Smlouva o dílo

uzavřená dle ust. § 2586 a násl. zák. č. 89/2012 Sb., občanského zákoníku (dále jen „občanský zákoník“)

Číslo smlouvy objednatele:
Číslo smlouvy zhotovitele: S-JAKA-000220

Objednatel:	**Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace**
Se sídlem:	Kamenice 798/1d, 625 00 Brno
Zastoupený:	MUDr. Hana Albrechtová, ředitelka
IČ:	00346292
DIČ:	CZ00346292

[redacted]

na straně jedné (dále jen „**objednatel**“)

a

Zhotovitel:	**YOUR SYSTEM, spol.s r.o.**
Se sídlem:	Türkova 2319/5b, Praha 4, PSČ 149 00
Zastoupený:	RNDr. Martin Nehasil, jednatel
IČ:	00174939
DIČ:	CZ 00174939
Plátce DPH:	ANO

[redacted]

Zapsaný v OR vedeném Městským soudem v Praze, 18. července 1990, oddíl C, vložka č. 72

na straně druhé (dále jen „**zhotovitel**“)

Úvodní ustanovení

1.1. Plnění této smlouvy o dílo je součástí projektu „Kybernetická bezpečnost Zdravotnické záchranné služby Jihomoravského kraje“ (dále jen „Projekt“), registrační číslo projektu reg. č. CZ.06.3.05/0.0/0.0/15_011/0006960, který je spolufinancován z výzvy č. 10 Integrovaného regionálního operačního programu (IROP) s názvem „KYBERNETICKÁ BEZPEČNOST“, prioritní osy PO 3: Dobrá správa území a zefektivnění veřejných institucí,

specifického cíle SC 3.2: Zvyšování efektivity a transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality systémů IKT.

I. Předmět smlouvy

1. Předmětem této smlouvy je závazek zhotovitele provést na svůj náklad a nebezpečí pro objednatele dílo spočívající v komplexní dodávce a implementaci technologií, dodávce SW, HW a infrastruktury pro realizaci technických bezpečnostních opatření dle § 5 odst. 3) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „ZKB“) pro zabezpečení informačních systémů provozovaných objednatelem. Konkrétně se jedná o zvýšení kybernetické bezpečnosti pro Informační systém zdravotnického operačního střediska Zdravotnické záchranné služby Jihomoravského kraje (dále jen „ZZS JMK“) a pro Informační systém Elektronická pošta dle požadavků objednatele vymezených dále v této smlouvě a vyplývajících ze zadávacích podmínek na veřejnou zakázku (dále jen „dílo“), a to řádně, bez vad a nedodělků. Podrobná specifikace díla je uvedena v příloze č. 1 a příloze č. 2 této smlouvy. Zhotovitel je povinen obstarat si vše, co je nutné k provedení díla.
2. Objednatel se zavazuje dílo převzít a zaplatit zhotoviteli za řádně a včas provedené dílo cenu ve výši a za podmínek dle této smlouvy.

II. Cena

1. Celková cena za provedení díla dle této smlouvy je sjednána v souladu s cenou, kterou zhotovitel nabídl v rámci zadávacího řízení na veřejnou zakázku.
2. Celková cena činí: 11 050 000,00 Kč bez DPH. K této částce bude připočtena DPH v platné sazbě.
3. Celková cena včetně DPH je sjednána jako závazná a nejvýše přípustná.
4. V celkové ceně jsou zahrnuty veškeré náklady zhotovitele nezbytné pro řádné a včasné provedení díla dle této smlouvy, tedy veškeré práce, dodávky, služby, poplatky, výkony a další činnosti nutné pro řádné splnění předmětu této smlouvy.

III. Platební podmínky

1. Objednatel se zavazuje zaplatit zhotoviteli cenu bezhotovostním převodem na bankovní účet zhotovitele uvedený v záhlaví této smlouvy na základě faktury vystavené zhotovitelem po řádném splnění předmětu plnění dle této smlouvy. Splatnost faktury činí 30 (kalendářních) dní od jejího prokazatelného doručení kupujícímu. K vyrovnání závazku Objednatele dojde odepsáním částky z jeho účtu ve prospěch účtu Zhotovitele
2. Zhotovitel vystaví fakturu do 7 kalendářních dnů po převzetí a akceptaci díla objednatelem v souladu s čl. V. této Smlouvy. Podmínkou pro vystavení faktury je řádné předání díla a zároveň jeho vyúčtování; přílohou faktury proto musí být soupis skutečně provedených služeb, prací apod., resp. předávací protokol dle čl. V. této smlouvy.

3. Zhotovitel se touto smlouvou zavazuje, že jím vystavená faktura bude obsahovat všechny náležitosti řádného daňového dokladu dle platné právní úpravy a informaci, že se jedná o projekt Integračního regionálního operačního programu a označení registračním číslem projektu uvedeném v úvodním ustanovení této smlouvy.
4. V případě, že účetní doklady nebudou mít odpovídající náležitosti, je objednatel oprávněn zaslat je ve lhůtě splatnosti zpět zhotoviteli k doplnění, aniž se tak dostane do prodlení se splatností. Důvody vrácení sdělí objednatel zhotoviteli písemně zároveň s vráceným daňovým dokladem. V závislosti na povaze závady je zhotovitel povinen daňový doklad včetně jeho příloh opravit nebo vyhotovit nový. Lhůta splatnosti počíná běžet znovu od opětovného zaslání náležitě doplněných či opravených daňových dokladů.

IV. Termín plnění

1. Zhotovitel se zavazuje provést dílo dle podmínek sjednaných v čl. V. této smlouvy maximálně 180 kalendářních dnů od doručení písemné výzvy objednatele k zahájení plnění. Detailní harmonogram je uveden v příloze č. 1 této smlouvy.
2. Zhotovitel se zavazuje zahájit realizaci díla ihned po nabytí účinnosti této smlouvy.

V. Místo plnění a předání díla

1. Místem plnění je sídlo objednatele na adrese Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace, Kamenice 798/1d, 625 00 Brno a Záložní zdravotnické operační středisko ZZS JMK [redacted]
2. [redacted]
3. Dílo bude provedeno jeho celkovým předáním a převzetím, a to bez vad a nedodělků v místě sídla objednatele, o čemž smluvní strany pořídí předávací protokol. Předávací protokol bude obsahovat alespoň: označení předmětu plnění (dílo), označení a identifikační údaje objednatele a zhotovitele, číslo smlouvy a datum jejího uzavření, prohlášení objednatele, že dílo přejímá, popř. nepřejímá, soupis provedených činností, datum a místo sepsání, jména a podpisy zástupců objednatele a zhotovitele. Součástí tohoto předání a převzetí je poskytnutí dokumentace skutečného provedení/stavu po implementaci, systémová dokumentace a bezpečnostní dokumentace včetně hodnocení aktiv a rizik ke dni tohoto předání a převzetí, a to na CD nebo jiném pevném disku v jednom vyhotovení.
4. Povinností zhotovitele je dodat dílo bezvadné, tzn. prosté všech vad a nedodělků.
5. Povinnost zhotovitele je splněna předáním bezvadného díla, příp. až odstraněním vad a nedodělků. V případě, že objednatel převezme dílo s drobnými vadami, dohodne se v zápise o předání a převzetí díla způsob a lhůta k jejich odstranění. Nebude-li tento termín dohodnut,

platí, že vady budou odstraněny do 10 dnů ode dne předání a převzetí díla. Nároky objednatele na zaplacení eventuálních sankcí a škod nejsou tímto dotčeny.

6. Nebudou-li vady či nedodělky odstraněny ve stanovené lhůtě, má objednatel právo nechat je odstranit 3. osobou na náklady zhotovitele. Nároky objednatele na zaplacení eventuálních sankcí a škod tímto nejsou dotčeny.

VI. Záruční podmínky

1. Zhotovitel se zavazuje objednateli poskytnout záruku za jakost na veškeré dodané technologie včetně nezbytných provozních a servisních služeb, není –li v technických podmínkách uvedena lhůta delší, v délce trvání minimálně:

   a) 60 měsíců na informační systém(y), aplikace a služby spojené s realizací díla,

   b) 36 měsíců – u HW infrastruktury a systémového SW, pokud není u konkrétního vybavení uvedeno jinak. Delší záruka je uvedena jen u částí, kde je na trhu běžné poskytování delší záruky v pořizovací ceně.

   c) 12 měsíců na spotřební materiál, případně drobné vybavení podléhající rychlému opotřebení. Případný spotřební materiál musí být explicitně označen v nabídce a smlouvě a musí být prokázáno, že splňuje tento charakter.
2. Záruka začíná běžet ode dne převzetí díla objednatelem. Veškeré opravy po dobu záruky budou bez dalších nákladů pro provozovatele (objednatele). Veškeré komponenty, náhradní díly a práce budou poskytnuty bezplatně v rámci záruky.
3. Vady musí objednatel uplatnit u zhotovitele bez zbytečného odkladu poté, co se o nich dozví.
4. Objednatel má právo zvolit následující způsob odstranění vady - opravou nebo úpravou díla, žádat přiměřenou slevu z ceny díla nebo odstoupení od této smlouvy.
5. Zhotovitel je povinen na základě připomínek objednatele k dílu, upravit řešení a doplnit řešení díla. Budou-li po předání a převzetí díla zjištěny vady či nedodělky, je zhotovitel povinen odstranit je do 10 dnů od vyhotovení předávacího protokolu, v němž jsou takové vady a nedodělky uvedeny.
6. Odstoupení od smlouvy se řídí příslušnými ustanoveními občanského zákoníku. Zhotovitel je povinen provádět dílo v souladu s touto smlouvou, požadavky objednatele, zadávacími podmínkami na veřejnou zakázku a v souladu s obecně závaznými právními předpisy. Jestliže zhotovitel tyto povinnosti vyplývající ze smlouvy poruší a nezjedná nápravu ani v dodatečné přiměřené lhůtě, jedná se o podstatné porušení smlouvy ze strany zhotovitele a objednatel má právo od smlouvy okamžitě odstoupit.

VII. Odstoupení od smlouvy

1. Kterákoliv smluvní strana může od této smlouvy odstoupit, pokud zjistí podstatné porušení této smlouvy druhou smluvní stranou.
2. Pro účely této smlouvy se za podstatné porušení smluvních povinností považuje takové porušení, u kterého strana porušující smlouvu měla nebo mohla předpokládat, že při

takovémto porušení smlouvy, s přihlédnutím ke všem okolnostem, by druhá smluvní strana neměla zájem smlouvu uzavřít; zejména

a) prodlení zhotovitele s provedením díla o více než 60 dní;
b) jestliže zhotovitel ujistil objednatele, že dílo má určité vlastnosti, zejména vlastnosti objednatelem vymíněné, anebo že nemá žádné vady, a toto ujištění se následně ukáže nepravdivým;
c) nemožnost odstranění vady díla; nebo
d) v případě, že se kterékoliv prohlášení zhotovitele uvedené v této smlouvě ukáže jako nepravdivé.

3. Objednatel je oprávněn odstoupit od smlouvy v případě, že nezíská účelovou dotaci na spolufinancování předmětu Smlouvy, a tedy nedojde k uzavření „Smlouvy o poskytnutí podpory z Integrovaného regionálního operačního programu“(nebo obdobné smlouvy nebo vydání rozhodnutí) nebo v případě, že Objednateli bude dotace krácena.
4. Odstoupení od této smlouvy musí mít písemnou formu, musí v něm být přesně popsán důvod odstoupení, podpis odstupující smluvní strany, jinak je odstoupení od této smlouvy neplatné. Tato smlouva zaniká ke dni doručení oznámení odstupující smluvní strany o odstoupení druhé smluvní straně, v pochybnostech 3. den po odeslání.
5. Odstoupení od této smlouvy se nedotýká práva na náhradu škody vzniklého z porušení smluvní povinnosti, práva na zaplacení smluvní pokuty a úroku z prodlení, ani ujednání o způsobu řešení sporů a volbě práva.

VIII. Sankce

1. Pro případ prodlení zhotovitele s termínem plnění uvedeným v článku IV. této smlouvy, se zhotovitel zavazuje uhradit objednateli smluvní pokutu ve výši 0,1 % z celkové ceny včetně DPH uvedené v čl. II této smlouvy, a to za každý i započatý den prodlení.
2. V případě prodlení objednatele s úhradou ceny je zhotovitel oprávněn požadovat po objednateli zaplacení úroků z prodlení ve výši 0,1 % z dlužné částky za každý započatý den prodlení.
3. Uplatněním práv z vad či uplatněním smluvních pokut není dotčeno právo na náhradu újmy v plné výši. Smluvní pokutu je objednatel oprávněn započíst oproti pohledávce zhotovitele.
4. Pro výpočet smluvní pokuty určené procentem je rozhodná celková cena včetně DPH.
5. Smluvní pokuta je splatná do 30 dnů ode dne doručení výzvy k jejímu zaplacení. Dnem splatnosti se rozumí den připsání příslušné částky na účet objednatele.
6. Zhotovitel je povinen nahradit objednateli v plné výši újmu, která objednateli vznikla vadným plněním nebo jako důsledek porušení povinností a závazků zhotovitele dle této smlouvy.
7. Zhotovitel uhradí objednateli náklady vzniklé při uplatňování práv z odpovědnosti za vady.

IX. Závěrečná ustanovení

1. Práva vzniklá z této smlouvy nesmí být postoupena bez předchozího písemného souhlasu druhé smluvní strany. Za písemnou formu nebude pro tento účel považována výměna e-mailových, či jiných elektronických zpráv.

2. Tato smlouva je uzavřena podle práva České republiky. Ve věcech výslovně neupravených touto smlouvou se smluvní vztah řídí občanským zákoníkemv účinném znění.
3. Smluvní strany se zavazují plně dodržovat ustanovení Nařízení (EU) 2016/679 (GDPR) vůči všem relevantním informacím získaným v rámci realizace této smlouvy a v rámci realizace této smlouvy.
4. Zhotovitel se zavazuje učinit veškeré nezbytné úkony a opatření vedoucí ke splnění všech podmínek IROP v rámci plnění svých povinností z této smlouvy, a to zejména:

    a. uchovávat veškerou dokumentaci související s realizací projektu včetně účetních dokladů nejméně do konce roku 2029,

    b. poskytovat požadované informace a dokumentaci související s realizací projektu zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, NKÚ, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.

5. Smluvní strany na sebe přebírají nebezpečí změny okolností v souvislosti s právy a povinnostmi smluvních stran vzniklými na základě této smlouvy. Smluvní strany vylučují uplatnění ustanovení § 1765 odst. 1 a § 1766 a § 2620 občanského zákoníku na svůj smluvní vztah založený touto smlouvou.

6. Nevymahatelnost nebo neplatnost kteréhokoli ustanovení této smlouvy neovlivní vymahatelnost nebo platnost této smlouvy jako celku, vyjma těch případů, kdy takové nevymahatelné nebo neplatné ustanovení nelze vyčlenit z této smlouvy, aniž by tím pozbyla platnosti. Smluvní strany se pro takový případ zavazují vynaložit v dobré víře veškeré úsilí na nahrazení takového neplatného nebo nevymahatelného ustanovení vymahatelným a platným ustanovením, jehož účel v nejvyšší možné míře odpovídá účelu původního ustanovení a cílům této smlouvy.

7. Smluvní strany si nepřejí, aby nad rámec výslovných ustanovení této 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 této smlouvy, ledaže je ve smlouvě výslovně sjednáno jinak. Vedle shora uvedeného si smluvní strany potvrzují, že si nejsou vědomy žádných dosud mezi nimi zavedených obchodních zvyklostí či praxe.

8. Smluvní strany berou na vědomí, že tato smlouva, včetně jejích případných změn a dodatků, musí být uveřejněna podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) v registru smluv, vyjma údajů, které požívají ochrany dle zvláštních zákonů, zejména osobní a citlivé údaje a obchodní tajemství a berou za tuto povinnost odpovědnost. Povinnost zveřejnit smlouvu v registru smluv zajistí objednatel.

9. Smlouva nabude platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem zveřejnění v registru smluv dle předchozího odstavce.

10. Změna nebo doplnění smlouvy může být uskutečněna pouze písemným dodatkem k této smlouvě podepsaným oběma smluvními stranami.

11. Smlouva bude vyhotovena ve dvou vyhotoveních, z nichž každá smluvní strana obdrží po jednom exemplář.

Nedílnou součástí této smlouvy jsou její přílohy:
Příloha č. 1 – Technická specifikace dodávky (jedná se o dokument, který byl přílohou č. 3 zadávací dokumentace pro veřejnou zakázku s názvem „Kybernetická bezpečnost Zdravotnické záchranné služby Jihomoravského kraje“)
Příloha č. 2 – Popis nabízeného řešení (jedná se o dokument, který byl součástí nabídky dodavatele)
Příloha č. 3 – Kalkulace nabídkové ceny (jedná se o dokument, který byl přílohou č. 5 zadávací dokumentace pro veřejnou zakázku s názvem „Kybernetická bezpečnost Zdravotnické záchranné služby Jihomoravského kraje“ a který dodavatel vyplnil v rámci podané nabídky)
Příloha č. 4 – Servisní smlouva

V Brně, dne ……..

Za objednatele:

MUDr. Hana Albrechtová
Digitálně podepsal MUDr. Hana Albrechtová
Datum: 2019.11.13 08:45:26 +01'00'

……

Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace
MUDr. Hana Albrechtová, ředitelka

V Praze dne ……..

Za zhotovitele:

RNDr. Martin Nehasil
Digitálně podepsal RNDr. Martin Nehasil
Datum: 2019.11.12 10:13:42 +01'00'

……,…..

YOUR SYSTEM, spol.s r.o.
RNDr. Martin Nehasil, jednatel

Příloha č. 3: Technická specifikace dodávky

V této příloze jsou uvedeny výchozí podmínky a požadavky na dodávku v rámci této veřejné zakázky.

OBSAH

VYUŽITÉ ZDROJE

Nejsou

SEZNAM TABULEK

SEZNAM ZKRATEK A POJMŮ

Zkratka/pojem	Význam
365x7x24	Poskytování služeb 365 dní v roce, 24 hodiny denně, 7 dnů v týdnu
ACL	Access Control List
AD	Microsoft Active Directory
AVL	Systém sledování polohy vozidel
CD / CD-ROM / DVD / USB	Datový nosič
ČR	Česká republika
DB	Databáze
DC	Datové centrum

Zkratka/pojem	Význam
EKP	Elektronická karta pacienta
EU	Evropská unie
FW	Firewall
GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob
GIS	Geografický informační systém
GUI	Grafické uživatelské rozhraní
HW	Hardware
HZS (ČR)	Hasičský záchranný sbor České republiky
ICT	Informační a komunikační technologie
IOP	Integrovaný operační program
IP	Internet Protocol
IROP	Integrovaný regionální operační program
IS	Informační systém
IT	Informační technologie
IZS	Integrovaný záchranný systém
JMK	Jihomoravský kraj
KII	Kritická informační infrastruktura
ks	Počet kusů
LAN	Lokální počítačová síť
LCT	Linkový radiový komunikační terminál radiové sítě Pegas/Matra
MS	Microsoft
MV ČR	Ministerstvo vnitra České republiky
MZD	Mobilní zadávání dat
NDIC	Národní dopravní informační centrum
NIS IZS	Národní informační systém IZS
OŘ	Operační řízení
OS	Operační systém
PČR	Policie České republiky
PD	Projektová dokumentace

Zkratka/pojem	Význam
PNP	Přednemocniční neodkladná péče
RCT	Radiový komunikační terminál radiové sítě Pegas/Matra
SaP	Síly a prostředky
SLA	Úroveň a podmínky poskytování služeb technické a technologické podpory
SMS	Krátká textová zpráva
SNMP	Simple Network Monitoring Protocol
SQL	Strukturovaný dotazovací jazyk pro práci v relačních databázích
SW	Software
TS	Technická specifikace
VPN	Virtuální privátní síť
VŘ	Výběrové řízení
VZ	Veřejná zakázka
WAF	Webový aplikační firewall
WAN	Rozsáhlá počítačová síť
ZD	Zadávací dokumentace
ZKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
ZOS	Zdravotnické operační středisko
ZVZ	Zákon o zadávání veřejných zakázek
ZZOS	Záložní zdravotnické operační středisko
ZZS	Zdravotnická záchranná služba (ve všeobecném významu)
ZZS JMK	Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace

Tabulka 1: Seznam zkratek a pojmů

1 PŘEDMĚT PLNĚNÍ

Předmětem plnění veřejné zakázky (dílem) je komplexní dodávka a implementace technologií, dodávky SW, HW a infrastruktury pro realizaci technických bezpečnostních opatření dle § 5 odst. 3) zákona č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB) pro zabezpečení IS provozovaných Zadavatelem, kterým je Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace. Součástí plnění VZ jsou dále servisní služby po dobu udržitelnosti projektu.

Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace je základní složkou IZS a v souladu s legislativou plní úkoly i v případě mimořádných událostí a krizových situací, kdy mohou být těmito událostmi/situacemi zasaženy i informační systémy (IS) ZZS JMK a došlo by tedy k omezení, případně znemožnění plnění úkolů ZZS JMK.

Konkrétně se jedná o zvýšení kybernetické bezpečnosti pro následující IS:

1. Informační systém zdravotnického operačního střediska ZZS JMK – jedná se o primární IS sloužící pro hlavní činnost ZZS JMK, tj. poskytování PNP na území Jihomoravského kraje.
2. Elektronická pošta – jedná se o hlavní informační systém (IS) ZZS JMK zajišťující komunikaci mezi zaměstnanci ZZS JMK a podporu výkonu jejich činností.

Zabezpečením uvedených informačních systémů bude zajištěna kontinuita jejich provozu i v případě projevů kybernetických bezpečnostních událostí, tj. zamezení kybernetickým bezpečnostním incidentům, a tím bude zajištěno poskytování služeb veřejné správy ze strany zaměstnanců ZZS JMK s využitím těchto IS.

Zvýšením kybernetické bezpečnosti v případě projevů kybernetických bezpečnostních událostí a zamezení kybernetickým bezpečnostním incidentům jak v době míru, tak v případě mimořádných událostí a krizových situací bude výrazně sníženo riziko omezení provozuschopnosti IS ZZS JMK vyplývajících z projevů kybernetických rizik (kybernetických bezpečnostních událostí).

Zvýšením bezpečnosti bude dosaženo nejen garantované provozování uvedených IS, ale bude zajištěna vyšší ochrana zpracovávaných osobních údajů v souladu s legislativou ČR a EU. Opatření v rámci projektu a souvisejících aktivitách budou sloužit i jako opatření v návaznosti na Nařízení evropského parlamentu a rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR).

Předmět plnění (dílo) je detailně popsán v kap. 3.1 – Předmět a rozsah dodávky.

Požadavky na servisní služby k tomuto Dílu jsou definovány v samostatném dokumentu, který je v rámci VZ samostatnou přílohou ZD a současně se stane přílohou Servisní smlouvy.

