typ services

5.2.2.2 Storage

Název	Parametry

5.2.2.3 Network

5.2.2.4 Koncová zařízení

5.2.2.5 SW

- Operační systém
- Virtualizace
- Zálohování
- Dohled
- Archivace
- Databáze
- Aplikace

5.2.2.6 Ostatní požadavky

5.2.3 POŽADAVKY NA NASTAVENÍ BEZPEČNOSTNÍ INFRASTRUKTURY

5.2.4 ÚTLUM NAHRAZENÝCH SYSTÉMŮ

5.3 LICENCE

5.3.1 APLIKAČNÍ LICENCE

5.3.1.1 Vstupní předpoklady

5.3.1.2 Návrh licenčního pokrytí

5.3.2 INFRASTRUKTURNÍ LICENCE

5.3.2.1 Vstupní předpoklady

Infrastruktura	Počet

5.3.2.2 Návrh licenčního pokrytí

6 TESTOVÁNÍ A ŠKOLENÍ

6.1 TESTOVACÍ SCÉNÁŘE

6.1.1 UŽIVATELSKÉ APLIKAČNÍ TESTY

6.1.2 TESTY INFRASTRUKTURY

6.1.3 BEZPEČNOSTNÍ A PENETRAČNÍ TESTY

6.2 ŠKOLENÍ

7 PROVOZ SYSTÉMU

7.1 PLÁN ZÁLOHOVÁNÍ

7.2 PLÁN DOHLEDU

7.2.1 APLIKAČNÍ DOHLED

7.2.2 INFRASTRUKTURNÍ DOHLED

7.3 STRATEGIE OBNOVY

7.4 PATCHOVÁNÍ, UPGRADE

7.5 AKTUALIZACE PROSTŘEDÍ TESTOVÁNÍ, ŠKOLENÍ

7.6 NEPRODUKČNÍ PROSTŘEDÍ

7.7 SERVISNÍ MODEL

8 ŘÍZENÍ PROJEKTU

8.1 HARMONOGRAM REALIZACE

8.2 ANALÝZA RIZIK PROJEKTU

8.3 SOUČINNOST

8.4 AKCEPTAČNÍ KRITÉRIA

9 OTEVŘENÉ BODY

10PŘÍLOHY

10.1SOULAD S INTERNÍ ŘÍDICÍ DOKUMENTACÍ

Jedná se zejména o níže uvedené dokumenty. Navrhované řešení je v souladu s dokumenty ŘD.