2 ČLENĚNÍ DOKUMENTU

Tento dokument obsahuje jen a pouze požadavky na dodávku a související služby (Dílo) a je členěn následovně:

- **Kapitola 3 – Požadavky na dodávky a související služby** – kapitola obsahuje požadavky na dodávky a služby (Dílo), které musí zhotovitel splnit ve svém řešení a ve své nabídce. Kapitola obsahuje základní koncept řešení, legislativní požadavky, konkrétní funkční a technické požadavky na řešení předmětu plnění v rámci VZ.
- **Kapitola 4 - Harmonogram** – kapitola obsahuje harmonogram realizace předmětu plnění VZ.
- **Kapitola 5 – Místa plnění** – kapitola obsahuje místa plnění v rámci realizace předmětu plnění VZ.
- **Kapitola 6 – Výchozí stav** – kapitola obsahuje popis výchozího stavu pro realizaci předmětu VZ, tj. uvedení seznamu dotčených subjektů, jejich vztah k předmětu VZ, informační a komunikační technologie a vybavení, kterými subjekty disponují nebo které budou k dispozici pro realizaci VZ, případně další organizační a technické podmínky, které jsou důležité pro realizaci VZ.

Uvedené kapitoly a jejich obsah jsou uvedeny dále v tomto dokumentu.

Požadavky na servisní služby k tomuto Dílu jsou definovány v samostatném dokumentu, který v rámci VZ je přílohou ZD a současně se stane přílohou Servisní smlouvy.

3 POŽADAVKY NA DODÁVKY A SOUVISEJÍCÍ SLUŽBY

V této kapitole jsou uvedeny požadavky na dodávky a související služby v rámci této VZ.

3.1 PŘEDMĚT A ROZSAH DODÁVKY

Předmětem dodávky je komplexní dodávka a implementace technologií, dodávky SW, HW a infrastruktury pro realizaci technických bezpečnostních opatření dle § 5 odst. 3) zákona č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB) pro zabezpečení IS provozovaných Zadavatelem, kterým je Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace.

Cílem projektu je zvýšení kybernetické bezpečnosti pro následující IS:

1. Informační systém zdravotnického operačního střediska ZZS JMK – jedná se o primární IS sloužící pro hlavní činnost ZZS JMK, tj. poskytování PNP na území Jihomoravského kraje.
2. Elektronická pošta – jedná se o hlavní informační systém (IS) ZZS JMK zajišťující komunikaci mezi zaměstnanci ZZS JMK a podporu výkonu jejich činností.

Detailní popis IS je uveden v kap. 6.2 – Informační a komunikační systémy k zabezpečení.

Předmětem projektu je realizace následujících technických bezpečnostních opatření pro zabezpečení IS ZZS JMK (písmena odpovídají ZKB):

b) nástroj pro ochranu integrity komunikačních sítí

c) nástroj pro ověřování identity uživatelů

h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

i) aplikační bezpečnost

Rozsah dodávky je uveden v následující kapitole.

3.1.1 Rozsah dodávky

Rozsah dodávky je následující:

#	Položka rozpočtu	Počet	Stručný popis položky
1	FireWall s IPS pro ZZOS	1 ks	Dodávka Firewallu s IPS pro ochranu interní sítě ZZS proti útokům z externích sítí v ZZOS včetně pokročilých funkcí inspekce provozu. Součástí je dodávka, instalace, nastavení, propojení s dalšími síťovými prvky, implementace nastavení a pravidel a napojení na systém pro sběr dat a vyhodnocení kybernetických bezpečnostních událostí a související služby.
2	FireWall pro ochranu segmentů ZOS	1 ks	Dodávka Firewallu pro ochranu segmentů ZOS v primární lokalitě. Součástí je dodávka, instalace, nastavení, propojení s dalšími síťovými prvky, implementace nastavení a pravidel a napojení na systém pro sběr dat a vyhodnocení kybernetických bezpečnostních událostí a související služby.

#	Položka rozpočtu	Počet	Stručný popis položky
3	L3 switche pro ZZOS	2 ks	Dodávka L3 switchů do lokality ZZOS pro zajištění segmentace sítí v lokalitě ZZOS. Součástí je dodávka, instalace, nastavení, propojení s dalšími síťovými prvky, implementace nastavení a pravidel a napojení na systém pro sběr dat a vyhodnocení kybernetických bezpečnostních událostí a související služby.
4	Aplikační firewall pro IS ZOS	1 ks	Dodávka aplikačního firewallu pro IS ZOS který bude chránit webové služby před potenciálními útočníky, kteří by mohli využít zranitelná místa aplikací nebo protokolů pro sledování nebo modifikaci dat nebo ohrožení chodu takové aplikace. Součástí je dodávka, instalace, nastavení, implementace nastavení a pravidel a napojení na systém pro sběr dat a vyhodnocení kybernetických bezpečnostních událostí a související služby.
5	Systém analýzy bezpečnostních logů (SW)	1 soubor	Dodávka SW nástroje pro sběr dat a vyhodnocení kybernetických bezpečnostních událostí včetně integračního rozhraní pro napojení informačních systémů, HW a síťové infrastruktury, systémového SW a technologií. Součástí je dodávka, instalace, nastavení, implementace a související služby včetně konfigurace systémových konfigurací aktivních prvků, Operačních systémů a elektronické pošty.
6	Infrastruktura (HW) pro systém analýzy bezpečnostních logů (HW)	1 soubor	Infrastruktura (HW) pro Systém analýzy bezpečnostních logů (SW) (SW nástroj pro sběr dat a vyhodnocení kybernetických bezpečnostních událostí). Jedná se o diskové pole, server, implementaci a související služby.
7	Systémový SW pro systém analýzy bezpečnostních logů (SW)	1 soubor	Systémový SW pro Systém analýzy bezpečnostních logů (SW) (SW nástroj pro sběr dat a vyhodnocení kybernetických bezpečnostních událostí). Jedná se o operační systémy, případně databázový SW, případně jiný SW nezbytný pro běh systému, implementaci a související služby.
8	Úpravy IS ZOS	1 soubor	Úpravy IS ZOS v následujícím rozsahu: 1. pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů. 2. Autentizace uživatelů operačního řízení prostřednictví AD. 3. Integrace na personální systém. 4. Monitoring a reporting a přístupů. Součástí je dodávka úprav, implementace, nastavení a

#	Položka rozpočtu	Počet	Stručný popis položky
			napojení na systém pro sběr dat a vyhodnocení kybernetických bezpečnostních událostí a související služby.
9	Konfigurace systému elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů	1 soubor	Konfigurace systému elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů. Součástí je dodávka úprav nastavení, implementace, nastavení a napojení na systém pro sběr dat a vyhodnocení kybernetických bezpečnostních událostí a související služby.
10	Dvoufaktorová autentizace administrátorských VPN přístupů	1 soubor	Dodávka a zavedení nástrojů pro dvoufaktorovou autentizaci administrátorských VPN přístupů Součástí je dodávka, implementace, nastavení a napojení na systém pro sběr dat a vyhodnocení kybernetických bezpečnostních událostí a související služby.
11	Nástroje pro bezpečnostní audit a penetrační testy	1 soubor	Dodávka nástrojů pro bezpečnostní audit a testy zranitelnosti pro penetrační testy v souladu se standardy ZKB a závěrečných testů zranitelnosti z externí sítě na systémy IS ZOS a Elektronickou poštu a následné periodické testování bezpečnostních zranitelností systémů, které komunikují s externími subjekty. Součástí je dodávka, instalace, nastavení, implementace a související služby.
12	Bezpečnostní audit a penetrační testy	1 soubor	Bezpečnostní audit a penetrační testy v souladu se standardy ZKB a závěrečných testů zranitelnosti z externí sítě na systémy IS ZOS a Elektronickou poštu.

Tabulka 2: Předmět a rozsah dodávky

3.1.2 Související služby a náležitosti dodávky

Součástí dodávky jsou dále následující služby a náležitosti:

1. Projektové řízení dodávky řešení
2. Zpracování návrhu dodávky a konfigurace technických opatření – konkretizace implementačního postupu, přesné konfigurace a instalačního a montážního návrhu řešení z nabídky a související konzultace.
3. Dodávka, implementace, instalace, zapojení a konfigurace technických opatření.
4. Konfigurační změny zabezpečovaných IS a implementace změn informačních systémů a jejich součástí.
5. Výchozí import datových zdrojů a metadat do systému (initial load, bude-li třeba).
6. Ověření funkčnosti dodaných technologií, zabezpečovaných IS a jejich součástí.
7. Provedení bezpečnostního auditu.
8. Provedení penetračních testů.

9. Dodávka dokumentace dodaného vybavení a jeho částí (min. administrátorská dokumentace, dokumentace skutečného provedení/stavu po implementaci, systémová dokumentace, zpracování bezpečnostní dokumentace včetně hodnocení aktiv a rizik). Dokumentace může být jedním dokumentem, nicméně musí obsahovat všechny relevantní informace.
10. Seznámení s obsluhou dodávaného systému a jeho budoucím provozem.
11. Zařazení do provozního prostředí objednatele (dohled, zálohování apod.).
12. Provedení zkušebního provozu.
13. Poskytnutí záruky min. 5 roky na vybavení v rámci technických opatření.

Doplňující požadavky na implementaci:

1. Zajištění kontinuity provozu ZZS JMK. Po stránce nepřetržitého provozu ZZS JMK předpokládá pouze plánovanou odstávku pouze na nezbytnou dobu.
2. Požaduje se kontinuita nastavených parametrů IS a existujících technologií a jiných aspektů provozu. Nepředpokládá investici do opětovného zadávání a pořizování těchto údajů.

3.1.3 Dodávkou nedotčené oblasti stávajícího řešení

Dodávkou nebudou dotčeny následující oblasti stávajícího řešení:

1. Současné systémy, technologie a pracoviště stávajícího zdravotnického operačního střediska (ZOS) zůstanou zachovány a nebudou negativně dotčeny realizací projektu.

3.1.4 Vyloučení z dodávky

Předmětem dodávky není:

1. Zajištění v rámci požadavků neuvedené komunikační infrastruktury (sítě apod.) mezi jednotlivými prvky systému.
2. Infrastruktura, HW a systémový SW poskytovaný Objednatelem (ZZS JMK) uvedený ve výchozím stavu a neuvedený v požadavcích.
3. Spotřební materiál využívaný v následném provozu informačních systémů neuvedený v rámci požadavků.

Koncept řešení, principy a požadavky na dodávky a služby jsou uvedeny dále v tomto dokumentu.

3.2 VÝCHODISKA A PŘIPRAVENOST

Pro řešení jsou stanovena následující východiska:

#	Popis východiska
1.	Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace je základní složkou IZS a v souladu s legislativou plní úkoly i v případě mimořádných událostí a krizových situací, kdy může být těmito událostmi/situacemi zasaženo i zdravotnické operační středisko (ZOS) a došlo by tedy k omezení, případně znemožnění poskytování úkolů ZZS JMK. Z uvedeného plyne, že informační systémy podporující procesy poskytování PNP ze strany ZZS JMK musí být poskytovat své funkcionality i v případě mimořádných událostí a krizových situací, kdy může být těmito událostmi/situacemi zasaženo i zdravotnické operační středisko (ZOS).
2.	Současné řešení bylo realizováno v roce 2015 v projektu „Krajský standardizovaný projekt zdravotnické záchranné služby Jihomoravského kraje“, který byl Jihomoravským krajem realizován

#	Popis východiska
	pro Zdravotnickou záchrannou službu Jihomoravského kraje (ZZS JMK) v rámci Integrovaného operačního programu (IOP), výzvy č. 11. Současné řešení musí plnit podmínku zajištění udržitelnosti projektu „Krajský standardizovaný projekt zdravotnické záchranné služby Jihomoravského kraje“ min. do roku 2021. Současné řešení není možné nahradit, jen modernizovat při zachování funkcionality a min. vybavení dodaných v rámci uvedeného projektu v roce 2015.
3.	Připravenost datového centra bude zajištěno min. v následujícím rozsahu: 1. Dostatečně kapacitní napájení datového centra pro umístění technologií. 2. Klimatizace v datovém centru. 3. Strukturovaná kabeláž v rámci DC a mezi dodávanými technologiemi a zabezpečovanými IS. 4. Napojení na ostatní komunikační technologie.
4.	Nutnost zajištění ochrany osobních údajů a bezpečnosti v souladu s legislativou a moderními principy – Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob (GDPR), zákona č. 181/2014 Sb. – Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a požadavky kladené na KII.

Tabulka 3: Východiska

Další východiska jsou definována výchozím stavem uvedeným v kap. 6 – Výchozí stav.

3.3 ZÁKLADNÍ POŽADAVKY NA ZABEZPEČENÍ IS

Základní požadavky na požadované řešení jsou následující:

1. Předmětem je zabezpečení následujících informačních systémů:
   a. Informační systém zdravotnického operačního střediska ZZS JMK – jedná se o primární IS sloužící pro hlavní činnost ZZS JMK, tj. poskytování PNP na území Jihomoravského kraje.
   b. Elektronická pošta – jedná se o hlavní informační systém (IS) ZZS JMK zajišťující komunikaci mezi zaměstnanci ZZS JMK a podporu výkonu jejich činností.
2. Budou zajištěny všechny současné integrace uvedených IS a vazby na jiné IS a technologie nezbytné pro provoz ZZS JMK.
3. Zajištění ochrany osobních údajů a bezpečnosti v souladu s legislativou a moderními principy – Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob (GDPR), zákona č. 181/2014 Sb. – Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a požadavky kladené na KII.
4. Izolovanost informačních systémů – přístup do systémů a přístup ze systémů ven je možný pouze přes definované přístupové body.
5. Vysoká dostupnost bezpečnostních technologií.

Detailní popis požadavků na dodávky je uveden v následující kapitole.

3.4 POŽADAVKY NA DODÁVKY

V této kapitole jsou uvedeny požadavky na dodávky.

3.4.1 Obecné a společné požadavky

V této kapitole jsou uvedeny obecné požadavky na požadované řešení:

#	Požadavek
P.1	Dodávané technologie musí svojí architekturou splňovat obecné zásady informační bezpečnosti v míře, odpovídající charakteru užití a kategorii zpracovávaných dat (GDPR).
P.2	Veškeré nabízené SW i HW prvky musí být plně kompatibilní se stávajícími systémy a technologiemi ZZS JMK.
P.3	Součástí implementace musí být i veškeré potřebné licence a služby nezbytné pro dodávku a provoz dodávaných technologií min. po dobu účinnosti servisní smlouvy.
P.4	Zaručená perspektiva rozvoje a podpory je minimálně po dobu dalších 6 let od uvedení do provozu.
Legislativa a další normy	
P.5	Soulad s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob (GDPR – General data protection regulation) v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
P.6	Soulad se Zákonem č. 181/2014 Sb., o kybernetické bezpečnosti v aktuálním znění a vyhláškou Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti v aktuálním znění.
P.7	Soulad s prováděcím nařízením Komise (EU) 2018/151 ze dne 30. ledna 2018, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný (dále jen "PNK").
P.8	Soulad se Zákonem č. 239/2000 Sb. o integrovaném záchranném systému a o změně některých zákonů v aktuálním znění.
P.9	Soulad se Zákonem č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů v aktuálním znění.
Ostatní obecné požadavky	
P.10	Zajištění jednotného času na všech technologiích a zařízeních (synchronizace s time serverem).

Tabulka 4: Obecné požadavky

Pro konkrétní oblasti jsou uvedeny specifické požadavky samostatně v dílčích podkapitolách.

3.4.2 FireWall s IPS pro ZZOS

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.11	Dodávka firewallu s IPS pro řízení bezpečného přístupu mezi vnějšími sítěmi (Internet, NIS IZS, PČR atd.) a vnitřní sítí ZZOS a ZOS.

P.12	Dodávka FireWallu pro záložní ZOS:
	• FireWall bude oddělovat externí sítě připojené v rámci záložního ZOS (internet apod.)
	• Stavový aplikační firewall jako samostatné HW zařízení, který musí nabízet
	  ○ Dynamický a statický NAT/PAT (překlad IP adres)
	  ○ Podporu dynamických směrovacích protokolů RIP, OSPF, BGP a Policy based Routing
	  ○ Plnou podporou protokolu IPv6
	  ○ Podpora redundance pro případ výpadku ve formě Active/Active failover, Active/Standby failover (redundantní prvek není součástí dodávky)
	  ○ Podpora filtrace IPv4, IPv6 a filtrace podle identity uživatele nebo jeho skupiny definované v AD
	• Aplikační firewall
	  ○ Pokročilá hloubková analýza dat na aplikačních vrstvách ISO modelu
	  ○ Podpora pasivního monitorování (TAP režim)
	  ○ Rozeznávání a kategorizace aplikací, geografických lokalit, uživatelů
	  ○ Možnost rozšíření o identifikace a zamezení přístupu na nedůvěryhodné či škodlivé webové stránky – filtrace podle reputace serverů
	  ○ Security Inteligence database – známé adresy anonymních proxy, otevřených mail relay, uzly botnet sítí
	  ○ Možnost integrovat vlastní reputační databáze
	• IPS senzor, který musí nabízet
	  ○ Možnost definovat typ provozu předávaný k inspekci do IPS
	  ○ Možnost obejití IPS funkcí při zahlcení nebo nedostupnosti
	  ○ IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií
	  ○ Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s reputací
	  ○ IPS musí umět detekovat a blokovat útoky průzkumných aktivit
	  ○ IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS
	  ○ IPS musí umět detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host“ jako je spyware, phishing nebo Botnet C&C
	  ○ aktuálních databázích AV dodavatelů
	  ○ Ochrana před malware typu „zero day attack“ které nelze detekovat tradičními antiviry
	  ○ Retrospektivní ochrana prostředí – pokud SW kód je později detekován jako malware, je na to IPS schopna reagovat
	  ○ Podpora databází reputací adres v internetu (Security Intelligence)
	• VPN koncentrátor
	  ○ Zakončení „full-tunnel“ IPSec nebo SSL VPN pro alespoň 300 současné připojených uživatelů – licence pro 25 uživatelů
	  ○ Možnost rozšíření (licence apod.) „odlehčené“ SSL VPN pro uživatele formou

#	Požadavek
	zabezpečeného přístupu na webový portál bez nutnosti tlustého klienta ○ Zakončení alespoň 300 současně připojených site-to-site IPsec tunelů ○ Implementace IPsec musí podporovat protokoly IKEv1 i IKEv2 a šifrovací standardy 3DES/AES a algoritmy nové generace popsané ve standardu NSA Suite-B • Výkonnostní parametry a provedení ○ Minimální propustnost NGFW (hloubková inspekce) 850 Mbps ○ Minimální propustnost NGFW (hloubková inspekce + IPS modulem) minimálně 450 Mbps. ○ Minimální propustnost pro IPsec VPN komunikaci (šifrování 3DES/AES) 250 Mbps ○ Formát zařízení Appliance v provedení do racku max 2RU ○ Samostatný port pro management ○ Minimální 8 portů pro data 10/100/1000 BaseT Ethernet ○ Podporovaný počet VLAN min. 100 Součástí dodávky je implementace (montáž, instalace, konfigurace, zaškolení a seznámení s funkcionalitami a obsluhou, dokumentace) Podpora na 5 let typu NBD, oprava v místě instalace zařízení včetně aktualizací v šech signatur a SW komponent včetně jejich funkčnosti.
P.13	Umístění firewallu s IPS do DC v rámci záložního zdravotnického operačního střediska.
P.14	Nastavení pravidel pro kontrolu přístupu do segmentů IS ZOS a ZZOS z externích sítí a kontrolovat ho před případnými externími i interními útoky. Konfigurace FireWallu bude realizována na základě požadavků ZZS s přihlédnutím ke konfiguraci stávajících oprávnění v rámci centrálního FireWallu v ZOS. Nastavení bude umožňovat bezproblémový chod IS OŘ ze ZZOS (stávajících technologií) včetně využití připojení k externím sítím v ZZOS (Internet apod.). Pro konfiguraci přístupu vzdálených uživatelů v rámci VPN bude využito stejné konfigurace jako v primární lokalitě ZOS v době implementace FW (centrální RADIUS serverů), tak aby byla umožněna jednotná konfigurace těchto přístupů bez ohledu na lokalitu přístupu. *Konfigurace stávajících firewallů a nastavení sítě budou poskytnuty v rámci implementační analýzy.*
P.15	Výchozí nastavení pravidel pro alertování upozorňující na bezpečnostní události detekované na tomto bezpečnostním prvku. *Bezpečnostní alerty v rámci IS ZOS budou definovány a konfigurovány na základě požadavků ZZS v rámci implementační analýzy.*
P.16	Napojení a předávání alertů a logů do Systému analýzy bezpečnostních logů (viz kap. 3.4.6). Včetně specifikace korelace kritických bezpečnostních alertů z tohoto bezpečnostního prvku týkajících se IS ZOS.
P.17	Dodávka FireWallu jako kompaktního zařízení, tj. HW včetně vnitřního SW zajišťujícího všechny požadované funkcionality. Pro případný podpůrný SW sloužící pro instalaci, konfiguraci a aktualizace FW ZZS umožní využití stávající virtualizační infrastruktury ZZS za předpokladu, že nepřesáhne požadavek na jeden server

#	Požadavek
	(4 vCPU, 8 GB RAM a 500 MB vHD, OS MS Windows Server 2016 Standard nebo Linux). V případě vyšších požadavků na server dodavatel dodá i nezbytný HW a systémový SW včetně licencí pro běh podpůrného SW (HW ve verzi rack mount).
P.18	Možnost aktivace/deaktivace izolace systému IS ZOS od externích sítí nebo i od interních LAN/WAN segmentů ze systému IS OŘ (viz kap. 3.4.8 – Úpravy IS ZOS). Vlastní izolace bude provedena na firewallech v rámci ZOS (součinnost poskytne ZZS) a ZZOS (součástí dodávky).
P.19	Bude proveden detailní záznam událostí izolace systému IS ZOS včetně jejich časové souslednosti, případně o uživatelích, kteří opatření realizovali, a to jak do logu IS OŘ, tak do Systému analýzy bezpečnostních logů (viz kap. 3.4.6).

Tabulka 5: FireWall s IPS pro ZZOS

3.4.3 FireWall pro ochranu segmentu ZOS

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.20	Dodávka Firewallu pro ochranu segmentů ZOS v primární lokalitě.
P.21	FireWall pro ochranu segmentu ZOS musí plnit min. parametry stejné jako FireWall s IPS pro ZZOS s výjimkou že nejsou požadovány vlastnosti VPN koncentrátoru. Dále jsou požadovány následující výkonnostní parametry: • Minimální propustnost NGFW (hloubková inspekce) 2 000 Mbps • Minimální propustnost NGFW (hloubková inspekce + IPS modulem) 800 Mbps.
P.22	Umístění firewallu do DC v rámci primárního zdravotnického operačního střediska.
P.23	Implementace v pasivním módu s možností implementace fyzického oddělení segmentu IS ZOS
P.24	Výchozí nastavení pravidel pro alertování upozorňující na bezpečnostní události detekované na tomto bezpečnostním prvku. *Bezpečnostní alerty v rámci IS ZOS budou definovány a konfigurovány na základě požadavků ZZS v rámci implementační analýzy.*
P.25	Napojení a předávání alertů a logů do Systému analýzy bezpečnostních logů (viz kap. 3.4.6). Včetně specifikace korelace kritických bezpečnostních alertů z tohoto bezpečnostního prvku týkajících se IS ZOS.
P.26	Dodávka FireWallu jako kompaktního zařízení, tj. HW včetně vnitřního SW zajišťujícího všechny požadované funkcionality. Pro případný podpůrný SW sloužící pro instalaci, konfiguraci a aktualizace FW ZZS umožní využití stávající virtualizační infrastruktury ZZS za předpokladu, že nepřesáhne požadavek na jeden server (4 vCPU, 8 GB RAM a 500 MB vHD, OS MS Windows Server 2016 Standard nebo Linux). V případě vyšších požadavků na server dodavatel dodá i nezbytný HW a systémový SW včetně licencí pro běh podpůrného SW (HW ve verzi rack mount).

Tabulka 6: FireWall pro ochranu segmentu ZOS

3.4.4 L3 switche pro ZZOS

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.27	Dodávka centrálního L3 switche ZZOS složeného ze dvou vzájemně propojených switchů pro segmentaci LAN sítí ZZOS.
P.28	L3 switche musí plnit následující min. parametry (každý jeden switch): 1. provedení rack mount 2. ethernetový spravovatelný přepínač vrstvy 3 3. min. 24x 10/100/1000Mbs portů a min. 4x 10Gb SFP/SFP+ na jeden switch 4. propojení switchů do jednoho stacku (přepínače se chovají jako jeden z pohledu managementu i připojených zařízení – včetně automatického loadbalancingu) vysokorychlostním redundantním propojením min. 80Gbps. 5. software podporující CLI (Telnet/SSH), SNMP management, včetně omezení přístupu na management z definovaných adres a subnetů, 6. podpora Jumbo Frames, min. 9 kB, podpora agregace portů (LACP) s využitím dvou switchů ve stacku (jedna agregace pře dva switche), 7. access listy (access control lists – ACL) aplikovatelné na IP L2 a L3 pro filtrování provozu; podpora globálních ACL, VLAN ACL, port ACL, a podpora IPv6 ACL, 8. bezpečnost – port security a implementace 802.1X, automatické zařazování do VLAN 802.1x – RADIUS server Windows AD, 9. šifrování na L2 dle IEEE 802.1AE (min. uplink porty), 10. podpora IPv4 a IPv6, 11. implementace (montáž, instalace, konfigurace, seznámení s funkcionalitami a obsluhou, dokumentace) 12. záruka 5 let.
P.29	Umístění L3 switchů do DC v rámci záložního zdravotnického operačního střediska.
P.30	Propojení do stávající infrastruktury, která zajišťuje propojení lokalit ZOS a ZZOS. (viz kap. 6.4).
P.31	Napojení a předávání alertů a logů do Systému analýzy bezpečnostních logů (viz kap. 3.4.6). Včetně specifikace korelace kritických bezpečnostních alertů z tohoto aktivního prvku týkajících se IS ZOS.

Tabulka 7: L3 switche pro ZZOS

3.4.5 Aplikační firewall pro IS ZOS

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.32	Dodávka webového aplikačního firewallu pro zabezpečení webových služeb (web services) v rámci externí komunikace IS ZOS. Minimálně následující aplikace: • Endpoint NIS IZS (SOS5) – publikováno do sítě NIS IZS

#	Požadavek
	• SOSView a SOSnow služby – publikováno do sítě Internet Jedná se o služby IS ZOS dostupné z externích sítí.
P.33	Funkcionalita webového aplikačního firewallu (WAF) bude poskytovat ochranu webových aplikací před kybernetickými útoky s využitím pozitivní i negativní bezpečnostní logiky v bezpečnostních politikách (detekci a ochranu před známými útoky a povolení explicitního legitimního provozu s minimální propustností 200Mbps. K těmto základním bezpečnostním politikám požadujeme implementaci dalších dodatečných bezpečnostních vlastností, jako je ochrana před útoky prolomením logovacích URL hrubou silou (Brute Force útoky) s možností eskalace a potlačení technologií CAPTCHA v případě podezření, že je aplikace pod útokem.
P.34	Je požadováno, aby WAF obsahoval technologie pro detekci a potlačení robotických (nelidských) uživatelů s možností výjimek (např. pro legitimní robotické klienty). WAF také zajistí ochranu před únosy HTTP relací. WAF musí podporovat SSL terminaci.
P.35	Aplikační firewall musí plnit následující min. parametry: 1. Ochrana proti aplikačním DoS a DDoS útokům (SlowLoris, R.U.D.Y, ApacheKiller, SSL útoky, SYN flood, HTTP flood aj.) 2. Ochrana proti "forcefull browsing", XSS, SQL-INJ, CSRF, remote command execution a ostatním útokům podle OWASP Top 10 3. Ochrana proti manipulaci s cookies 4. Ochrana parametrů webové aplikace 5. Session Management – ochrana proti únosům relací 6. Brute Force Ochrana – ochrana před prolomení hrubou silou 7. Detekce a potlačení robotických uživatelů aplikace 8. Ochrana AJAX a JSON aplikací, zabezpečení XML komunikace 9. Možnost rozšíření o detekci a ochranu před robotickými klienty pro nativní mobilní aplikace IOS a Android 10. Blokování požadavků z podezřelých prohlížečů (proaktivní ochrana proti botnetům) 11. Automatická instalace a aktualizace databáze pro detekci útoků, botnetů nebo kampaní kybernetických útoků 12. Blokování útočníků na základě geolokace 13. Podpora různých typů reportů – PCI, geolokační reporty, OWASP Top 10 14. Identifikace zařízení a potlačení škodlivých zařízení v bezpečnostní politice (fingerprinting) 15. Podpora rozkládání zátěže na více než 3 servery a podpora různých typů mechanismů rozkladu zátěže, minimálně kruhová metoda (round-robin), vážená kruhová metoda s (weighted round-robin) podle počtu spojení 16. Podpora zajištění konektivity uživatelů k serveru (persistence) na základě IP adresy, HTTP cookie 17. Podpora REST API pro správu a monitoring zařízení 18. Možnost doprogramovat filtrovací pravidla pro aplikace 19. Ochrana proti L7 DDoS útokům, web scrapingu a útokům pomocí hrubé síly (brute force), mitigace DDoS útoků založená na behaviorální analýze 20. Podpora SSL (šifrování a dešifrování)

#	Požadavek
	21. Povoleni jednotlivých HTTP metod pro jednotlivá URL 22. Detekce anomálií a podezřelých operacích na aplikační vrstvě 23. implementace (instalace, konfigurace, seznámení s funkcionalitami a obsluhou, dokumentace) 24. záruka a aktualizace SW apod. na 5 let.
P.36	Implementace WAF na externě dostupné aplikace IS ZOS včetně jejich optimalizací a nastavení pravidel optimalizovaných pro chod těchto aplikací/rozhraní s ohledem na jejich funkčnost a dostupnost s detailní znalostí těchto aplikací/rozhraní.
P.37	Pro chod aplikačního FW je možné využít jak HW, který bude součástí dodávky řešení (viz kap. 3.4.7) nebo i stávající virtualizační infrastruktury ZZS za předpokladu, že nepřesáhne požadavek na jeden server (4v CPU, 8 GB RAM a 100 GB HD, OS MS Windows Server 2016 Standard nebo Linux). V případě vyšších požadavků na server dodavatel dodá i nezbytný HW a systémový SW včetně licencí pro běh FW (HW ve verzi rack mount).
P.38	Umístění aplikačního firewallu do DC v rámci primárního zdravotnického operačního střediska. S možností migrace do ZZOS v případě plné aktivace ZZOS (s možností využití stávající virtualizační platformy ZZOS).
P.39	Napojení a předávání alertů a logů do Systému analýzy bezpečnostních logů (viz kap. 3.4.6). WAF musí podporovat logování ve formátu minimálně Syslog, a případně s navrženým logovacím systémem (viz kap. 3.4.6). Součástí předávání logů do Systému analýzy bezpečnostních logů musí být veškeré kritické bezpečnostní události související s chráněnými aplikacemi ZOS a případných útocích na ně vedených. Součástí předávaných logů musí být také varování před nestandartními stavy jako jsou anomální nárůsty požadavků, pokusy o přístup do nepublikovaných částí aplikací apod. WAF musí dále předávat logy o veškerých přístupech (úspěšné i neúspěšné) do managementu WAF a informace o změnách konfigurací WAF.

Tabulka 8: Aplikační firewall pro IS ZOS

3.4.6 Systém analýzy bezpečnostních logů (SW)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.40	Dodávka SW nástroje pro sběr dat (logů, alertů a dalších vstupů) a vyhodnocení kybernetických bezpečnostních událostí ze zabezpečovaných informačních systémů, infrastruktury, HW, systémového SW a technologií včetně IS ZOS a systému elektronické pošty. Systém bude sdružovat záznamy o událostech z jednotlivých aplikačních modulů IS ZOS, elektronické pošty a z okolí uvedených systémů (to je ze všech důležitých zařízení, systémů, sítě LAN/WAN a navazujících aplikací). Tyto záznamy bude ukládat a bude tyto záznamy dávat do souvislostí – korelovat a zajistí tak okamžitou detekci nebezpečného, případně nestandardního chování právě v IS ZOS, systému elektronické pošty nebo jejich infrastruktury.

#	Požadavek
P.41	Pro sběr dat z OS a DB serverů IS ZOS a elektronické pošty požadujeme minimálně následující události: • Přihlášení • Odhlášení • Neúspěšné pokusy o přihlášení Ukládání sesbíraných dat do úložiště nástroje pro následnou analýzu.
P.42	Zpracování (korelace) záznamů s cílem detekce nebezpečného, případně nestandardního chování v zabezpečovaných IS infrastruktury, infrastruktury, HW, systémového SW a technologií.
P.43	Zpracování bezpečnostních logů z IS ZOS a jeho komunikačních modulů/aplikací a elektronické pošty tak, aby bylo možné jej využít k identifikaci a korelaci bezpečnostních incidentů, a to nejenom na úrovni přístupů, včetně možnosti zablokování, ale i chování uživatele v rámci aplikace,
P.44	Minimální požadavky na systém analýzy bezpečnostních logů: 1. podporované protokoly: Syslog, Windows Events Collection (WinRM/RPC), FTP, S/TP/SCP, SNMP, ODBC/JDBC, CP-LEA, SDEE, 2. bezagentový sběr logů (sběr bez nutnosti instalovat agenta na cílový systém), 3. licence pro zpracování 300 EPS (událostí za sekundu) s možností rozšíření až na 5000 EPS, 4. možnost řešení jak prostřednictvím VirtualAppliance nebo samostatným HW, 5. počet zdrojů pro sběr logů minimálně 150, 6. možnost sběru logů samostatným lokálním kolektorem s přeposíláním do centrálního systému, 7. možnost záložního uložení logů (rozšiřitelné úložiště neodpovídá tomuto požadavku), 8. centrální management všech komponent a administrativních funkcí ve webovém uživatelském rozhraní, 9. možnost definovat uživatelům systému přístup k jednotlivým zařízením, jejich skupinám či síťovým segmentům, 10. automatická identifikace systémů – zdrojů logů, 11. podpora šifrované komunikace mezi zdroji logů a systémem analýzy bezpečnostních logů, 12. integrace s adresářovým systémem (LDAP, Active Directory) pro potřeby autentifikace uživatelů, 13. minimální administrace /výběr zařízení ze seznamu od výrobce/pro připojení dalších zdrojů událostí (servery Windows, Unix/Linux, přepínače, routry, FW apod.), 14. Log Management s minimální postimplementační administrací. /agregace událostí dle typů, analýza, vyhodnocování/ pro případy, jako je zavedení nového zdroje událostí, nastavení pravidel pro sběr dat a archiv událostí, 15. definice základních korelačních pravidel v návaznosti na IS ZOS s důrazem na jeho bezpečnost a případné pokusy o zneužití, a to vše s korelací získávaných informací z okolí systému (provoz, aktivní prvky, OS atd.), 16. podpora sběru síťových toků (NetFlow, JFLow, Sflow) z navržených infrastrukturních prvků (switche, routery, NetFlow sondy), 17. řešení musí umožňovat automatické aktualizace,

#	Požadavek
	18. webové uživatelské rozhraní pro management, analýzu a reporting, 19. poskytování automatického backup/recovery procesu, 20. poskytovat interní kontroly stavu zařízení (healthcheck) a upozornění uživatele v případě problému, 21. možnost integrovaného managementu rizik na základě síťových toků a konfigurace aktivních prvků do GUI, 22. poskytování analytických a korelačních funkcí bez dalších zásahů a činností (out-of-the-box), 23. řešení musí být dodáno jako all-in-one appliance (vAppliance), 24. sběr logů z dalších bezpečnostních a síťových systémů (např. FlowMon, AFW f5, FW Cisco, AV Symantec, IronPort Cisco) a prvků navržených v rámci tohoto projektu, 25. výkonová rozšiřitelnost – přidání nových zařízení, lokací, aplikací, 26. možnost rozšíření výběrů o uživatelské položky z obsahu logů, 27. zajištění integrity nasbíraných dat, 28. umožnění nárůstu zdrojů událostí bez nutnosti pořizování dalšího hardware (v případě fyzického HW), 29. Near-real-time analýza událostí, 30. analýza dlouhodobých trendů událostí, 31. řešení musí být hodnocené v segmentu „leaders“ v GartnerMagicQuadrantu za minulé dva roky, 32. pokročilé "drill-down" dohledávání v případě potřeby, 33. možnost agregace události z logů i podle položek které nejsou standardně zahrnuty v řešení, 34. podpora a normalizace časových značek z různých časových zón, 35. sběr textových logů ze souborů, 36. sběr logů z databází pomocí JDBC/ODBC, 37. sběr log záznamů z prostředí Windows a Linux/Unix/AIX. Sběr Windows EVT záznamů i z Windows Server, a navržených OS v rámci SOBD, 38. rozčlenění vyhledaných dat (Drilldown): Vyhledávací rozhraní systému správy logů musí nabízet možnost rozčlenění vyhledaných dat až na detailní úroveň, IP adresa, typ události, protokol, port atd., 39. způsob zadávání vyhledávání: vyhledávací rozhraní systému správy logů musí poskytovat podporu jak pro zadání dotazu s použitím Booleovy logiky, tak pro regulární výrazy, 40. poskytování alertů na detekované anomálie, změny chování sítě a změny v generování logů a událostí, a to i v návaznosti na aplikaci operačního řízení, 41. kombinované hledání v indexovaných i neindexovaných datech v systému správy logů s použitím regulárních výrazů a fulltextového vyhledávání v nestrukturovaném textu současně, 42. korelační modul musí poskytovat již po instalaci (out-of-the-box) metody korelačních pravidel, která automatizují zjišťování incidentů a související workflow procesy, 43. korelace mezi zařízeními již po instalaci (out-of-the-box). Zjišťování chyb autentizace, chování perimetru a výskytu infiltrací (červů apod.) bez potřeby specifikovat typy sledovaných zařízení,

#	Požadavek
	44. řešení musí poskytnout alerting vycházející z detekovaných bezpečnostních hrozeb od monitorovaných zařízení a aplikace operačního řízení, 45. alerting založený na vypozorovaných anomáliích a změnách chování sítě (analýza síťových toků). Řešení musí poskytovat NBAD (Network Behavior Anomaly Detection) funkcionalitu, 46. řešení musí poskytnout alerting porušení bezpečnostních pravidel, založený na stanovené bezpečnostní politice (např. IM provoz je zakázán), 47. vykonávání akcí v závislosti na přijatém logu jako např. zaslat email, 48. schopnost pracovat s IP geolokacemi (botnet kanály atp.), 49. generování alertu při výpadku logů z konkrétního zařízení, 50. vestavěný mechanismus na klasifikaci systémů podle typu (např. mail server vs. databázový server), 51. vyhodnocení chybějících sekvencí (např. služba přestala běžet), 52. schopnost monitorovat historii útoků (typů událostí) na kritické komponenty a historii útoků jednotlivých uživatelů, 53. schopnost korelovat události DHCP, VPN a Active Directory a sledovat průběh uživatelské relace (session) v rámci celé instituce (přesná identifikace uživatele), 54. schopnost korelovat data o událostech se statickými a dynamickými seznamy označujícími položky, které mají či nemají být v síti povoleny (tj. seznam nezabezpečených protokolů), 55. poskytování rozhraní pro reporting, pomocí kterého lze vytvářet nové sestavy bez nutnosti sestavovat SQL dotazy, 56. nezměněná funkcionalita reportingu i při změně nebo náhradě některé technologie jako např. firewallu nebo IDS, 57. přístup k datům skrze otevřené REST API pro integraci s dalšími systémy, 58. postupné doplňování funkcionalit pro log management a security intelligence (rozšíření o další analytické moduly by mělo mít minimální dopad přidávání komponent třetích stran a mělo by být primárně umožněno jen licenčním klíčem), 59. řešení musí být schopno pracovat s interními překrývajícími se rozsahy adres, 60. řešení si musí pasivně budovat tabulku zařízení v síti z informací obsažených v již příchozích zdrojích (flows), 61. schopnost agregovat záznamy o síťovém provozu z obou stran datového toku do jedno záznamu, 62. provádění deduplikace záznamů o síťovém provozu v případě identických záznamů z různých zařízení, 63. podpora korelace dat proti výsledkům scanům zranitelností třetích stran, 64. uchovávání logů i flows jak v normalizovaném formátu, tak i „raw“ formátu, 65. řešení nebude licenčně omezeno počtem používaných korelačních pravidel a nebude licenčně omezeno počtem generovaných reportů, 66. možnost nasazení High Availability režimu v jakékoliv fázi životního cyklu řešení bez nutnosti reinstalace řešení.
P.45	Záruka 5 let, 5x8, garantovaná doba opravy do následujícího pracovního dne na místě včetně update SW a všech modulů.

#	Požadavek
P.46	Součástí dodávky musí být instalace a konfigurace řešení, včetně součinnosti při konfiguraci jednotlivých zařízení a aplikací a nastavení notifikací, a to včetně seznámení s funkcionalitami a obsluhou. Dále je požadováno za měsíc a za 3 měsíce vyhodnocení provozu a doladění korelačních pravidel na základě získaných dat během provozu implementovaného systému a dle požadavků Zadavatele.
P.47	Implementace notifikací s využitím stávajících notifikačních nástrojů ZZS a to včetně implementace napojení na svolávací systém. Notifikace budou prováděny následujícími nástroji: • Email • SMS • Hlasová zpráva (text-to-Speech) • Push aplikace na mobilní zařízení • Využití záložního svolávacího systému (jiná ZZS) *Pro notifikaci emailem bude využíván protokol SMTP, rozhraní stávajícího svolávacího systému bude poskytnuto v rámci implementační analýzy.*
P.48	Sběr logů z aplikačních, bezpečnostních a síťových systémů využívaných v rámci ZZS nebo dodávaných v rámci dodávky.
P.49	Nástroje/rozhraní pro logování z IT infrastruktury: 1. Aktivní prvky (sítě) 2. Informační systémy – IS ZOS/ZZOS a systém elektronické pošty 3. Databáze (ORACLE, MS SQL) 4. Operační systémy (MS Windows, Linux) – servery, pracoviště ZOS/ZZOS V případě, že se bude jednat o jeden nástroj zajišťující všechny uvedené služby, musí nástroj umožnit samostatný přístup k různým službám pro různé osoby na základě oprávnění definovaného správcem a možnost instalace na oddělený samostatný server (Syslog server v kap. 6.4.1 – Datové centrum, HW infrastruktura, systémový SW).
P.50	Dodávka a implementace nástroje na logování z IT infrastruktury, IS ZOS a elektronické pošty, tzn. aktivní prvky, aplikace, operační systémy apod. ve kterém bude možnost plošně prohledávat sesbíraná data a mít k dispozici statistiku a analytické funkce – přičemž zdrojem dat může být stávající syslog systém a bude rozšířen o následující funkce: 1. Schopnosti provádět korelace přes více datových zdrojů a hledání specifických vzorů 2. Dlouhodobé retence dat (minimálně 3 měsíce, optimálně 6 měsíců) 3. Předpokládaný objem logovaných dat do 5 GB za den 4. Jeden společný datový sklad pro všechna indexovaná data – jeden dotaz nebo report může zahrnout všechna indexovaná data 5. Není třeba vytvářet datové schéma nebo připravit vyhledávací dotazy ještě před indexováním 6. Možnost využití nestrukturovaných souborů a datového skladu bez pevného schématu (bez relační databáze s pevným schématem)

#	Požadavek
	7. Schopnost indexovat a připravit pro vyhledávání všechna originální data bez jakékoliv modifikace (bez normalizace/redukce dat) 8. Automatická komprese indexovaných dat pro redukci nároků na úložný prostor 9. Flexibilní nastavení uchování dat s možností odstupňování řízení toho, co se stane s postupně stárnoucími daty. Neaktuální data mohou být přesunuta na externí (levnější) datové úložiště k archivaci a (nebo) smazána. 10. Flexibilní kontrola přístupu na základě rolí pro řízení přístupu uživatelů a přístupů přes API. 11. Integrace autentizace a autorizace s Microsoft Active Directory, případně samostatný oddělený systém pro auditní účely (mimo stávající systém AD). 12. Generování hashe pro každou událost v době indexování tak aby umožnilo při vyhledávání zjistit, zda s daty nebylo manipulováno 13. Monitoring své vlastní konfigurace a využití s cílem udržet si kompletní, digitálně podepsané auditní záznamy o tom, kdo přistupuje k systému, jaké dotazy spouští, na jaké reporty se dívá, jaké konfigurační změny provádí a další. 14. Řešení by mělo umožnit snadné vytváření široké palety vizualizací (nejen pevně dané, předpřipravené reporty) 15. Dostupné vizualizace by měly zahrnovat: čárový graf, časový graf, plošný graf, sloupcový graf vertikální, sloupcový graf horizontální, jediná hodnota s trendem (růst, pokles), koláčový graf, bodový graf, bublinový graf, ciferníkový (budíkový) ukazatel, graf typu teploměr (zobrazení hodnoty ve vztahu k rozsahu), geolokační mapa, graf zobrazující rozložení hodnot v geografických regionech, kruhový graf, výplňový graf, tabulky (vč. doplňkových funkcí jako jsou automatické sumy, procentuálních vyjádření, číslování řádků, atd.)
P.51	Implementace nástroje na logování bude obsahovat nejenom zprovoznění a základní nastavení systému ale vytvoření i reportů a dashboardů (náhledů) na jednotlivé komponenty IT infrastruktury a IS ZOS. Minimálně následující náhledy: 1. Aktivní prvky (LAN/WAN/FW) – přihlášení, změny konfigurací, chyby atd. 2. FW/VPN – přístupy (oprávněné a neoprávněné) včetně geolokace (zobrazení na mapě a v tabulce) 3. Operační systémy a databáze IS ZOS – přihlášení, chyby atd. 4. Emailová komunikace – přístupy (oprávněné a neoprávněné) včetně geolokace, chyby systému atd.
P.52	Je požadována realizace jednotného bezpečnostního portálu pro správce a management ZZS, který bude zahrnovat dodané technologie v rámci projektu. Minimální požadavky na přehledový bezpečnostní portál: 1. Webové rozhraní 2. Autentizace/autorizace uživatelů proti Microsoft Active Directory 3. Zobrazení posledních incidentů na základě analýzy bezpečnostních logů 4. Zobrazení VPN připojení (úspěšné i neúspěšné) 5. Zobrazení přihlášení do aplikací IS ZOS (úspěšné i neúspěšné)

#	Požadavek
	6. Zobrazení přehledu emailové komunikace ZZS (chyby, vytížení apod.) 7. Možnost dalšího rozvoje dle požadavků ZZS – otevřený systém
P.53	Systém analýzy bezpečnostních logů (SW) bude provozován na infrastruktuře (HW a systémový SW) požadovaný a dodávaný dle kap. 3.4.7 – Infrastruktura (HW) a systémový SW pro systém analýzy bezpečnostních logů.

Tabulka 9: Systém analýzy bezpečnostních logů (SW)

3.4.7 Infrastruktura (HW) a systémový SW pro systém analýzy bezpečnostních logů

V této kapitole jsou uvedeny požadavky na infrastrukturu (HW) a nezbytný systémový SW pro provoz dodávaných technologií – Systém analýzy bezpečnostních logů (SW).

Zadavatel nepředepisuje technologii, jen principy a požadavky na řešení. Technologie bude navržena dodavatelem v nabídce v rámci veřejné zakázky.

HW a SW infrastrukturu není možné v této dokumentaci dostatečně specifikovat, protože jsou závislé na zvolené technologii v rámci řešení konkrétního uchazeče. Zde jsou stanoveny limitní podmínky, které musí uchazeč splnit, tj. nejen technologické podmínky v DC, technologie využívané zadavatelem, ale i požadavky na min. doby pro ukládání dat a v návaznosti na splnění těchto podmínek a potřeb technologie, uchazeč navrhne a dodá vhodnou HW a SW infrastrukturu.

#	Požadavek
P.54	Dodávka min. 1 ks následujících serverů s min. konfigurací: 1. provedení Rack mount (včetně potřebných montážních komponent a ramene pro kabeláž) pro až 28 disků velikosti 2,5“, maximální velikost 2U, pro přístup ke všem komponentám serveru bez použití nářadí 2. minimálně jeden šestnácti jádrový procesor s hodnotou dle SPECint_rate2006 base min. 1700 bodů a dle SPECfp_rate2006 base min. 1300 pro 2 CPU konfiguraci (údaje musí být k dispozici na www.spec.org) 3. min. 192 GB RAM (min. 32GB moduly 2666MHz) s celkem 24 DIMM pozicemi 4. min. 14x 900GB SAS 15K v raid 5 pro data 5. hw řadič s min. 2GB cache a podporou raid 0, 1, 5, 6, 50 6. min. 4x 1Gbase-T ethernet síťové porty s podporou IPv4, IPv6 7. min. 2x 10Gbit SFP+ ethernet síťové porty s podporou TOE, IPv4, IPv6 včetně dvou SFP+ DA kabelů pro připojení do stávající infrastruktury 8. 2 redundantní síťové napájecí zdroje min. 750W 9. management serveru nezávislý na operačním systému s dedikovaným USB či SD úložištěm (data na úložišti musí být dostupná i v případě výpadku interních disků a musí být možné ji rozdělit na několik nezávislých partition s možnosti volby boot sekvence) poskytující management funkce a vlastnosti: webové rozhraní a dedikovaná IP adresa, sledování hardwarových senzorů (teplota, napětí, stav, chybové senzory); podpora virtuální mechaniky 10. vyžadována je schopnost monitorovat a spravovat server out-of-band bez nutnosti instalace agenta do operačního systému 11. management musí podporovat dvou faktorovou autentifikaci, filtrování přístupu na

#	Požadavek
	základě IP adres (IP blocking) a AD/LDAP 12. Záložní BIOS v dedikované ROM s možností manuální/automatické obnovy 13. požadujeme vestavěné GUI s podporou HTML5 a možnost komunikace pomocí: HTTPS, CLI, IPMI, WSMAN, REDFISH 14. certifikace pro aktuální verze VMware ESX, vSphere, Windows Server 2016, Red Hat Enterprise Linux a SUSE 15. součástí je licence MS Windows Server 2016 Datacenter pro min. 16 jader (odpovídající nabízenému procesoru) 16. podpora na 5 let typu NBD, oprava v místě instalace zařízení Server bude předán v místě plnění po základní instalaci HW v místě plnění, konfiguraci a instalaci SW (virtualizační platforma) včetně aktualizace firmware a ověření funkčnosti kupujícím.
P.55	Dodávka a instalace systémového SW: 1. Požadujeme dodávku systémového SW pro všechny nabízené systémy. Jedná se o minimálně následující systémový SW: ○ Operační systémy serverů, kde požadujeme dodávku všech licencí potřebných operačních systémů a mimo to požadujeme jako součást HW dodávaných serverů (viz požadavek na dodávku serveru výše) licenci Windows Datacenter. ○ Databáze pro dodávané systémy dle jejich požadavků ○ Pro virtualizaci dodávaných serverů požadujeme kompatibilní řešení se stávající virtualizací tak, aby bylo možné zařadit do jedné konfigurační konzole – Minimálně licence na dodávaný počet CPU (VMware vSphere 6 Standard for CPU) s podporou výrobce na 5 let. 2. V případě, že nabízené řešení vyžaduje další nespecifikovaný systémový SW tak musí být součástí nabídky.
P.56	Součástí dodávky je integrace dodávaných technologií do stávajícího monitorovacího nástroje (WhatsUp firmy Ipswitch), který není součástí dodávky tohoto projektu. Monitoring musí jednoznačně identifikovat chod jednotlivých komponent.
P.57	Součástí dodávky není strukturovaná kabeláž.
P.58	Dodávka, zapojení, instalace technologií, instalace a zprovoznění dodávaných technologií a prvků na dodaných technologiích.

Tabulka 10: Infrastruktura (HW) a systémový SW pro systém analýzy bezpečnostních logů

3.4.8 Úpravy IS ZOS

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
Napojení na Systém analýzy bezpečnostních logů (SW) (viz kap. 3.4.6)	
P.59	Je požadována úprava systémů IS ZOS pro zaznamenávání činností v rámci operací těchto systémů do externích systémů pro následné zpracování a analýzy – Systém analýzy bezpečnostních logů (SW) (viz kap. 3.4.6).

#	Požadavek
P.60	**IS OŘ:** Předávání logů z IS OŘ do systému analýzy bezpečnostních logů v následujícím rozsahu: 1. Přihlášení a odhlášení do systémů a modulů 2. Chybná přihlášení do systému a modulů 3. Operace s daty (pořízení, modifikace a zobrazení) 4. Možnost předávání logů s anonymizovanými položkami – dle druhu informace a účelu jejího pořízení – na základě konzultace a požadavků ZZS
P.61	**GIS:** Předávání logů z GIS do systému analýzy bezpečnostních logů v následujícím rozsahu: 1. Přihlášení a odhlášení do systému 2. Chybná přihlášení do systému Logy jsou ukládány na diskové úložiště, odkud mohou být automatizovaně zpracovávány Systémem analýzy bezpečnostních logů. V případě využití této možnosti je součástí dodávky parsování logů, jejich analýza a ukládání do Systému analýzy bezpečnostních logů.
P.62	**EKP/MZD:** Předávání logů z EKP/MZD do systému analýzy bezpečnostních logů v následujícím rozsahu: 1. Přihlášení a odhlášení do systémů a modulů 2. Chybná přihlášení do systému a modulů 3. Operace s daty (pořízení, modifikace a zobrazení) 4. Možnost předávání logů s anonymizovanými položkami – dle druhu informace a účelu jejího pořízení – na základě konzultace a požadavků ZZS
P.63	**IS Pojišťovna:** Předávání logů z IS Pojišťovna do systému analýzy bezpečnostních logů v následujícím rozsahu: 1. Přihlášení a odhlášení do systémů a modulů 2. Chybná přihlášení do systému a modulů 3. Operace s daty (pořízení, modifikace a zobrazení) 4. Možnost předávání logů s anonymizovanými položkami – dle druhu informace a účelu jejího pořízení – na základě konzultace a požadavků ZZS
P.64	**Systém sledování vozidel (AVL):** Předávání logů z AVL do systému analýzy bezpečnostních logů v následujícím rozsahu: 1. Přihlášení a odhlášení do systému 2. Chybná přihlášení do systému 3. Informace odeslání informací k dané události do technologie AVL ve voze 4. Možnost předávání logů s anonymizovanými položkami – dle druhu informace a účelu jejího pořízení – na základě konzultace a požadavků ZZS Logy jsou ukládány na diskové úložiště, odkud mohou být automatizovaně zpracovávány Systémem analýzy bezpečnostních logů. V případě využití této možnosti je součástí dodávky parsování logů, jejich analýza a ukládání do Systému analýzy bezpečnostních logů.
P.65	**Svolávací systém** využívá data IS OŘ a jeho volání je vždy z IS OŘ, tj. data budou sbírána cestou IS OŘ.

#	Požadavek
P.66	**Telefonní ústředna** je integrována s IS ZOS prostřednictvím API serveru. Vlastní přístup na server určený pro API rozhraní je logován v rámci systémových prostředků OS. Data jsou tedy sbírána na systémové úrovni. Součástí dodávky parsování logů, jejich analýza a ukládání do Systému analýzy bezpečnostních logů.
P.67	**Záznamový systém (REDAT)** je uzavřené řešení pro nahrávání hovorů. Dispečeři ZOS mají přístup k nahrávkám prostřednictvím systému IS OŘ, který loguje přístupy k aplikačnímu serveru systému REDAT v rámci IS OŘ. Tyto informace jsou tak předávány v rámci přeposílání logů IS OŘ. Součástí dodávky parsování logů z IS OŘ je jejich analýza a ukládání do Systému analýzy bezpečnostních logů.
P.68	**Integrace telefonie a radiofonie** je vázaná na dané dispečerské pracoviště a informace o přihlášení a přístupu uživatele budou brány z IS OŘ dle toho, který dispečer na daném pracovišti pracoval (vlastní integrace nevyužívá speciální přístupy a ovládá komunikační prostředky na daném pracovišti). Vlastní přístup na server určený pro integraci je logován v rámci systémových prostředků OS. Data jsou tedy sbírána na systémové úrovni. Součástí dodávky parsování logů z IS OŘ je jejich analýza a ukládání do Systému analýzy bezpečnostních logů.
P.69	**Záložní IS ZOS (ZZOS):** ZZOS využívá v současné době repliku systému IS OŘ. Je požadováno, aby pro tento systém byla sbíraná data stejná v primární i záložní lokalitě.
P.70	Aplikační SW na pracovištích ZOS/ZZOS: Vlastní přístup do OS na pracovištích ZOS a ZZOS bude logován v rámci systémových prostředků operačního systému. *Sbíraná data z operačních systémů a dalších technologie na pracovištích ZOS/ZZOS budou sbírána na systémové úrovni.*
Napojení IS OŘ na FireWall s IPS pro ZZOS (viz kap. 3.4.2)	
P.71	V rámci IS OŘ bude možné přijímat i alerty upozorňující na bezpečnostní události a to nejenom z uvedených bezpečnostních prvků ale všech komponent zabezpečení. Bude se jednat o alerty bezpečnostních událostí relevantních k provozu centrálního dispečinku a celého IS ZOS s kritickou důležitostí. Bezpečnostní alerty v rámci IS ZOS budou definovány a konfigurovány na základě požadavků ZZS v systémech analýzy a sběru bezpečnostních logů, který tyto alerty bude předávat do IS OŘ – dispečerského pracoviště. Tak bude aktivně informován provoz centrálního dispečinku ZOS o vážných bezpečnostních událostech.
P.72	Oprávněné osoby centrálního dispečinku budou mít možnost pomocí rozhraní v IS ZOS (IS OŘ) na základě vzniklých bezpečnostních událostí a jejich průběhu rozhodnout o možnosti aktivace (a následné deaktivace) izolace systému IS ZOS od externích sítí nebo i od interních LAN/WAN segmentů. Vlastní izolace bude realizována na uvedených bezpečnostních prvcích (ZOS/ZZOS). Oprávněný uživatel bude před vlastní aktivací daného typu izolace informován o rozsahu izolace a z toho plynoucích omezení centrálního dispečinku a IS ZOS. O těchto událostech bude proveden detailní záznam událostí včetně jejich časové souslednosti a uživatelích, kteří taková opatření realizovali a neprodleně automaticky informováni definovaní pracovníci ZZS v rámci stávajícího

#	Požadavek
	svolávacího systému ZZS.
Autentizace uživatelů operačního řízení prostřednictvím AD	
P.73	V rámci sjednocení ověřování identity uživatelů v rámci IT a operačního řízení je požadováno využití stávající domény v rámci Microsoft Active Directory. Pro tyto účely požadováno rozšíření stávajícího IS ZOS o možnost autentizace a autorizace v rámci struktury Active Directory.
P.74	**IS OŘ:** Správce IS OŘ bude pak schopen zvolit způsob autentizace jednotlivých uživatelů dle potřeb ZZS a typu modulů/subsystémů. Je požadováno, aby bylo možné plně využít pro autentizaci a autorizaci uživatelů IS OŘ jednotných účtů v rámci MS Active Directory. Autorizace uživatelů pro jejich oprávnění pak bude spočívat v příslušnosti k dané skupině uživatelů.
P.75	**EKP/MZD:** EKP/MZD musí umožňovat autentizaci a autorizaci uživatelů jak interní (stávající stav) nebo v rámci MS Active Directory. Správce IS v návaznosti na okolní systémy bude schopen zvolit způsob autentizace EKP/MZD dle požadavku ZZS. Autorizace uživatelů pro jejich oprávnění pak bude spočívat v příslušnosti k dané skupině uživatelů.
Integrace s personálním systémem	
P.76	IS OŘ a EKP/MZD musí umožnit využití integrace s personálním systémem, a to jak při zakládaní uživatele a případně jejich základní role v rámci personálního systému (která se promítne do AD) využití zneplatnění účtů uživatelů, u kterých bude ukončen pracovní poměr (zneplatnění/vymazání účtu v AD). Tím bude zajištěna maximální aktuálnost uživatelských účtů zaměstnanců ZZS.
Monitoring a reporting a přístupů	
P.77	Pro správu a reporting oprávnění bude dodán i samostatný portál pro správu uživatelů IS OŘ a přiřazování jejich rolí. Tento portál bude sloužit pro vedoucí pracovníky OŘ, kteří budou tato oprávnění spravovat a kontrolovat a monitorovat.
P.78	Součástí dodávky bude nástroj pro reportingu všech změn provedených jednotlivými uživateli/administrátory v rámci Microsoft Active Directory (AD) ZZS, tak aby bylo možné kontrolovat změny oprávnění, které byly v rámci AD provedeny. Je požadováno reportovat minimálně: • Vytvoření nového uživatele nebo skupiny • Vymazání uživatele nebo skupiny • Zneplatnění (disable) uživatele • Přidání člena skupiny • Vymazání člena skupiny
Infrastruktura (HW) a systémový SW pro úpravy IS ZOS	
P.79	Stávající infrastruktura (HW) a systémový SW pro běh IS ZOS po realizaci úprav zůstane beze změny, tj. nedojde ke změně konfigurace, parametrů, licencí systémového SW využívaných pro běh IS ZOS.

Tabulka 11: Úpravy IS ZOS

3.4.9 Konfigurace systému elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.80	Napojení na Systém analýzy bezpečnostních logů (SW) a předávání následujících dat ze systému elektronické pošty: • Úspěšná a neúspěšná připojení k systému dostupnými protokoly • Využívání systému elektronické pošty jednotlivými uživateli • Dostupné bezpečnostní logy používaného systému • Dostupné chybové a provozní logy používaného systému Předávání veškerých logů systému do nástroje/rozhraní pro logování.
P.81	Toto nastavení realizovat pro všechny komponenty systému elektronické pošty.
P.82	Předávání logů systému online prostřednictvím syslog služby.
P.83	Součinnost při konfiguraci FireWallu ZOS a konfigurace FireWallu ZZOS pro získávání informací o bezpečnostních událostech na prvcích FireWall, týkajících se systému elektronické pošty. Minimálně: • Odepření přístupu z dané IP adresy na systém (reputace dynamický ACL apod.) • IPS a AntiMalware události • Identifikace chyb v protokolu
P.84	Systém dynamických ACL na základě parametrického vyhodnocení bezpečnostních logů systému. Dynamický ACL bude vytvářen prostřednictví analýzy logů na základě neoprávněného přístupu k systému. Pro vytváření dynamických ACL bude možné systémově nastavovat následující parametry: • Počet špatných přihlášení k danému protokolu • Minimální čas od posledního výskytu špatného přihlášení Publikace dynamického ACL pro systém elektronické pošty bude pro účely aktualizace pravidel FireWallu realizována web serverem jako standardní textový soubor s výčtem (list) IP adres (jedna IP na jednom řádku).
P.85	Nástroj/rozhraní pro logování bude zpracovávat i uvedený dynamický ACL pro systém elektronické pošty a zobrazovat časový průběh počtu IP adres obsažených v listu a upozorňovat na enormní nárůst.
P.86	Provedení konfigurace FireWallu ZZOS (kap. 3.4.2) a součinnost pro konfiguraci FireWallu ZOS pro implementaci dynamického ACL – aktualizace listu IP adres

Tabulka 12: Úpravy elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů

3.4.10 Dvoufaktorová autentizace administrátorských VPN přístupů

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.87	Pro autentizaci administrátorských VPN přístupů je požadován systém dvoufaktorové autentizace. Minimální požadavky: 1. Integrace se stávajícím FireWallem ZOS a autentizačním serverem 2. Správa pomocí webové konzole nebo Microsoft Management Console (MMC) 3. Bez potřeby dalšího zařízení nebo tokenu 4. Kompatibilní se všemi telefony, které umožňují přijímat SMS 5. Jednorázové heslo nejen přes mobilní aplikaci, push notifikaci, hardwarové tokeny a SMS, ale i vlastní cestou (např. e-mailem). 6. Push autentifikace – možnost autentifikace potvrzením v aplikaci na mobilním telefonu, bez nutnosti přepisovat jednorázové heslo (podpora iOS, Android i Windows Mobile). 7. Podpora Virtual Private Networks (VPN) – Cisco ASA, Remote Desktop Protocol (RDP) a RADIUS.
P.88	Licence pro 20 min. uživatelů.
P.89	Je požadována záruka na funkčnost, podpora a aktualizace po dobu min. 5 let.

Tabulka 13: Dvoufaktorová autentizace administrátorských VPN přístupů

3.4.11 Nástroje pro bezpečnostní audit a penetrační testy

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.90	Je požadována dodávka nástroje/nástrojů pro periodické testování bezpečnostních zranitelností interních systémů i systémů, které komunikují s externími subjekty i jako součást penetračních testů (nástroj/nástroje budou využity v rámci kap. 3.4.12 – Bezpečnostní audit a penetrační testy.
P.91	Minimální rozsah: externí testy, interní testy a testy zranitelností operačních systémů, databází a informačních systémů (aplikací). Jedná se minimálně o: 1. Host Discovery – vyhledávání aktivních strojů; 2. Port Scanning – skenování portů; 3. Service Discovery – vyhledání běžící služby; 4. Web Applications – skenování webových aplikací;
P.92	Je požadováno, aby nástroj/nástroje umožňoval: 1. Vzdálené privilegované a neprivilegované skeny 2. Neomezené množství koncových IP adres 3. Pravidelné aktualizace signatur/detekčních metod (cca 1xtýdně)
P.93	Předmětem dodávky není periodické provádění testů zranitelností (nad rámec testů v rámci vedlejších aktivit), ale zajištění nástrojů pro provádění a vyhodnocování uvedených testů.

#	Požadavek
P.94	S ohledem na vysokou citlivost zpracovávaných dat musí být dodaný nástroj možné kompletně instalovat na server/počítač umístěný v lokální síti, která je pod správou Zadavatele. Výstupy z testů/skenů musí být rovněž zpracovávány lokálně, bez zasílání do cloudu. Dodaný nástroj musí umožňovat ovládání s pomocí webového GUI.
P.95	Instalaci nástroje musí být možné realizovat na prvky s operačními systémy Microsoft Windows 7 a vyšší, Microsoft Windows Server 2008 a vyšší, macOS i Linux. Součástí dodávky nebude HW, OS ani další aplikační vybavení nutné pro provoz nástroje. Předpokládá se instalaci na prostředky Zadavatele (virtuální server nebo testovací PC/notebook).
P.96	Dodané řešení musí podporovat realizaci vzdálených bezagentských privilegovaných i neprivilegovaných skenů neomezeného počtu zařízení/IP adres a musí být schopné realizovat bezpečnostní skeny webových aplikací.
P.97	Řešení musí být schopné identifikovat chybějící záplaty/zranitelné služby a aplikace běžící na skenovaných systémech.
P.98	Součástí dodávky bude licence relevantního nástroje s podporou a funkčností po dobu 5 let, instalace a aktivace jednoho skeneru v prostředí Zadavatele a úvodní zaškolení administrátorů a uživatelů.

Tabulka 14: Nástroje pro bezpečnostní audit a penetrační testy

3.4.12 Bezpečnostní audit a penetrační testy

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.99	Bezpečnostní analýza stávajícího prostředí z pohledu souladu se zákonem 181/2014 Sb., ve znění pozdější novelizace a s vyhláškou 82/2018 Sb.
P.100	Hodnocení stávajícího rozsahu řízení bezpečnosti informací: 1. Politiky 2. Metodiky a. Metodika identifikace a hodnocení aktiv b. Metodika analýzy rizik 3. Proces a výstupy hodnocení aktiv 4. Proces a výstupy hodnocení rizik 5. Revize primárních a podpůrných aktiv, jejich vzájemné vazby, určení jejich hodnoty a hodnocení jejich správy garanty 6. Plán zvládání rizik 7. Prohlášení o aplikovatelnosti bezpečnostních opatření 8. Zajištění zpětné vazby 9. Plán rozvoje bezpečnostního povědomí 10. Strategie řízení kontinuity 11. Pravidla řešení kybernetických bezpečnostních incidentů 12. Pravidla řízení provozu ICT

#	Požadavek
	13. Hodnocení definice kontextu organizace, hodnocení jeho rozdělení na vnitřní a vnější kontext a hodnocení SLA mezi těmito 2 kontexty
P.101	Přezkoumání implementace technických opatření do praxe. Technické ověření souladu implementace primárních a podpůrných aktiv dle požadavků ZKB: 1. Aplikace 2. Operační systémy 3. Síťové prvky 4. Bezpečnostní prvky 5. Fyzická bezpečnost 6. Zálohování 7. Apod.
P.102	Výsledkem auditu bude: 1. Zpráva z přezkoumání stávajícího prostředí Zadavatele s následujícím obsahem: a. Pro každé opatření bude uveden popis aktuálního stavu b. Zhodnocení z pohledu požadavků prováděcí vyhlášky KB (ZKB) c. Případné zhodnocení z pohledu „best practice“, pokud bude takovéto doporučení žádoucí. d. Každé opatření bude popsáno minimálně v rozsahu ½ A4. e. Obsahem zprávy jsou veškeré paragrafy obsažené v prováděcí vyhlášce ZKB, tzn. Že se organizace zkoumá z pohledu organizační opatření, technických opatření i fyzické bezpečnosti. 2. Hodnocení stavu a. Přehledový dokument s výpočetní logikou, který bude hodnotit výsledek pro ▪ Technické role ▪ Odděleně a s menší mírou detailu pro manažerské role b. Hodnocení bude provedeno jednotlivě pro každý požadavek paragrafů ZKB 3. Obecný návrh nápravných opatření a. Cílem není hodnotit veškeré možné technické varianty nápravných opatření, ale určit orientační výši nákladů pro zajištění souladu se ZKB a určit druh technologie. 4. Prezentace výsledků projektu pro projektový tým a. PT prezentace a diskuze s týmem 5. Prezentace výsledků projektu pro vrcholový management
P.103	Provedení penetračních testů a testů zranitelnosti: 1. Provedení penetračních testů a testů zranitelnosti pro IS ZOS, IS ZZOS a systému elektronické pošty (informační systémy a technologie jsou popsány v kap. 6.2 – Informační a komunikační systémy k zabezpečení). 2. Pro systémy IS ZOS, IS ZZOS a Elektronickou poštu budou provedeny závěrečné testy zranitelnosti z externí sítě. V zájmu ověření korektního fungování webového aplikačního firewallu (WAF) a zajištění vysoké úrovně bezpečnosti provozovaných webových aplikací je požadováno provedení

#	Požadavek
	jednorázových penetračních testů.
P.104	Závěrečné testy zranitelnosti budou provedeny z externí sítě na IS ZOS, IS ZZOS a Elektronickou poštu. Jedná se tedy o testy zranitelnosti realizované přes bezpečnostní prvky – perimetry (FireWall) implementované v ZOS a ZZOS. Tyto testy musí obsahovat min.: 1. Host Discovery – vyhledávání aktivních strojů; 2. Port Scanning – skenování portů; 3. Service Discovery – vyhledání běžící služby; 4. Web Applications – skenování webových aplikací; Účelem těchto testů je ověření konfigurace perimetrů a nalezení zranitelností publikovaných služeb/systémů.
P.105	Součástí bezpečnostního auditu budou i penetrační testy, které musí splňovat minimálně: 1. Penetrační testy se budou týkat uvedených aplikací provozovaných zadavatelem a jejich účelem bude identifikovat případné nedostatky v nastavení nasazeného WAF a odhalit případné zranitelnosti ve výše uvedených aplikacích, které jsou jím chráněny, a zajistit tak jejich bezpečnost v rámci plnění požadavků §25 vyhlášky 82/2018 Sb. V souladu s bezpečnostní strategií a dalšími dokumenty zadavatele. 2. Součástí testů nebude vyhledávání zranitelností v síťové ani jiné infrastruktuře, virtualizačních platformách ani dalším SW vybavení serverů provozujících uvedené aplikace, které s provozem daných aplikací přímo nesouvisí. Před vlastními penetračními testy bude proveden test zranitelnosti nástrojem uvedeným v kapitole 3.4.11. viz předcházející požadavek. 3. Testy budou realizovány dle aktuální verze OWASP Testing Guide (OTG) a v souladu s metodikou OSSTMM a budou primárně zaměřeny na odhalování zranitelností dle platné verze OWASP Top 10. Využito při tom bude automatizovaných nástrojů i manuálního testování.
P.106	Výstupem testů zranitelnosti a penetračních testů musí být: 1. Závěrečná zpráva, která bude obsahovat soupis provedených testů a jejich výsledků, detailní popis odhalených zranitelností, ohodnocení jejich nebezpečnosti včetně konkrétního postupu umožňujícího jejich odstranění. 2. Doporučení řešení odhalených zranitelností – konkrétní postupy umožňující jejich odstranění u oblastí/technologií, které nejsou součástí dodávky. 3. Realizace opatření k odstranění odhalených zranitelností ve formě nastavení a implementace u oblastí, které jsou součástí dodávky.

Tabulka 15: Bezpečnostní audit a penetrační testy

3.4.13 Bezpečnostní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.107	Systém bude chránit osobní údaje pacientů a bude v souladu s Nařízením Evropského parlamentu

#	Požadavek
	a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob (GDPR) v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
P.108	Vybavení musí plnit podmínky zákona č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
P.109	Autorizace: Poskytnutí přístupu autentizovaného uživatele k aktivu systému (data, aplikace), odpovídající pracovnímu zařazení uživatele a přidělené roli (rolím) v systému. Systém umožní řídit přístupová oprávnění jednotlivých subjektů jen k údajům, ke kterým mají a mohou mít přístup.
P.110	Zabránění vstupu neautorizovaného subjektu do systému – zamezení možnosti přístupu neoprávněného subjektu.
P.111	Zajištění šifrované komunikace mezi všemi součástmi systému a pracovišti uživatelů, případně zajištění komunikace v odděleném síťovém prostředí.
P.112	Evidence přístupů všech uživatelů do systémů a technologií (logování) včetně časových údajů.
P.113	Veškeré přístupy k datům a aktivita uživatelů v rámci dodávaných systémů a technologií budou logovány tak, aby byly zřejmé přístupy k jednotlivým údajům a zpětná kontrola těchto údajů.
P.114	Veškeré logy budou dostupné pro externí Systém analýzy bezpečnostních logů (SW).

Tabulka 16: Bezpečnostní požadavky

3.4.14 Implementační a provozní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.115	Všechny komponenty musí být připraven na provoz 24x7x365 (non-stop).
P.116	Počet uživatelů informačních systémů se nezmění.
P.117	Předmětem zakázky jsou i veškeré služby související s dodávkou – doprava, instalace, implementace do stávající infrastruktury, konfigurace a zprovoznění komunikace, nastavení datových toků, seznámení s obsluhou a správou systému, testování, bezplatné preventivní prohlídky v rámci poskytování servisních služeb. Veškeré seznámení s obsluhou bude probíhat v prostorách objednatele a v českém jazyce. Součástí nabídkové ceny musí být i veškeré práce či činnosti, které v této zadávací dokumentaci nejsou explicitně uvedeny, ale které musí dodavatel s ohledem na jím nabízený předmět veřejné zakázky a jeho řádnou a úplnou realizaci provést k dosažení objednatelem požadovaného cílového stavu.
P.118	Instalace do prostředí objednatele uvedeného v kap. 6.4 – Stav ostatních informačních a komunikačních technologií a kap. 6.2 – Informační a komunikační systémy k zabezpečení.
P.119	V rámci implementace musí dodavatel zajistit plnohodnotný provoz dodávaného řešení současně s provozem stávajících systémů a technologií. To vše s minimálním omezením provozu. Dodavatel

#	Požadavek
	je povinen přizpůsobit realizaci předmětu zakázky podmínkám objednatele.
P.120	Dodávka OS na servery, včetně instalace do prostředí objednatele, vč. Potřebných licencí, pokud se jedná o licencovaný OS.
P.121	Všechny dodávané nebo upravované součástí systémů (OS, DB, IS, klientské aplikace) musí logovat svou činnost do logů s možností nastavit úroveň logování pro potřeby diagnostiky.
P.122	Zálohování – dodávaný systém (virtualizace, OS) a DB musí být schopny a připraveny na zálohování systémem objednatele, tj. pro virtualizaci, OS a DB musí existovat agenti umožňující zálohování ze strany objednatele. Informace k zálohovacímu systému objednatele jsou uvedeny v kapitole 6.4.1 – Datové centrum, HW infrastruktura, systémový SW.
P.123	Zajištění administrátorských aplikací, konzolí pro všechny součástí systému (OS, DB, IS, …) pro zajištění konfiguračního managementu systému anebo jeho součástí.
P.124	Dohled – dodávané systémy a technologie musí předávat informace o svém stavu na žádosti SNMP GET. Zhotovitel poskytne parametry, podmínky a součinnost při nastavení dohledu dodaného řešení.
P.125	Architektura řešení celého systému musí korespondovat s požadavky na jeho dostupnost, uvedenými v servisní smlouvě.
P.126	Synchronizace času všech zařízení s time serverem nebo zprostředkovaně přes centrální systém.

Tabulka 17: Provozní požadavky

3.5 POŽADAVKY NA SLUŽBY

3.5.1 Realizace předmětu plnění

Součástí předmětu plnění je zajištění služeb souvisejících s realizací předmětu plnění minimálně v následujícím rozsahu:

1) Objednatel požaduje před zahájením implementačních prací zpracování **Implementační analýzy včetně návrhu řešení** (konkretizace implementačního postupu, přesné konfigurace a instalačního a montážního návrhu řešení z nabídky), která bude zahrnovat informace pro všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění. Implementační analýza včetně návrhu řešení musí být před zahájením prací schválena objednatelem. Implementační analýza včetně návrhu řešení musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu a musí obsahovat minimálně tyto části:
   a) Implementační analýza – zjištění týkající se prostředí objednatele, bude obsahovat alespoň následující:
      i) Seznam technologií, které mají vliv/dopad na dodávku
      ii) Identifikace zdrojů dat využitých pro dodávku
      iii) Evaluace bezpečnosti systému a rizikových faktorů
      iv) Implementační upřesnění specifikace požadavků
      v) Výstupy z analýzy okolí – sběr a analýza informací vztahujících se k dodávce (např. součinnosti apod.)

b) Detailní popis cílového stavu (instalační a montážní upřesnění návrhu řešení z nabídky)

Popis bude obsahovat alespoň:

i) Rozpracování návrhu řešení z nabídky zhotovitele z pohledu instalací a montáže dle informací z implementační analýzy

ii) Upřesnění rozhraní pro integraci na IS a technologie třetích stran (v případě nutnosti)

iii) Způsob zajištění projektového řízení na straně zhotovitele pro realizaci předmětu plnění (harmonogram, projektový tým, koordinační mechanismy apod.)

iv) Detailní návrh a popis postupu implementace, instalace a montáže předmětu plnění

v) Detailní popis zajištění bezpečnosti systému a informací

Detailní harmonogram projektu včetně uvedení kritických milníků. Kritické milníky jsou termíny dosažení určitých fází projektu, které jsou pro naplnění cílů projektu klíčové. Kritické milníky budou obsahovat minimálně aktivity vedené v kapitole 4 – Harmonogram, s uvedením konkrétních termínů, zhotovitel vhodným způsobem může rozšířit kritické milníky o další aktivity, které mohou být pro projekt klíčové.

vi) Detailní popis navrhovaného seznámení s funkcionalitami, obsluhou dodávaných technologií a budoucím provozem.

2) **Zajištění projektového vedení/řízení** realizace předmětu plnění ze strany zhotovitele a jeho případných subdodavatelů.

3) **Vývoj, implementace a nastavení** informačních a komunikačních technologií odpovídající schválenému návrhu řešení uvedenému v Implementační analýze a příprava pro ověření ze strany objednatele, alespoň v následujícím rozsahu:

a) Vývoj na straně zhotovitele – vývoj jednotlivých systémů, úpravy existujících produktů, jejich parametrizace a nastavení, vývoj a ověřování integračních rozhraní, součinnost se třetími stranami v souvisejících oblastech.

b) Instalace a implementace do prostředí objednatele v testovacím režimu.

c) Interní ověření na straně zhotovitele a příprava podkladů pro ověření na straně objednatele (dokumentace, organizace testování a další).

d) Příprava a naplnění základních dat – z integračních úloh, číselníky, uživatelé a další.

Provedením těchto činností bude zajištěna připravenost pro ověření ze strany objednatele.

4) **Dodávka předmětu plnění**. Součástí dodávky musí být instalace, upgrade a sestavení předmětu zakázky včetně:

a) Instalace, upgrade a zahoření HW na místě,

b) Instalace a nastavení HW a SW budou provedeny kvalifikovanými osobami pro dané typy zařízení

c) Nastavení HW a aplikací

5) **Zajištění instalace všech součástí dodávky** v určených lokalitách a prostorách objednatele.

6) **Zajištění instalace a připojení** k zařízením a technickým prostředkům zajištěným objednatelem.

7) **Realizace pilotního provozu** k ověření funkčnosti systému na menším obejmu dat, s menším počtem uživatelů a na menším počtu zařízení.

8) **Převedení systémů do zkušebního provozu** a plná podpora uživatelů v rámci zkušebního provozu včetně technické podpory. V této etapě budou realizována požadovaná seznámení s funkcionalitami, obsluhou dodávaného zařízení a budoucím provozem.

9) **Zpracování dokumentace skutečného provedení, systémové a provozní dokumentace** – součástí předmětu plnění je zajištění systémové a provozní dokumentace související s realizací předmětu plnění minimálně v následujícím rozsahu:

Název	Popis
Uživatelská dokumentace	Bude popisovat konkrétní funkčnost z pohledu uživatele tak, aby byl uživatel schopen práce s informačním systémem a pochopil význam jednotlivých částí systému a vazeb mezi nimi. V uživatelské příručce bude popisován způsob práce s jednotlivými částmi systému, vazby mezi nimi včetně popisu součástí jednotlivých částí systému. K usnadnění práce bude sloužit popis jednotlivých obrazovek, ovládacích prvků na obrazovkách a jejich významů, který bude uveden v rámci uživatelské dokumentace.
Dokumentace skutečného provedení a systémová/provozní dokumentace	Obsahuje popis informačního systému (rozhraní a služby) včetně popisu správy informačního systému, definování uživatelů, jejich oprávnění a povinností a detailní popis údržby systému.
Bezpečnostní dokumentace	Účelem bezpečnostní dokumentace je definovat závazná pravidla pro zajištění informační bezpečnosti včetně stanovení bezpečnostních opatření. Součástí této dokumentace bude uveden seznam, který bude obsahovat seznam všech externích zdrojů, ke kterým se jednotlivé servery (součásti systému) připojují, včetně uvedení síťových protokolů, pomocí kterých se s daným externím zdrojem komunikuje. V případě, že na servery (součásti systému) existuje vzdálený přístup, musí být tento přístup jasně specifikován (vzdálené zařízení, síťový protokol) a popsán zdůvodnění takovéhoto přístupu (dohled, správa DB atd.)
Disaster & Recovery Plan	Plán řešení situací v případě výpadků a obnovy funkčnosti systému. Součástí je plán a způsob provádění zálohy a případného způsobu obnovy a obnovy funkčnosti i v případě jiných technických výpadků. Dokument bude vytvářen v součinnosti s objednatelem.
Projektová dokumentace	Smluvní dokumentace, harmonogram realizace projektu, analýzy a prováděcí projekty, zápisy z jednání, protokoly (předávací, akceptační)

Tabulka 18: Dokumentace – požadavky na zpracování

Dokumentace bude dodána v relevantním rozsahu na všechna místa plnění projektu.

Dokumentace bude v souladu se zákonem č. 365/2000 Sb. O informačních systémech veřejné správy a prováděcích právních předpisů, v platném znění.

Dokumenty budou zpracovávány v následujících programech elektronicky a uloženy v následujících formátech:

- MS Office 2010 (MS Word 2010, MS Excel 2010, MS PowerPoint 2010)
- MS Project 2010
- WinZip (formát .zip)

- Portable Document Format (formát .pdf).

Preferovaná forma předávaných dokumentů, které nebudou vyžadovat podpisy konkrétních osob je elektronicky a to na elektronických nosičích (CD, DVD, flash disk, atp.). K předávání a k archivaci souborů se používají média s možností pouze zápisu, nikoliv přepisovatelná.

Veškerá dokumentace bude podléhat schvalování (akceptaci) při převzetí ze strany objednatele.

Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána ve 2x kopiích v elektronické formě ve standartních formátech (MS Office a PDF) používaných objednatelem na datovém nosiči a 1x kopii v papírové formě.

10) **Provedení akceptačních testů.** Zhotovitel je povinen kompletně připravit podklady pro akceptaci dodaného řešení. Součástí akceptace bude akceptační protokol a kompletní předávací dokumentace.
11) **Uvedení systému do produkčního provozu**, zajištění potřebných nastavení a přístupů pro všechny pracovníky objednatele, minimalizace dopadů na provoz objednatele při přechodu a zvýšená podpora bezprostředně po přechodu do produkčního provozu.
12) Zhotovitel dle svého uvážení doplní v nabídce další služby, které jsou dle jeho názoru nezbytné pro úspěšnou realizaci zakázky.
13) Veškeré náklady na zajištění služeb souvisejících s realizací předmětu plnění musí být zahrnuty v ceně odpovídající části předmětu dodávky.

3.5.2 Seznámení s funkcionalitami, obsluhou dodávaných technologií

V této kapitole jsou uvedeny požadavky na seznámení s funkcionalitami, obsluhou dodávaných technologií a jejich budoucím provozem:

1) Zhotovitel proškolí pracovníky objednatele se všemi typy dodaných zařízení a aplikací a problematikou jejich užití, provozu a obsluhy. Zhotovitel se zavazuje poskytnout informace minimálně k následujícím tématům v dostatečném detailu pro porozumění činnosti zařízení a způsobu provozu:
   a) Základní produktové seznámení s jednotlivými dílčími technologickými celky.
   b) Celkové schéma součinnosti jednotlivých zařízení a jejich návaznosti.
   c) Obsluha jednotlivých dílčích modulů, aplikací a technologických celků
   d) Použitá nastavení zařízení, detailnější rozbor použitých konfigurací.
   e) Základní kroky správy, diagnostiky a elementární postupy pro řešení problémů.
2) Poskytnuté informace zajistí seznámení pracovníků objednatele se všemi podstatnými částmi dodávky v rozsahu potřebném pro obsluhu, provoz, údržbu a identifikaci nestandartních stavů systému a jejich příčin.
3) Vše uvedené bude probíhat v prostorách objednatele s využitím vybavení dodaného v rámci této veřejné zakázky, případně zajištěné ze strany objednatele.
4) Konkrétní termíny určí objednatel dle postupu v rámci realizace projektu a dostupnosti zainteresovaných osob.
5) Seznámení s funkcionalitami, obsluhou dodávaných technologií se týká klíčových uživatelů, ostatní uživatelé budou proškoleni klíčovými uživateli.

Veškeré náklady na zajištění těchto činností musí být zahrnuty v ceně odpovídající části předmětu dodávky.

3.6 ZÁRUKY

V této kapitole jsou uvedeny požadavky na záruky dodávky jako celku, případně specificky dílčích částí dodávky.

Objednatel požaduje záruku na veškeré dodané technologie včetně nezbytných provozních a servisních služeb v délce trvání minimálně:

a) 60 měsíců na informační systém(y), aplikace a služby spojené s realizací projektu,
b) 36 měsíců – u HW infrastruktury a systémového SW, pokud není u konkrétního vybavení uvedeno jinak. Delší záruka je uvedena jen u částí, kde je na trhu běžné poskytování delší záruky v pořizovací ceně.
c) 12 měsíců na spotřební materiál, případně drobné vybavení podléhající rychlému opotřebení. Případný spotřební materiál musí být explicitně označen v nabídce a smlouvě a musí být prokázáno, že splňuje tento charakter.

Záruka začíná běžet od okamžiku předání do ostrého (produkčního) provozu. Veškeré opravy po dobu záruky budou bez dalších nákladů pro provozovatele (objednatele). Veškeré komponenty, náhradní díly a práce budou poskytnuty bezplatně v rámci záruky. Zhotovitel ve své nabídce výslovně uvede všechny podmínky záruk.

a) Po dobu záruky na části dodávky musí zhotovitel nebo výrobce všech zařízení garantovat běžnou dostupnost náhradních komponentů a dostupnost servisu.
b) Součástí záruky je i shoda dodávaných systémů s platnou legislativou.
c) Max. doba na odstranění vady díla je 30 dnů od prokazatelného oznámení dodavateli.
d) Zhotovitel uvede provozní služby požadovaného předmětu plnění veřejné zakázky včetně parametrů, které budou předmětem dodávek v rámci záruky systému a v rámci poskytování servisních služeb.

Poskytovatel zajistí HelpDesk pro hlášení vad.

4 HARMONOGRAM

Následující tabulka obsahuje požadovaný časový harmonogram realizace dodávky (T ~ datum účinnosti smlouvy o dílo):

#	Fáze	Doba trvání od zahájení	Doplňující informace
1	Zahájení realizace	0	Zahájení realizace bude dnem podpisu smlouvy na dodávku.
2	Analýza a návrh řešení	45	Zpracování analýzy a návrhu řešení pro potřeby upřesnění podmínek realizace.
3	Dodávka, implementace, instalace, konfigurace HW a SW infrastruktury.	140	Dodávka a implementace HW, SW a síťové infrastruktury.
4	Vývoj a implementace úprav SW, dodávka dokumentace k SW.	140	Vlastní vývoj a implementace úprav IS dle analýzy a návrhu řešení.
5	Ověření funkčnosti dodaných technologií a systémů.	150	Otestování funkčnosti technologií a systémů a ověření jejich plné funkčnosti.
6	Seznámení s funkcionalitami, obsluhou dodávaných technologií	150	Seznámení s funkcionalitami, obsluhou dodávaných technologií
7	Dodávka dokumentace dodaného systému a jeho částí.	150	Min. uživatelská dokumentace, dokumentace skutečného provedení, systémová dokumentace, projektová dokumentace.
8	Převedení do zkušebního provozu.	150	Převedení do zkušebního provozu, odstranění všech vad a nedodělků, dokončení realizace a převedení do ostrého provozu.
9	Bezpečnostní audit a penetrační testy	180	Zpracování a předání bezpečnostního auditu a penetračních testů. *Pozn.: zpracování bezpečnostního auditu bude zahájeno při zahájení realizace. Jedná se o termín předání a akceptace výstupů.*
10	Ukončení realizace dodávky.	180	Součástí je zahájení doby provozu dodaného systému a poskytování servisních služeb.

Tabulka 19: Harmonogram

Doplňující informace:

- Pod pojmem „den“ je míněn kalendářní den.
- Zhotovitel má možnost definovat kratší termíny plnění (v rámci dodávky), nelze zkrátit dobu zkušebního provozu, která musí být min. 30 dnů.
- Zkrácení zkušební doby je možné pouze na základě písemné dohody se Zadavatelem v rámci dodávky.

5 MÍSTA PLNĚNÍ

Realizace předmětu plnění bude probíhat v následujících místech plnění:

Místo	Adresa	Předmět realizace
Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace	Kamenice 798/1d, Brno PSČ: 625 00	Primární datové centrum ZZS JMK – dodávky v návaznosti na technologie umístěné v tomto DC a dodávka částí technologie. Primární lokalita, kde je provozován IS ZOS a kde je primární ZOS. Současně se jedná o primární lokalitu IS elektronická pošta. Sídlo ZZS JMK – místo předání výstupů projektu.
Záložní zdravotnické operační středisko ZZS JMK a záložní datové centrum	HZS Lidická 61 602 00 Brno	Záložní zdravotnické operační středisko ZZS JMK (ZZOS) a záložní datové centrum pro toto ZZOS, kde bude umístěna dodaná technologie ZZOS a které bude propojeno s primárním datovým centrem ZZS JMK.

Tabulka 20: Místa plnění

6 VÝCHOZÍ STAV

V této kapitole je uveden výchozí stav a výchozí podmínky pro dodávku předmětu plnění.

6.1 ZDRAVOTNICKÁ ZÁCHRANNÁ SLUŽBA JIHOMORAVSKÉHO KRAJE, PŘÍSPĚVKOVÁ ORGANIZACE (ZADAVATEL)

Kontext ZZS JMK v rámci řešení projektu je následující:

1. ZZS JMK plní úkoly zdravotnické záchranné služby k zajištění zvláštní zdravotní péče fyzickým osobám, které se náhle nebo nečekaně ocitly v ohrožení zdraví či života, tedy nepřetržitě zabezpečuje odbornou přednemocniční neodkladnou péči včetně přednemocniční péče o dárce a příjemce orgánů v souladu s příslušnými právními předpisy a pokyny zřizovatele a za plnění těchto úkolů odpovídá.
2. V rámci svých činností ZZS zajišťuje kvalifikovaný příjem, zpracování a vyhodnocení tísňových výzev k odborné zdravotnické první pomoci a určení nejvhodnějšího způsobu poskytování přednemocniční neodkladné péče.
3. ZZS je společně s PČR a HZS součástí a základní složkou Integrovaného záchranného systému (IZS), v rámci kterého vykonává svou činnost nejen v době míru, ale i v případě mimořádných událostí (dle zákona 239/2000 Sb.) a krizových situací (dle zákona 240/2000 Sb.) a další činnost dle legislativy.
4. ZZS JMK musí zajistit výkon veřejné správy v oblasti zdravotnické záchranné služby a podmínky pro zajištění připravenosti poskytovatele zdravotnické záchranné služby (ZZS JMK) na řešení i v případě mimořádných událostí a krizových situací (dle zákona č. 374/2011 Sb.) **a kybernetických bezpečnostních událostí** (dle zákona č. Zákon č. 181/2014 Sb.).
5. Pro tyto činnosti využívá informační systémy a technologie pro:
    a. podporu činností zdravotnického operačního střediska (ZOS) a posádek v terénu, vč. Komunikace s posádkami, mezi posádkami a složkami IZS. Soubor technologií a subsystémů se nazývá informační systém zdravotnického operačního střediska (IS ZOS).
    b. Pro podporu komunikace mezi zaměstnanci ZZS JMK je využívána elektronická pošta.

V následujícím textu je uveden současný stav informačních systémů a technologií a další relevantní informace.

6.2 INFORMAČNÍ A KOMUNIKAČNÍ SYSTÉMY K ZABEZPEČENÍ

V rámci projektu budou realizována opatření k zabezpečení ostatních informačních systémů (IS) ZZS JMK. V rámci projektu nebudou realizována opatření k zabezpečení kritické informační infrastruktury (KII), žádného informačního systému základních služeb (ISZS) ani žádného významného informačního systému.

Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace bude zabezpečovat své informační (IS) a komunikační systémy (KS). Stručný výčet IS je uveden v dalším textu této kapitoly.

Všechny uvedené IS jsou umístěny, provozovány a využívány uživateli v sídle ZZS JMK na adrese Kamenice 798/1d, 625 00 Brno. V této lokalitě je umístěno primární datové centrum i většina pracovišť uživatelů IS.

IS ZOS je také částečně provozován v lokalitě záložního zdravotnického operačního střediska ZZS JMK a záložního datového centra v objektu HZS v lokalitě Lidická 61, Brno. ZZS JMK má v záložní lokalitě k dispozici dispečerská pracoviště a repliku systému operačního řízení (část IS ZOS), kterou je možné

aktivovat a provozovat jako základní dispečink v této lokalitě a ZZOS se bude rozšiřovat o další součásti IS ZOS. Část technických opatření je zaměřena i na zabezpečení ZZOS tak, aby byla zajištěna provozuschopnost a bezpečnost provozovaných IS i v případě kybernetických bezpečnostních událostí, mimořádných událostí a krizových situací i v této lokalitě.

Žádný ze zabezpečovaných IS, ani žádná z jejich součástí, netvoří systém určený k ochraně utajovaných skutečností dle zákona č. 412/2005 Sb. O ochraně utajovaných informací a o bezpečnostní způsobilosti (ISOUI).

Uvedené IS nejsou informačními systémy základní služby podle §2, písm. I), bod 5 a písm. J) ZKB a ZZS JMK nebyla Národním úřadem pro kybernetickou a informační bezpečnost určena jako provozovatel základní služby podle §22a ZKB.

V následující tabulce je uveden výčet IS, které jsou určeny k zabezpečení a vůči nimž budou realizována technická opatření:

Název IS / KS	Správce	Stručný popis	Typ
IS ZOS	Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace	Informační systém a technologie pro podporu činností zdravotnického operačního střediska (ZOS) a posádek v terénu, vč. Komunikace s posádkami, mezi posádkami a složkami IZS. Jedná se o soubor technologií a subsystémů společně zajišťující podporu uvedených procesů. Jedná se o primární IS sloužící pro hlavní činnost ZZS JMK, tj. poskytování PNP na území Jihomoravského kraje. Součástí IS ZOS je jeho záložní část (ZZOS) umístěná do záložní lokality, která slouží pro zajištění poskytování PNP v případech, kdy toto není možné v primární lokalitě.	Informační systém (IS)
Elektronická pošta	Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace	Systém pro příjem a odesílání elektronické pošty v rámci komunikace ZZS JMK. Jedná se o hlavní informační systém (IS) ZZS JMK zajišťující komunikaci mezi zaměstnanci ZZS JMK a podporu výkonu jejich činností.	Informační systém (IS)

Tabulka 21: Výčet IS k zabezpečení

Detaily k uvedeným IS jsou uvedeny v následujícím textu a to jejich aktiva, části a další technické a provozní parametry relevantní pro dodávku.

6.2.1 IS ZOS

V této kapitole je detailně popsán IS ZOS a to včetně dotčených aktiv.

6.2.1.1 Informační systémy a aplikační software ZOS

V této kapitole je uveden stávající stav informačních systémů a aplikačního software pro stávající ZOS:

IS, SW, subsystém	Výchozí stav
IS OŘ	Jedná se o produkt SOS společnosti PER4MANCE s.r.o. využívaný ze strany 9 ZZS v ČR a min. jedné zahraniční ZZS (Maďarsko), tj. jedná se o široce používaný a standardizovaný produkt/systém. SOS je systém pro operační řízení dispečinku Zdravotnické záchranné služby (ZZS). Systém byl vyvinut na základě dlouhodobých zkušeností s provozem krajských ZZS se zahrnutím moderních požadavků na efektivní řízení Krajských záchranných operačních středisek (ZOS). Poskytuje funkcionalitu pro všechny činnosti ZOS ZZS počínaje náběrem tísňové výzvy (calltaking) přes operační řízení po vyhodnocení činnosti ZOS. Základní moduly implementované na ZZS JMK: 1. Dispečink 2. Základna 3. Správa směn 4. Evidence směn 5. Svolávání 6. Statistiky 7. Kontrolní pracoviště 8. Kniha Jízd 9. Administrace 10. Správa stanic Současně s tímto jsou implementovány následující integrace: 1. Interní (v rámci IS ZOS) a. Integrace telefonie – příjem tísňové výzvy. b. Integrace na GIS – zobrazení polohy tísňové výzvy, polohy vozidla, lokalizace události v mapě a zobrazení dalších objektů při práci dispečera pod. c. Integrace na systém sledování vozidel – předávání výzvy k výjezdu, příjem a sledování stavů, sběr informací o výjezdu vozidel. d. MZD/EKP – předávání dat o události a pacientovi/pacientech k výjezdu pro posádku/posádky. e. Integrace na záznamový systém – připojování záznamů hovorů, zachycení nahrávek obrazovek dispečerského pracoviště a přehrávání vzniklých záznamů apod. f. Národní dopravně informační centrum – odesílání informací do NDIC o dopravních nehodách ze zaznamenaných událostí.

IS, SW, subsystém	Výchozí stav
	g. Integrace telekomunikací a radiokomunikací – pro ovládání spojení telefonů a RS. 2. Externí a. Národní informační systém IZS (NIS IZS) – výměna dat o událostech a SaP s tímto systémem. b. RUIAN – aktualizace dat adres dle Registru územní identifikace, adres a nemovitostí (data jsou čerpána z veřejného rozhraní RUIAN a je ukládána jejich offline kopie). c. Integrace s poskytovateli zdravotních služeb v rámci projektu eHealth JMK. Součástí je řada dalších důležitých funckionalit, které jsou popsané v dokumentaci k IS. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací.
GIS	Geografický systém je zajištěn produktem Fleetware od společnosti RADIUM s.r.o. Základní funkcionality jsou: 1. Zobrazení mapových podkladů a základní práce s mapou na všech pracovištích. 2. Zobrazování poloh a stavů vozidel ZZS ze systému sledování vozidel (AVL). 3. Zobrazování poloh událostí SaP dalších spolupracujících složek IZS v rámci integrace na NIS IZS. 4. Lokalizace pro IS OŘ, vyhledávání jiných objektů při práci dispečera v mapě a další geografické služby. Současně s tímto jsou realizovány následující integrace: 1. Interní (v rámci IS ZOS) a. IS OŘ – lokalizace, zobrazování výzev, událostí, poloh vozidel a další služby. b. Systém sledování vozidel (AVL) – čerpání poloh a stavů vozidel a jejich zobrazování v mapě. 2. Externí a. Národní informační systém IZS (NIS IZS) – výměna dat o událostech a SaP s tímto systémem. Součástí je řada dalších důležitých funckionalit, které jsou popsané v dokumentaci k IS. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací.

IS, SW, subsystém	Výchozí stav
EKP/MZD	Jedná se o produkt společnosti EMD dodaný a využívaný většinou ZZS v ČR. Elektronická karta pacienta (EKP) slouží pro zaznamenávání všech relevantních údajů o výjezdech a pacientech v rámci těchto výjezdů. Data jsou na vstupu čerpána z IS OŘ a následně během nebo po ukončení výjezdu z MZD, kontrolována a následně zpracována do formy pro vykazování pojišťovnám. Mobilní sběr dat (MZD) o pacientech slouží pro zadávání dat o pacientech v rámci výjezdu ZZS v terénu prostřednictvím mobilních zařízení (tabletů) a následně jejich předávání do centrálního systému EKP pro následné zpracování. Systémy poskytují následující funkce: 1. Přebírání dat o výjezdu z IS OŘ (součástí integrace). 2. Posílání dat do mobilních zařízení posádek v terénu. 3. Funkčnost pro vyplnění posádkami v terénu. 4. Předání z MZD zpět do EKP. 5. Přebírání dat ze systému sledování vozidel. 6. Následné úpravy, dopracování, kontrola dat na výjezdových základnách. 7. Předávání do IS Pojišťovna. Současně s tímto jsou realizovány následující integrace: 1. Interní (v rámci IS ZOS) a. IS OŘ – přebírání dat k výjezdu pro následné předání posádkám. b. Nahrávací systém (REDAT) – přebírání lokalizace volajícího. c. Systém sledování vozidel (AVL) – informace o výjezdu z vozidel. d. IS Pojišťovna – předávání zpracovaných dat z výjezdu pro vyúčtování zdravotním pojišťovnám. 2. Externí a. Nejsou. Součástí je řada dalších důležitých funckionalit, které jsou popsané v dokumentaci k IS. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací. **Subsystém nepodporuje zavedení elektronické zdravotnické dokumentace, kterou je třeba do subsystému doplnit.**
IS Pojišťovna	Jedná se o produkt společnosti EMD dodaný a využívaný většinou ZZS v ČR. Slouží pro vyúčtování poskytnuté zdravotnické péče zdravotním pojišťovnám. Současně s tímto jsou realizovány následující integrace: 1. Interní (v rámci IS ZOS) a. EKP/MZD – přebírání dat o pacientech a výjezdech pro vyúčtování. 2. Externí

IS, SW, subsystém	Výchozí stav
	a. Informační systémy zdravotních pojišťoven. Součástí je řada dalších důležitých funckionalit, které jsou popsané v dokumentaci k IS. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací.
Systém sledování vozidel (AVL)	Jedná se o produkt Fleetware od společnosti RADIUM s.r.o. Základní funkcionality jsou: 1. Sledování polohy a stavu vozidel ZZS. 2. Předávání těchto stavů, vč. Doprovodných údajů z vozidel do IS OŘ a EKP. 3. Předávání dat pro zobrazení polohy a stavů vozidel v mapě. 4. Zasílání výzvy do vozidel. Současně s tímto jsou realizovány následující integrace: 1. Interní (v rámci IS ZOS) a. IS OŘ – poskytování stavů vozidel a výjezdů. b. GIS – zobrazování poloh a stavů vozidel v mapě. c. Poskytování poloh a stavů vozidel do NIS IZS v rámci součinnosti. 2. Externí a. Národní informační systém IZS (NIS IZS) – výměna dat o událostech a SaP s tímto systémem. Součástí je řada dalších důležitých funckionalit, které jsou popsané v dokumentaci k IS. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací. Subsystém realizuje vlastní sledování vozidel ZZS a mimo to předává informace o výjezdech do konkrétních vozidel dle přiřazení jednotlivých událostí do IS OŘ. Tato data jsou systémem AVL mazána (po 24 hod.) a nejsou tak v DB dlouhodobě uchovávána. Tato data tak nejsou nijak v rámci systému AVL modifikována a jsou pouze předávána konkrétnímu vozidlu a dostupná pro dispečerská pracoviště řešící aktuální operační situaci.
Svolávací systém	Je součástí IS OŘ – viz výše. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací. Integrační rozhraní jsou: 1. Svolávací systém ZZS JMK: webové služby 2. Svolávací systém jiné ZZS: webové služby, rozhraní bude totožné jako u ZZS JMK, přesné určení ZZS bude při zahájení dodávky.

IS, SW, subsystém	Výchozí stav
	Přesný popis a definice integračních rozhraní budou předány v rámci implementační analýzy.
Telefonní ústředna	Telefonní ústředna je produkt Siemens. Telefonní ústředna připojená na příjem tísňové linky 155 u telekomunikačního operátora. Telefonní ústředna je interně napojena na: 1. Nahrávací systém (REDAT) pro nahrávání veškerých hovorů a přebírání lokalizace hovorů. 2. Integrace telefonie a radiofonie pro řízení a obsluhu volání přes ústřednu. Součástí je řada dalších důležitých funckionalit, které jsou popsané v dokumentaci k IS. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací.
Záznamový systém (REDAT)	Jedná se o produkt ReDat společnosti RETIA, a.s. Záznamový systém (REDAT) slouží pro záznam telefonních hovorů na tísňové lince, záznam všech hovorů na ZOS, a to jak telefonních, tak radiofonních. Záznamový systém je integrována na: 1. Telefonní ústřednu – záznam hovorů. 2. Integraci telefonie a radiofonie – pro záznam radiového hovoru. 3. IS telekomunikačního operátora – přebírání polohy volajícího v rámci příjmu tísňové výzvy. 4. IS OŘ – předávání polohy volajícího v rámci příjmu tísňové výzvy. Součástí je řada dalších důležitých funckionalit, které jsou popsané v dokumentaci k IS. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací.
Integrace telefonie a radiofonie	Jedná se o produkty společnosti Komcentra s.r.o. Integrace telefonie a radiofonie zajišťuje propojení IS OŘ s telefonií (telefonní ústředna), obsluhou radiové sítě Pegas/Matra MV ČR, záznamovým zařízením a poskytuje obsluze jednotný, a hlavně jednoduchý systém obsluhy pomocí dotykové obrazovky na pracovišti operátora. Základní funkcionality a integrace jsou: 1. Zajištění integrace a obsluhy telefonní komunikace prostřednictvím telefonní ústředny. 2. Zajištění integrace a obsluhy radiofonní komunikace prostřednictvím radiové sítě Pegas/Matra. 3. Integrace s IS OŘ – volání, návaznost hovorů na výzvy a události.

IS, SW, subsystém	Výchozí stav
	4. Záznamové zařízení (REDAT) – nahrávání radiofonní komunikace. 5. Poskytnuté aplikace na dotykové obrazovce obsluhy. Součástí je řada dalších důležitých funckionalit, které jsou popsané v dokumentaci k IS. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací.
Záložní IS ZOS (ZZOS)	ZZS JMK má v externí lokalitě (HZS, Lidická 61, Brno) k dispozici dispečerská pracoviště a repliku systému operačního řízení (část IS ZOS), kterou je možné aktivovat a provozovat jako základní dispečink v této lokalitě. V rámci ZZOS nejsou implementovány další technologie jako je MZD/EKP, AVL apod. Hlasová komunikace v rámci ZZOS je realizována pomocí mobilních telefonů a ručních radiostanic.

Tabulka 22: IS ZOS

6.2.1.2 Pracoviště ZOS

V následující tabulce je uveden popis pracovišť operátorů na ZOS, na kterých je provozován IS ZOS a jeho součásti:

Prvek	Údaje, parametry a informace
Počet pracovišť	Počet pracovišť: - Primární ZOS: 12 - Záložní ZOS: 4 Další položky se týkají každého jednotlivého pracoviště. Počet stávajících pracovišť na primárním ZOS – jedná se o pracoviště operátorů a vedoucího směny.
Virtualizovaný desktop / PC	Počet ks / pracoviště: 1 Operační systém: MS Windows 7/Windows 10 Možnost připojení až 4 monitorů full HD (1920x1080) DVI/HDMI/DP Velikost paměti min.: 2 GB DDR3 SDRAM Podporované protokoly: Citrix ICA 12 (Citrix Online Plugin 12); Microsoft RDP 7; VMWare ViewManager 4.5 a vyšší, pro virtualizované pracoviště. Síťové rozhraní: 10/100/1000 Gigabit Ethernet Porty: USB 2.0 a USB 3.0, 4x DVI/HDMI/DP, 1 RJ-45, 1 sluchátka, 1 vstup pro mikrofon, podpora dotykových obrazovek U dotykových monitorů podpora kurzoru nezávislého na kurzoru myši.
Klávesnice	Počet ks / pracoviště: 1 Standardní plnohodnotná klávesnice.

Prvek	Údaje, parametry a informace
Myš	Počet ks / pracoviště: 1
LCD monitory	Počet ks / pracoviště: 3 Velikost panelu: úhlopříčka 61 cm (24“) Rozlišení 1920x1080 Technologie podsvícení LED Konektivita: 1 konektor DVI-D, 1 konektor VGA (Video GraphicsArray), 1 port USB 2.0 pro odesílání dat, 2 porty USB 2.0 pro periferní zařízení Uchycení na stojan: VESA 100mm Přídavné reproduktory na spodní hraně monitoru
Dotykový LCD monitor	Počet ks / pracoviště: 1 Typ panelu: LCD Velikost panelu: 19“ Rozlišení: 1280x1024 Konektor: DVI/HDMI, USB a RS232 Uchycení na stojan: VESA 100mm
IP telefon	Počet ks / pracoviště: 1 Kompatibilní s integrací telefonie a telefonní ústřednou.
Náhlavní souprava	Počet ks / pracoviště: 1 Drátová náhlavní souprava

Tabulka 23: Pracoviště ZOS

6.2.2 Elektronická pošta

Systém pro příjem a odesílání elektronické pošty v rámci komunikace ZZS JMK. Část primární činnosti ZZS JMK, tj. poskytování PNP není podpořena IS ZOS (popsaný v předchozí kapitole), protože se jedná o ad-hoc postupy při situacích, které nejsou zcela běžné a vyžadují individuální přístup. Jedná se o nestandardní situace v běžném provozu, mimořádné události, krizové situace a samozřejmě kybernetické bezpečnostní události, případně incidenty. Současně s tímto není do primárních procesů v IS ZOS zapojeno vedení a technickohospodářský personál ZZS JMK zajišťující podporu hlavní činnosti ZZS JMK, tj. poskytování PNP.

Bez zajištění výměny informací (dokumentů, dat) mezi uvedenými skupinami uživatelů a při uvedených situacích, není možné garantovat poskytování PNP ze strany ZZS JMK, protože nebude možné řešit provozně technické problémy provozu při poskytování PNP.

Pro zajištění komunikace a výměny informací (dokumentů, dat) za uvedených situací a mezi uživateli zajišťující řízení poskytování PNP (personál ZOS) a vedením, resp. technickohospodářskými pracovníky, je využíván informační systém elektronické pošty.

Jedná se o hlavní informační systém (IS) ZZS JMK zajišťující komunikaci mezi zaměstnanci ZZS JMK a podporu výkonu jejich činností jak při standardních situacích, tak při nestandardních situacích, jak je uvedeno dříve v tomto textu.

Elektronická pošta je provozována jako samostatný informační systém ZZS JMK a je provozována v datovém centru ZZS JMK, tj. nejedná se o hosting ani službu.

Všichni uživatelé v rámci personálu ZZS JMK mají instalovány klienty tohoto IS, případně jsou napojení z obdobných klientů v rámci mobilních zařízení.

Komunikace mezi serverem a klienty je šifrovaná, přístup je na základě identifikace a autorizace uživatele (napojení na AD), nicméně neprobíhá systematický sběr logů (provozních dat) a vyhodnocení kybernetických bezpečnostních událostí.

Elektronická pošta je provozována následujícím způsobem:

1. Je provozována v primárním datovém centru ZZS JMK – detaily viz kap. 6.3 – Umístění v rámci virtualizovaného prostředí.
2. Systém elektronické pošty využívá systém Kerio Connect ve verzi 9.x na OS Ubuntu a je složen ze dvou částí:
    a. Centrální mail server – umístěn v interní síti pro 780 uživatelů
    b. Mail Realy server včetně antivir a antispam komponent – umístěn v DMZ
1. Aktiva jsou sdílenými aktivy v rámci primárního DC v rámci virtualizované infrastruktury (viz výše detailní popis k IS ZOS). V rámci projektu budou zabezpečena jen centrální aktiva v DC.
2. Provoz je zajištěn v režimu 7x24x365 – Elektronická pošta sice není kritickým systémem, ale je provozována nonstop z důvodu specifického provozu ZZS.
3. Součástí projektu jsou nástroje pro sběr dat a vyhodnocení kybernetických bezpečnostních událostí, tj. technické opatření „h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí“. Nástroje pro sběr dat a vyhodnocení kybernetických bezpečnostních událostí budou také zpracovávat i bezpečnostní logy centrálního mailového systému ZZS a vyhodnocovat tak případné bezpečnostní události v rámci systému elektronické pošty.

6.3 UMÍSTĚNÍ IS ZOS, ZZOS, SYSTÉMU ELEKTRONICKÉ POŠTY A DC

V následující tabulce jsou uvedena umístění IS ZOS:

Místo	Adresa	Předmět realizace
Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace	Kamenice 798/1d, Brno PSČ: 625 00	Datové centrum ZZS JMK a všechna aktiva IS ZOS a systému elektronické pošty jsou umístěná v tomto DC. Dispečerská pracoviště ZOS, kde jsou aktiva (pracoviště) operátorů ZOS.
Záložní zdravotnické operační středisko ZZS JMK a záložní datové centrum	HZS Lidická 61 602 00 Brno	Záložní zdravotnické operační středisko ZZS JMK a záložní datové centrum jsou umístěny v externí lokalitě v objektu HZS. V této lokalitě je umístěna technologie ZZOS, která je propojena s primárním datovým centrem ZZS JMK a primárním IS ZOS. V lokalitě je dostupná DB replika systému operačního řízení a dvě dispečerská pracoviště vybavena PC. Hlasové spojení je realizováno pomocí krizových mobilních přístrojů a ručních radiostanic. Předmětem projektu bude

Místo	Adresa	Předmět realizace
		zabezpečení i aktiv záložního IS ZOS umístěného do tohoto DC.

Tabulka 24: Umístění

6.4 STAV OSTATNÍCH INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ

V této kapitole je uveden základní popis výchozího stavu jednotlivých prvků ostatních informačních a komunikačních technologií.

6.4.1 Datové centrum, HW infrastruktura, systémový SW

V následující tabulce je uveden popis datového centra, HW infrastruktury a systémového SW:

Parametr	Údaj(e), parametry a informace
Datové centrum	
Záložní zdroj el. energie	Celá serverovna je zálohována diesel agregátem, který zajistí dodávku napájení při delších výpadcích napájení. Pro kratší výpadky je technologie napojena na bateriové záložní zdroje el. energie (UPS)
HW infrastruktura	
Rackové skříně	Veškerá technologie v rámci serverovny je umístěna v RACK skříních, které jsou umístěny ve dvou řadách s dostupností jak zepředu, tak zezadu. Pro nově dodávané technologie ZZS zajistí umístění v rozsahu max. 10 U. Konkrétní umístění a zapojení budou předmětem implementační analýzy.
Servery	Jako virtualizační servery jsou využívány tři servery DELL PowerEdge R720. Servery jsou osazeny síťovým rozhraním jak na technologii Gigabit ethernet, tak také TenGigabitethernet.
Disková úložiště	Úložiště je realizováno diskovým polem DELL EqualLogic řady PS6xxx 10Gbps iSCSI a doplněno polem pro odkládání záloh QNAP NAS, který je také osazený 10Gbit rozhraním. Pro komunikaci diskových polí jsou vyhrazeny dva 10Gbps switche DELL, které tak tvoří infrastrukturu pro iSCSI.
Systémový SW	
Operační systémy	V rámci dodávky virtualizačních serverů jsou k dispozici licence Windows Server. Pro vybrané dodávky ZZS zajistí prostředí včetně OS (viz jednotlivé kapitoly). Konkrétní umístění a nastavení bude předmětem implementační analýzy.
Virtualizační SW	Pro virtualizační servery je využito licencí VMware verze 6.x. VMware: 1. VMware vCenter Server 6 Standard for vSphere 6 2. VMware vSphere 6 Standard (6 CPU).

Parametr	Údaj(e), parametry a informace
DB	V rámci IS ZOS jsou využity databázové licence, a to jak ORACLE, tak Microsoft SQL server. Nepředpokládá se jejich využití pro dodávky v rámci tohoto projektu.
Dohled	V rámci infrastruktury ZZS je využíván produkt WhatsUp Gold firmy IPSwitch pro dohled a monitoring infrastruktury. ZZS poskytne součinnost pro zapojení nově dodávaných technologií do dohledu. Konkrétní nastavení bude předmětem implementační analýzy.
Syslog server	V rámci stávající infrastruktury je provozován syslog server Syslog-ng. HW DELL PowerEdge R740, 1xCPU 16core, 32GRAM, 5x4TB 7,2k, 3x 1,92TB SSD.
Proxy server	V rámci stávající infrastruktury je využíván pro přístup do sítě internet proxy server Cisco Web Security Appliance
Reverzní proxy	Pro chod některých aplikací je využívána reverzní proxy umístěná v DMZ
Wifi sítě	Pro připojení do sítě ZZS prostřednictvím WiFi je využívána infrastruktura přístupových bodů (access pointů) rozmístěných v rámci WAN ZZS a řízených centrálním řídícím prvkem WLC. V rámci WiFi připojení je využíváno více oddělených SSID pro různé technologie a určení.
Personální systém	V rámci stávajících systémů je využíván personální systém VEMA včetně modulu pro MS Active Directory.
Zálohování	Zálohování virtualizovaného prostředí je realizováno v rámci nastavených zálohovacích scénářů pomocí SW Veeam Backup pro VMware. ZZS poskytne součinnost pro zapojení nově dodávaných technologií do zálohování. Konkrétní nastavení bude předmětem implementační analýzy.
Autentizační server	V rámci stávající infrastruktury jsou využíván pro autentizaci VPN připojení autentizační servery RADIUS realizované jako služba Network Policy Server (NPS) v rámci Microsoft Windows serverů napojených na stávající Active Directory.
Doména – Active Directory	V rámci infrastruktury je využívána stávající doména v rámci Microsoft Windows 2012R2 – MS Active Directory. V rámci MS Active Directory jsou definováni všichni uživatelé. Doména MS Active Directory bude využita pro autentizaci a autorizaci dle zadání. ZZS v rámci součinnosti poskytne AD a odpovídá i za její licencování. Současný počet aktivních uživatelů je cca 800.
Antivirové řešení	Pro řešení antivirové ochrany na koncových stanicích a Windows serverech je využívána licence systému ESET Endpoint Antivirus včetně centrální správy.

Tabulka 25: Datové centrum, HW infrastruktura, systémový SW

6.4.2 Datové sítě

V rámci projektu budou využity následující sítě:

Datová síť	Popis
WAN ZZS	Bude využita pro komunikaci mezi lokalitami z důvodu nutné výměny dat souvisejících s realizací a provozem projektu.
Internet	V centrální lokalitě je zajištěno připojení k internetu, které bude možné využít i pro požadavky technologií v rámci realizace a provozu projektu.

Tabulka 26: Datové sítě

6.4.3 Síťová infrastruktura

V následující tabulce je uveden popis síťové infrastruktury:

Parametr	Údaj(e), parametry a informace
Primární datové centrum ZZS	
Směrovače	Lokality ZZS jsou propojeny do jedné WAN sítě. Pro tyto účely jsou všechny lokality vybaveny směrovačem WAN operátora. Tyto směrovače jsou ve správě WAN operátora. Stávající WAN operátor jsou Radiokomunikace.
Firewally	V rámci centrální lokality je umístěn centrální FireWall Cisco ASA 5515 s FirePower (IPS/AMP), který zajišťuje zabezpečení WAN ZZS do sítě Internet a v rámci konfigurace centrálního FW jsou ukončovány i VPN přístupy pracovníků ZZS a externích firem do sítě ZZS. VPN přístupy jsou autentizovány a autorizovány v rámci RADIUS serverů (viz výše). V rámci záložní lokality ZZS je umístěn FireWall ASA 5510. FireWally oddělují interní síť ZZS nejenom od sítě Internet, ale i od ostatních externích sítí jako je NIS IZS apod.
LAN	V rámci centrální lokality jsou realizovány LAN prvky, a to na bázi switchů. Přičemž centrální stack switchů Cisco Catalyst 3750 realizuje i routování VLAN segmentů LAN sítě.
Připojení k síti NIS IZS - MV ČR NIS IZS a PČR	V rámci centrální serverovny je realizováno i napojení na síť NIS IZS a síť PČR. Toto je realizováno samostatnými zálohovanými linkami ve správě NAKIT a tuto síť garantuje MV ČR.
Připojení k internetu	V centrální lokalitě je i centrální napojení do sítě Internet. Toto připojení je zabezpečeno FireWallem (viz výše). Poskytovatelem připojení do sítě Internet je CESNET.

Tabulka 27: Síťová infrastruktura

6.4.4 Provoz

Provoz stávajícího řešení je zajišťován s následujícími parametry:

1. Provoz systému je v režimu 7x24x365 – jedná se o kritický systém, jehož služby jsou uživatelům k dispozici nonstop, protože ZZS poskytuje služby a plní své úkoly nonstop.

2. IS ZOS je provozován jako vysoce dostupný systém s řadou redundantních prvků přispívajících k vysoké dostupnosti a zajištění funkčnosti i v případech výpadků některých prvků.
3. V rámci provozu je zajištěn dohled, jak je uvedeno dříve v tomto dokumentu.
4. V rámci provozu je zajištěno zálohování, jak je uvedeno dříve v tomto dokumentu.
5. Technická a technologická podpora systému:
    a. Je zajišťována v režimu 7x24x365, aby byla zajištěna vysoká dostupnost dle předchozího bodu.
    b. Součástí je maintenance technologií a dodaného SW, technická a technologická podpora nad rámec záruky s kratšími SLA než v případě záruky.
    c. Je poskytován 1st level support, vyhodnocení hlášených problémů a řešení závad ze strany dodavatele a poskytovatele služeb technické a technologické podpory.
6. Administrace systému je v zodpovědnosti správců ZZS JMK.
7. V rámci provozu také probíhají:
    a. Nezbytné úpravy systému vyplývající ze změn legislativy, vyhlášek, případně dalších závazných dokumentů.
    b. Rozvoj systému v návaznosti na nové potřeby ZZS JMK.
    c. Pozáruční servis HW a SW infrastruktury.

Zajištění provozu u stávajících IS a technologií musí být zachováno min. v tomto rozsahu.

KONEC ZÁKLADNÍ ČÁSTI DOKUMENTU

Příloha č. 2 Smlouvy o dílo - Podrobný popis nabízeného plnění

Popis navrhovaného řešení zpracovaný na základě požadavků Příloha č. 3 Technická specifikace dodávky.

Požadavek:

Popis nabízeného plnění, ze kterého bude zadavatel schopen posoudit naplnění požadavků zadavatele stanovených v zadávací dokumentaci. V popisu nabízeného řešení budou uvedeny i všechny podmínky záruk a licenční podmínky.

K prokázání splnění technických podmínek dodavatel v rámci své nabídky předloží podrobný popis nabízeného plnění dodávky (nikoliv servisních služeb), ze kterého bude zadavatel schopen posoudit naplnění všech požadavků zadavatele stanovených v zadávací dokumentaci. V popisu nabízeného řešení budou uvedeny i všechny podmínky záruk a licenční podmínky. V případě, že dodavatel v rámci své nabídky nepředloží popis nabízeného plnění nebo popis nabízeného plnění bude neúplný nebo nabízené plnění uvedené v popisu nebude splňovat požadavky zadavatele stanovené v zadávací dokumentaci, může být účastník vyloučen z další účasti v zadávacím řízení. Popis nabízeného plnění dodávky vybraného dodavatele se stane přílohou smlouvy o dílo (příloha č. 1 zadávací dokumentace).

V této příloze jsou uvedeny výchozí podmínky a požadavky na dodávku v rámci této veřejné zakázky.

OBSAH

VYUŽITÉ ZDROJE

Nejsou

SEZNAM TABULEK

1 PODROBNÝ POPIS NABÍZENÉHO PLNĚNÍ

V této kapitole je uveden podrobný popis nabízeného plnění a to tak, aby byl zadavatel schopen posoudit naplnění všech požadavků zadavatele stanovených v zadávací dokumentaci. V popisu nabízeného řešení budou uvedeny i všechny podmínky záruk a licenční podmínky.

Předmětem plnění veřejné zakázky (dílem) je komplexní dodávka a implementace technologií, dodávky SW, HW a infrastruktury pro realizaci technických bezpečnostních opatření dle § 5 odst. 3) zákona č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB) pro zabezpečení IS provozovaných Zadavatelem, kterým je Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace. Součástí plnění VZ jsou dále servisní služby po dobu udržitelnosti projektu.

Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace je základní složkou IZS a v souladu s legislativou plní úkoly i v případě mimořádných událostí a krizových situací, kdy mohou být těmito událostmi/situacemi zasaženy i informační systémy (IS) ZZS JMK a došlo by tedy k omezení, případně znemožnění plnění úkolů ZZS JMK.

Konkrétně se jedná o zvýšení kybernetické bezpečnosti pro následující IS:

- Informační systém zdravotnického operačního střediska ZZS JMK – jedná se o primární IS sloužící pro hlavní činnost ZZS JMK, tj. poskytování PNP na území ZZS JMK.
- Elektronická pošta – jedná se o hlavní informační systém (IS) ZZS JMK zajišťující komunikaci mezi zaměstnanci ZZS JMK a podporu výkonu jejich činností.

1.1 PODROBNÝ POPIS JEDNOTLIVÝCH ČÁSTÍ NABÍZENÉHO PLNĚNÍ

1.1.1 FireWall s IPS pro ZZOS

Nabízené řešení je v souladu s požadavky na FireWall s IPS pro ZOS dle ZD.

Jako firewall s IPS pro řízení bezpečného přístupu mezi vnějšími sítěmi (internet, NIS IZS, PČR atd.) a vnitřní sítí ZZOS a ZOS nabízíme řešení Cisco Systems ASA 5516-X with FirePOWER services, 8GE, AC, 3DES/AES. Bude se jednat o dodávku jednoho HW FireWallu s požadovanými výkonnostními parametry s možností rozšíření o další redundantní box (není součástí dodávky) s možností konfigurace HA režimu.

Tento FireWal bude doplněn licencí „Cisco ASA5516 FirePOWER IPS and AMP“ pro řešení požadavků ZD na Aplikační firewall a IPS senzor. Pro tuto licenci bude navíc instalována management console ve virtuálním dodávané infrastruktury „Cisco Firepower Management Center, (VMWare) for 2 devices“, který umožní konfiguraci vlastností IPS a AMP až dvou FireWallů z jedné management console.

Pro řešení VPN koncentrátoru bude nabízené řešení doplněno o licenci „Cisco AnyConnect 25 User“, která zajistí požadované funkčnosti VPN koncentrátoru pro vzdálené připojení SSL VPN. Licence site-to-site a IPSec pro 300 současně připojených uživatelů/ipsec tunelů je součástí ASA 5516-X.

Součástí dodávky je podpora na 5 let typu NBD, oprava v místě instalace zařízení včetně aktualizací všech signatur a SW komponent včetně jejich funkčnosti

Součástí implementace (montáž, instalace, konfigurace, zaškolení a seznámení s funkcionalitami a obsluhou, dokumentace) bude realizována konfigurace na základě požadavků ZZS s přihlédnutím ke konfiguraci stávajících oprávnění v rámci centrálního FireWallu v ZOS. Nastavení bude umožňovat

bezproblémový chod IS OŘ ze ZZOS (stávajících technologií) včetně využití připojení k externím sítím v ZZOS (Internet apod.). Pro konfiguraci přístupu vzdálených uživatelů v rámci VPN bude využito stejné konfigurace jako v primární lokalitě ZOS v době implementace FW (centrální RADIUS serverů), tak aby byla umožněna jednotná konfigurace těchto přístupů bez ohledu na lokalitu přístupu.

Součástí implementace bude také:

- Výchozí nastavení pravidel pro alertování upozorňující na bezpečnostní události detekované na tomto bezpečnostním prvku.
- Bezpečnostní alerty v rámci IS ZOS budou definovány a konfigurovány na základě požadavků ZZS v rámci implementační analýzy (viz. dále).
- Napojení a předávání alertů a logů do systému analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí včetně specifikace korelace kritických bezpečnostních alertů z tohoto bezpečnostního prvku týkajících se IS ZOS.

Dále bude umožněna na dodávaném FireWallu možnost aktivace/deaktivace izolace systému IS ZOS od externích sítí nebo i od interních LAN/WAN segmentů ze systému IS OŘ (viz. dále). V rámci řešení úpravy IS ZOS bude proveden detailní záznam událostí izolace systému IS ZOS včetně jejich časové souslednosti, případně o uživatelích, kteří opatření realizovali, a to jak do logu IS OŘ, tak do systému analýzy bezpečnostních logů.

1.1.2 FireWall pro ochranu segmentu ZOS

Nabízené řešení je v souladu s požadavky na FireWall pro ochranu segmentu ZOS dle ZD.

Jako firewall pro ochranu segmentů ZOS v primární lokalitě s IPS nabízíme řešení Cisco Systems Cisco Firepower 2110 NGFW Appliance. Bude se jednat o dodávku jednoho HW FireWallu s požadovanými výkonnostními parametry s možností rozšíření o další redundantní box (není součástí dodávky) s možností konfigurace HA režimu.

Tento FireWal bude doplněn licencí „Cisco FPR2110 Threat Defense Threat and Malware“ pro řešení požadavků ZD na Aplikační firewall a IPS senzor. Pro tuto licenci bude navíc využita management console ve virtuálním dodávané infrastruktury „Cisco Firepower Management Center, (VMWare) for

2 devices“, která je součástí nabídky v kapitole „FireWall s IPS pro ZZOS“. Tato licence umožňuje konfiguraci vlastností IPS a AMP obou FireWallů z jedné management console.

Součástí dodávky je podpora na 5 let typu NBD, oprava v místě instalace zařízení včetně aktualizací všech signatur a SW komponent včetně jejich funkčnosti.

Součástí implementace bude také:

- Implementace v pasivním módu s možností implementace fyzického oddělení segmentu IS ZOS
- Výchozí nastavení pravidel pro alertování upozorňující na bezpečnostní události detekované na tomto bezpečnostním prvku.
- Bezpečnostní alerty v rámci IS ZOS budou definovány a konfigurovány na základě požadavků ZZS v rámci implementační analýzy (viz. dále).
- Napojení a předávání alertů a logů do systému analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí včetně specifikace korelace kritických bezpečnostních alertů z tohoto bezpečnostního prvku týkajících se IS ZOS.

1.1.3 L3 switche pro ZZOS

Nabízené řešení bude v souladu s požadavky na L3 switche pro ZZOS.

Nabízený centrální switch ZZOS bude složen ze dvou vzájemně propojených switchů Cisco Systems „Catalyst 9200L 24-port data, 4 x 10G“ + „Cisco Catalyst 9200L Stack Module“ který plně splňuje jak požadované výkonností tak funkční parametry a se zárukou 5let.

L3 Switch bude segmentovat LAN síť ZZOS a umožní šifrované propojení ZOS a ZZOS na L2 dle IEEE 802.1AE.

Součástí dodávky je dodávka, montáž (ZZOS) a implementace včetně propojení do stávající infrastruktury, která zajišťuje propojení lokalit ZOS a ZZOS a napojení a předávání alertů a logů do systému analýzy bezpečnostních logů (viz níže).

V rámci implementace systému analýzy bezpečnostních logů budou specifikovány korelace kritických bezpečnostních alertů z tohoto aktivního prvku týkajících se IS ZOS.

1.1.4 Aplikační firewall pro IS ZOS

Nabízené řešení bude v souladu s požadavky na aplikační FireWall pro IS ZOS dle ZD.

Nabízené řešení bude realizováno aplikačním FireWallem (WAF) „F5 - BIG-IP Virtual Edition Advanced Web Application Firewall 200 Mbps“, který bude zabezpečovat webové služeb (web services) v rámci externí komunikace IS ZOS.

Jedná se o služby IS ZOS dostupné z externích sítí – následující aplikace:

- Endpoint NIS IZS (SOS5) – publikováno do sítě NIS IZS
- SOSView – publikováno do sítě Internet

Funkcionalita webového aplikačního firewallu (WAF) bude poskytovat ochranu webových aplikací před kybernetickými útoky s využitím pozitivní i negativní bezpečnostní logiky v bezpečnostních politikách (detekci a ochranu před známými útoky a povolení explicitního legitimního provozu s propustností 200Mbps. Nabízené řešení umožňuje bezpečnostních vlastností, jako je ochrana před

útoky prolomením logovacích URL hrubou silou (Brute Force útoky) s možností eskalace a potlačení technologií CAPTCHA v případě podezření, že je aplikace pod útokem a technologie pro detekci a potlačení robotických (nelidských) uživatelů s možností výjimek (např. pro legitimní robotické klienty).

Nabízené řešení WAF také zajistí ochranu před únosy HTTP relací a podporuje SSL terminaci.

F5 - BIG-IP Virtual Edition Advanced Web Application Firewall bude nainstalován v rámci dodávané infrastruktury (viz. níže) jako virtuální zařízení případně na stávající infrastruktuře a redundance provozu bude zajištěna prostředky VMWare, kdy při výpadku jednoho virtualizačního serveru bude WAF spuštěn automaticky na redundantním serveru. Tím bude zajištěna vysoká dostupnost nabízené technologie.

Nabízené řešení splňuje veškeré výkonnostní a funkční požadavky dle ZD a záruka a aktualizace SW na 5 let

V rámci implementace bude realizovaná konfigurace na požadovaná aplikace (SOS5, SOSView) včetně jejich optimalizací a nastavení pravidel optimalizovaných pro chod těchto aplikací/rozhraní s ohledem na jejich funkčnost a dostupnost s detailní znalostí těchto aplikací/rozhraní (poddodavatel).

Vzhledem k využití technologie Virtual appliance na VMWare bude možné při plné aktivace ZZOS zprovozni WAF v záložní lokalitě ze záložní kopie (s možností využití stávající virtualizační platformy ZZOS).

Součástí implementace bude i napojení a předávání alertů a logů do systému analýzy bezpečnostních logů (viz níže).

Součástí předávání logů do systému analýzy bezpečnostních logů:

- kritické bezpečnostní události související s chráněnými aplikacemi ZOS a případných útocích na ně vedených
- varování před nestandartními stavy jako jsou anomální nárůsty požadavků, pokusy o přístup do nepublikovaných částí aplikací apod.
- logy o veškerých přístupech (úspěšné i neúspěšné) do managementu WAF a informace o změnách konfigurací WAF.

1.1.5 Systém analýzy bezpečnostních logů (SW)

Nabízíme požadovaný systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí zcela v souladu se ZD.

1.1.5.1 Systém analýzy bezpečnostních logů

Nabízíme jako základní produkt SW nástroje pro sběr dat (logů, alertů a dalších vstupů) a vyhodnocení kybernetických bezpečnostních událostí ze zabezpečovaných informačních systémů, infrastruktury, HW, systémového SW a technologií včetně IS ZOS a systému elektronické pošty systém IBM QRADAR Software + 1x Event Capacity 200EPS (celková kapacita 300EPS s možností rozšíření na 5000EPS)

Systém QRADAR bude sdružovat záznamy o událostech z jednotlivých aplikačních modulů IS ZOS, elektronické pošty a z okolí uvedených systémů (to je ze všech důležitých zařízení, systémů, sítě LAN/WAN a navazujících aplikací). Tyto záznamy bude ukládat a bude tyto záznamy dávat do souvislostí – korelovat a zajistí tak okamžitou detekci nebezpečného, případně nestandardního chování právě v IS ZOS, systému elektronické pošty nebo jejich infrastruktury

Nabízené řešení QRADAR plně splňuje požadavky uvedené v ZD P.62 a to jak výkonové, tak funkční.

Řešení Security Information and Event managment QRADAR je otevřená platforma pro sběr a vyhodnocování bezpečnostních událostí. Řešení umožňuje bezpečnostním analytikům efektivně reagovat na již proběhlé bezpečnostní incidenty. Řešení QRADAR poskytuje log management, event management, reporting a analýzy chování pro sítě a aplikací nebo uživatelů. Silnou stránkou řešení je mimo jiné komplexní chápání různých zdrojů a relevantních bezpečnostních informací a to zejména díky univerzální a modulární platformě Security Intelligence.

Základní vlastnosti:

- Shromažďování logů o událostech ze zařízení a aplikací na síti
- Komplexní zpracování, korelace a vyhodnocení shromážděných logů a flows v reálném čase
- Monitorování chování v síti, tvorba přehledných reportů a přístup ke všem informacím z řešení webové konzole
- Identifikace a kategorizace zranitelností
- Informace o nalezené zranitelnosti, popis hrozby při jejím potenciálním zneužití a případné návrhy řešení, jak mezeru odstranit.
- Možnost filtrováni nalezených zranitelností a jejich priorizace.
- Možnost nad filtry zranitelností vytvářet pravidla pro korelaci
- Podpora operačních systémů Windows/Linux, mnoha síťových zařízení (routery, firewally), databází, webových serverů, mail serverů, DNS a mnoha dalších

Řešení QRADAR je možno nasadit formou HW appliance, nebo software na ekvivaletní HW jiného výrobce či formou Virtualní appliance což je příklad nabízeného řešení. QRADAR bude nasazen formou tzv. All-in-One řešení.

Řešení disponuje podporou normalizace několika stovek nejrůznějších zařízení napříč dodavateli, zároveň je ale možné velmi snadno rozšířit o další zařízení. Díky této vlastnosti lze logy IS ZOS do QRADAR řešení integrovat, zpracovávány a korelovat – tím vytvářet reálná varování před potenciálními problémy v rámci IS ZOS včetně aplikací.

Systému analýzy bezpečnostních logů QRADAR bude provozován na dodávané infrastruktuře. Podpora systému analýzy bezpečnostních logů na 5 let včetně update SW a všech modulů.

Součástí dodávky je instalace a konfigurace řešení, včetně součinnosti při konfiguraci jednotlivých zařízení a aplikací a nastavení notifikací, a to včetně seznámení s funkcionalitami a obsluhou. Za 1 měsíc a za 3 měsíce bude provedeno vyhodnocení provozu a doladění korelačních pravidel na základě získaných dat během provozu implementovaného systému a dle požadavků Zadavatele.

Součástí je také implementace notifikací s využitím jak stávajících notifikačních nástrojů ZZS, tak s využitím pokročilého notifikačního nástroje, který je součástí dodávky tohoto projektu.

1.1.5.2 Nástroj pro logování z IT infrastruktury

Pro analytickou práci s logy aplikací, bezpečnostních a síťových systémů využívaných v rámci ZZS nebo dodávaných v rámci dodávky nabízíme rozšíření systému analýzy bezpečnostních logů o nástroj pro logování z IT infrastruktury – SPLUNK Enteprise s licencí logovaných dat do 5 GB za den.

Nástrojem budou logovány minimálně:

- Aktivní prvky (sítě)

- Informační systémy – IS ZOS/ZZOS a systém elektronické pošty
- Databáze (ORACLE, MS SQL)
- Operační systémy (MS Windows, Linux) – servery, pracoviště ZOS/ZZOS

Nástroj umožňuje samostatný přístup k různým službám pro různé osoby na základě oprávnění definovaného správcem a bude instalován na oddělený samostatný server (log server).

Podpora systému analýzy bezpečnostních logů – nástroj pro logování z IT infrastruktury na 5 let včetně update SW a všech modulů.

Dodávka a implementace nástroje na logování z IT infrastruktury – Splunk, IS ZOS a elektronické pošty, tzn. aktivní prvky, aplikace, operační systémy apod. ve kterém bude možnost plošně prohledávat sesbíraná data a mít k dispozici statistiku a analytické funkce – přičemž zdrojem dat může být i stávající syslog systém a bude pomocí produktu Spluk rozšířen o požadované funkce dle ZD.

Součástí implementace nástroje na logování z IT infrastruktury bude obsahovat nejenom zprovoznění a základní nastavení systému Splunk ale vytvoření i požadovaných reportů a dashboardů (náhledů) na jednotlivé komponenty IT infrastruktury a IS ZOS.

Minimálně následující náhledy:

- Aktivní prvky (LAN/WAN/FW) – přihlášení, změny konfigurací, chyby atd.
- FW/VPN – přístupy (oprávněné a neoprávněné) včetně geolokace (zobrazení na mapě a
- v tabulce)
- Operační systémy a databáze IS ZOS – přihlášení, chyby atd.
- Emailová komunikace – přístupy (oprávněné a neoprávněné) včetně geolokace, chyby systému atd.

1.1.5.3 Jednotný bezpečnostní portál

Jako součást dodávky bude realizován jednotný bezpečnostního portálu pro správce a management ZZS, který bude zahrnovat dodané technologie v rámci projektu a splňovat minimální požadavky na přehledový bezpečnostní portál:

Webové rozhraní:

- Autentizace/autorizace uživatelů proti Microsoft Active Directory
- Zobrazení posledních incidentů na základě analýzy bezpečnostních logů
- Zobrazení VPN připojení (úspěšné i neúspěšné)
- Zobrazení přihlášení do aplikací IS ZOS (úspěšné i neúspěšné)
- Zobrazení přehledu emailové komunikace ZZS (chyby, vytížení apod.)
- Možnost dalšího rozvoje dle požadavků ZZS – otevřený systém

Jednotný bezpečnostní portál bude provozován na infrastruktuře (HW a systémový SW) dodávaného v rámci projektu.

Podpora systému analýzy bezpečnostních logů – jednotný bezpečnostní portál na 5 let včetně update SW a všech modulů.

1.1.6 Infrastruktura (HW) a systémový SW pro běh dodávaného SW

V této kapitole jsou uvedeny požadavky na infrastrukturu (HW) a nezbytný systémový SW pro provoz dodávaných technologií.

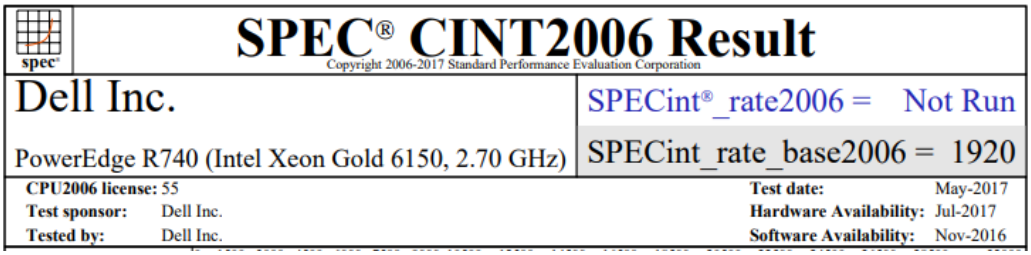
1.1.6.1 Server

Virtualizační server nabízíme server firmy DELL PowerEdge R740XD v konfiguraci plně splňující ZD.

Server je nabízen s procesorem Intel Xeon Gold 6150 2.7G, 18C/36T, který splňuje požadavky ZD a je dostačující na požadovaný provoz dodávaného řešení

SPECint_rate2006 base min. 1700 bodů:

http://www.spec.org/cpu2006/results/res2017q3/cpu2006-20170626-47215.pdf



SPEC® CINT2006 Result
Copyright 2006-2017 Standard Performance Evaluation Corporation

Dell Inc.

PowerEdge R740 (Intel Xeon Gold 6150, 2.70 GHz)

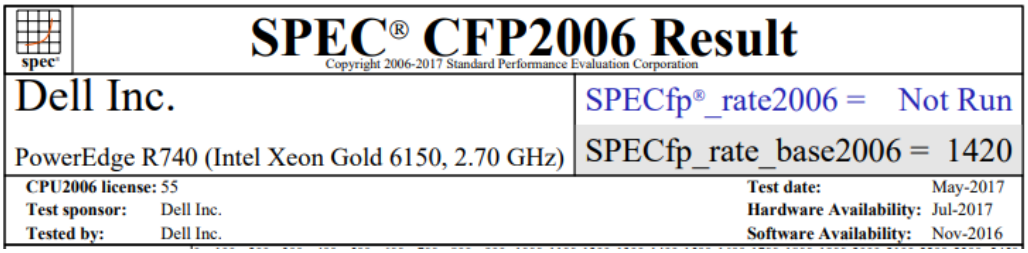
SPECint®_rate2006 = Not Run

SPECint_rate_base2006 = 1920

CPU2006 license: 55
Test sponsor: Dell Inc.
Tested by: Dell Inc.

Test date: May-2017
Hardware Availability: Jul-2017
Software Availability: Nov-2016

SPECfp_rate2006 base min. 1300:
http://www.spec.org/cpu2006/results/res2017q3/cpu2006-20170626-47213.pdf



SPEC® CFP2006 Result
Copyright 2006-2017 Standard Performance Evaluation Corporation

Dell Inc.

PowerEdge R740 (Intel Xeon Gold 6150, 2.70 GHz)

SPECfp®_rate2006 = Not Run

SPECfp_rate_base2006 = 1420

CPU2006 license: 55
Test sponsor: Dell Inc.
Tested by: Dell Inc.

Test date: May-2017
Hardware Availability: Jul-2017
Software Availability: Nov-2016

Konfigurace Serveru PowerEdge R740XD:

1 329-BDKH PowerEdge R740/R740XD Motherboard
1 338-BLMO Intel Xeon Gold 6150 2.7G, 18C/36T, 10.4GT/s 2UPI, 25M Cache, Turbo, HT (165W) DDR4-2666
1 379-BCQW iDRAC Service Module (ISM), Pre-Installed in OS
1 321-BDKE Chassis with up to 24x2.5" HDs, Mid-Bay Removed, 4x2.5" HDDs in FB for 1 and 2 CPU
1 325-BCHV PowerEdge 2U LCD Bezel
1 330-BBHF Riser Config 1, 4 x8 slots
1 370-AAIP Performance Optimized
1 370-ADNU 2666MT/s RDIMMs
6 370-ADNF 32GB RDIMM 2666MT/s Dual Rank
1 385-BBKT iDRAC9,Enterprise
1 385-BBLR VFlash Card Reader with 16GB Vflash SD card
10 400-ASGV 900GB 15K RPM SAS 12Gbps 512n 2.5in Hot-plug Hard Drive
4 401-ABCJ 900GB 15K RPM SAS 12Gbps 512n 2.5in Flex Bay Hard Drive

1 450-ADWS Dual, Hot-plug, Redundant Power Supply (1+1), 750W
1 540-BBUL Broadcom 57412 2 Port 10Gb SFP+ + 5720 2 Port 1Gb Base-T, rNDC
1 540-BBCX Broadcom 5720 DP 1Gb Network Interface Card
1 750-AABF Power Saving Dell Active Power Controller
1 770-BBBR ReadyRails Sliding Rails With Cable Management Arm
1 384-BBPZ 6 Performance Fans forR740/740XD
1 634-BILI Windows Server 2016 Datacenter,16CORE,Factory Installed, No Media,UnLTD VMs,NO CALs
1 634-BIOF Windows Server 2016 Datacenter,Media Kit
1 634-BILJ MS2016 DC Edition, Additional License,2CORE,NO MEDIA/KEY
1 865-BBMY ProSupport and Next Business Day Onsite Service, 60 Month(s)

Tabulka 1: Konfigurace serveru

1.1.6.2 Systémový SW

Pro potřeby dodávaného řešení nabízíme následující systémový SW:

- Jako součást HW virtualizačního serveru (viz požadavek na dodávku jednoho virtualizačního serveru výše) licenci Windows Datacenter pro provoz jak nových, tak stávajících Windows Serverů na dodávaném HW.
- Virtualizační platforma pro virtualizační servery bude dodána licence VMware vSphere 6 Standard for 1 CPU. Licence odpovídá nabízenému počtu serverů a CPU. Virtualizace je kompatibilní se stávající virtualizací a umožní v budoucnu spojení stávající a dodávané virtualizace do jedné management console bez nutnosti vypnou nebo reinstalovat provozované servery (pouze licenční změna).
- Pro zařazení virtualizačních serverů do systému zálohování bude poskytnuta součinnost při konfiguraci do stávajícího zálohovacího řešení.
- Databáze pro dodávané servery jsou buď již součástí licencí stávajících systémů, u kterých dochází k rozšíření jejich funkčnosti nebo případně ve free nebo integrovanou verzi.

Nabízené řešení je plně kompatibilní se stávajícími technologiemi.

1.1.6.3 Služby

Součástí dodávky infrastruktury je její dodávka, zapojení, instalace technologií, instalace a zprovoznění dodávaných technologií a prvků na dodaných technologiích. Součástí dodávky není strukturovaná kabeláž.

Součástí dodávky je integrace (napojení) dodávaných technologií do stávajícího monitorovacího nástroje (WhatsUp firmy Ipswitch), který není součástí dodávky tohoto projektu. Monitoring bude dle požadavku jednoznačně identifikovat chod jednotlivých dodávaných komponent.

1.1.7 Úpravy IS ZOS

1.1.7.1 Úprava systémů IS ZOS

Je požadována úprava systémů IS ZOS pro zaznamenávání činností v rámci operací těchto systémů do externích systémů pro následné zpracování a analýzy – napojení na nabízené rozšíření systému analýzy bezpečnostních logů.

Vlastní úpravy systémů IS ZOS budou provedeny dle požadavků ZD.

Jedná se o systémy:

- IS OŘ
- GIS
- EKP/MZD
- IS Pojišťovna
- Systém sledování vozidel (AVL)
- Svolávací systém
- Telefonní ústředna – API serveru
- Záznamový systém (REDAT)
- Integrace telefonie a radiofonie
- Aplikační SW na pracovištích ZOS/ZZOS
- Záložní IS ZOS (ZZOS)

Bude se jednat jak o úpravy uvedených systémů nebo využití logů IS OŘ pro práci s těmito systémy nebo systémové logy pro přístup k prostředků, a to dle ZD.

IS OŘ

U systému IS OŘ bude rozšířena úroveň logování dle požadavků ZD a připraveno samostatné view a uživatel pro export těchto dat pro následné zpracování a analýzy – v rámci „Systému analýzy bezpečnostních logů“.

Přitom se nebude jednat pouze o data v rámci IS OŘ ale i data interface na spolupracující technologie:

- Svolávací systém
- Záznamový systém (REDAT)
- Integrace telefonie a radiofonie

V rámci tohoto exportu dat může docházet i k anonymizaci položek dle druhu informace a účelu jejího pořízení – na základě konzultace a požadavků ZZS.

Pro kontrolu přístupu k systémových prostředků OS systémů:

Telefonní ústředna – API serveru

Integrace telefonie a radiofonie

Aplikační SW na pracovištích ZOS/ZZOS

Systém GIS

Systém sledování vozů

Budou na OS požadovaných systémů implementováni agenti pro sběr bezpečnostních logů včetně potřebné úpravy politik OS tak aby byly požadované bezpečnostní události logovány. Agenti pak budou exportovat tato data pro následné zpracování a analýzy – v rámci „Systému analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí“.

EKP/MZD a IS Pojišťovna

Systémy EKP/MZD a IS Pojišťovna budou vybaveny exportem dat dle ZD. Tyto data budou soužit pro následné zpracování a analýzy – v rámci „Systému analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí“.

AVL/GIS

Také systém sledování vozidel AVL umožňuje export logů z AVL dle požadavků ZD a možnost jejich zpracování v rámci „Systému analýzy bezpečnostních logů“. Servery GIS budou monitorovány na úrovni operačního systému a vyhodnocovány dle požadavků ZD.

Záložní IS ZOS (ZZOS)

ZZOS využívá v současné době repliku některých systémů IS ZOS (IS OŘ). V rámci implementace bude realizován sběr požadovaných dat nejenom z primární lokality ale i z záložní lokality – ZZOS.

1.1.7.2 Napojení IS OŘ na FireWall ZZOS

V rámci IS OŘ bude možné přijímat i alerty upozorňující na bezpečnostní události a to nejenom z uvedených bezpečnostních prvků ale všech komponent zabezpečení. Bude se jednat o alerty bezpečnostních událostí relevantních k provozu centrálního dispečinku a celého IS ZOS s kritickou důležitostí. Bezpečnostní alerty v rámci IS ZOS budou definovány a konfigurovány na základě požadavků ZZS v systémech analýzy a sběru bezpečnostních logů, který tyto alerty bude předávat do IS OŘ – dispečerského pracoviště. Tak bude aktivně informován provoz centrálního dispečinku ZOS o vážných bezpečnostních událostech.

Oprávněné osoby centrálního dispečinku budou mít možnost pomocí rozhraní v IS ZOS (IS OŘ) na základě vzniklých bezpečnostních událostí a jejich průběhu rozhodnout o možnosti aktivace (a následné deaktivace) izolace systému IS ZOS od externích sítí nebo i od interních LAN/WAN segmentů. Vlastní izolace bude realizována na uvedených bezpečnostních prvcích (ZOS/ZZOS). Oprávněný uživatel bude před vlastní aktivací daného typu izolace informován o rozsahu izolace a z toho plynoucích omezení centrálního dispečinku a IS ZOS. O těchto událostech bude proveden detailní záznam událostí včetně jejich časové souslednosti a uživatelích, kteří taková opatření realizovali a neprodleně automaticky informováni definovaní pracovníci ZZS v rámci stávajícího svolávacího systému ZZS.

1.1.7.3 Autentizace uživatelů operačního řízení prostřednictvím AD

V rámci sjednocení ověřování identity uživatelů v rámci IT a operačního řízení je požadováno využití stávající domény v rámci Microsoft Active Directory.

Pro tyto účely bude realizováno rozšíření stávajícího IS ZOS o možnost autentizace a autorizace v rámci struktury MS Active Directory, a to v následujících systémech dle ZD:

- IS OŘ
- EKP/MZD

V rámci implementace bude využita pro autentizaci a autorizaci dle zadání stávající doména ZZS MS Active Directory. ZZS v rámci součinnosti poskytne AD a odpovídá i za její licencování.

1.1.7.4 Integrace s personálním systémem

Stávající personální systém VEMA využívá modul integrace s centrálním MS Active Directory ZZS.

Systémy IS OŘ a EKP/MZD budou tuto integraci s personálním systémem využívat, a to jak při zakládaní uživatele a případně jejich základní role v rámci personálního systému (která se promítne do AD) využití zneplatnění účtů uživatelů, u kterých bude ukončen pracovní poměr (zneplatnění/vymazání účtu v AD). Tím bude zajištěna maximální aktuálnost uživatelských účtů zaměstnanců ZZS – tím i vyšší míra zabezpečení přístupu k datům.

1.1.7.5 Monitoring a reporting a přístupů

Pro správu a reporting oprávnění bude dodán i samostatný portál pro správu uživatelů IS OŘ a přiřazování jejich rolí. Tento portál bude sloužit pro vedoucí pracovníky OŘ, kteří budou tato oprávnění spravovat a kontrolovat a monitorovat. Tento portál bude realizován samostatným modulem systému SOS – portál, který požadované funkce nabízí a bude plně integrován jak systémem IS OŘ (SOS) tak AD ZZS.

Součástí dodávky bude nástroj pro reportingu všech změn provedených jednotlivými uživateli/administrátory v rámci Microsoft Active directory (AD) ZZS (počet aktivních uživatelů 800), tak aby bylo možné kontrolovat změny oprávnění, které byly v rámci AD provedeny.

Pro splnění požadavků uvedených v ZD bude využito samostatného produktu QUEST který zcela splňuje požadované vlastnosti. Nástroj bude instalován v prostředí AD ZZS.

1.1.7.6 Infrastruktura (HW) a systémový SW pro úpravy IS ZOS

Stávající infrastruktura (HW) a systémový SW pro běh IS ZOS po realizaci úprav zůstane beze změny, tj. nedojde ke změně konfigurace, parametrů, licencí systémového SW využívaných pro běh IS ZOS.

1.1.8 Konfigurace systému elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů

Pro napojení na systém analýzy bezpečnostních bude systém stávající elektronické pošty nakonfigurován tak aby předával následující data ze systému elektronické pošty:

- Úspěšná a neúspěšná připojení k systému dostupnými protokoly
- Využívání systému elektronické pošty jednotlivými uživateli
- Dostupné bezpečnostní logy používaného systému
- Dostupné chybové a provozní logy používaného systému Předávání veškerých logů systému do nástroje/rozhraní pro logování.

Toto nastavení realizovat pro všechny komponenty systému elektronické pošty a předávání logů systému online prostřednictvím syslog služby.

V rámci stávajícího systému Kerio Connect ve verzi 9.x je možné konfigurací odesílat požadované logy systému do syslog serveru a zde je následně zpracovávat a poskytovat do systému analýzy bezpečnostních logů. Mimo to budou data zpracovávána i pro požadovaný systém vytváření dynamických ACL.

Kromě událostí ze systémů elektronické pošty budou získávány i bezpečnostní události na prvcích FireWall, týkajících se systému elektronické pošty.

Minimálně:

- Odepření přístupu z dané IP adresy na systém (reputace dynamický ACL apod.)
- IPS a AntiMalware události
- Identifikace chyb v protokolu

Zpracovávané události týkající se elektronické pošty umožní i realizaci požadovaného systému dynamických ACL na základě parametrického vyhodnocení bezpečnostních logů systému. Dynamický ACL bude vytvářen prostřednictví analýzy logů na základě neoprávněného přístupu k systému.

Pro vytváření dynamických ACL bude možné systémově nastavovat následující parametry:

- Počet špatných přihlášení k danému protokolu
- Minimální čas od posledního výskytu špatného přihlášení

Publikace dynamického ACL pro systém elektronické pošty bude pro účely aktualizace pravidel FireWallu realizována web serverem jako standardní textový soubor s výčtem (list) IP adres (jedna IP na jednom řádku).

Nástroj/rozhraní pro logování bude zpracovávat i uvedený dynamický ACL pro systém elektronické pošty a zobrazovat časový průběh počtu IP adres obsažených v listu a upozorňovat na enormní nárůst.

Konfigurace FireWall ZOS bude realizovaná v součinnosti s ZZS a to jak pro nastavení logování tak pro implementaci dynamického ACL (aktualizace listu IP adres).

Stávající infrastruktura (HW) a systémový SW pro běh elektronické pošty po realizaci úprav zůstane beze změny, tj. nedojde ke změně konfigurace, parametrů, licencí systémového SW využívaných pro běh elektronické pošty.

1.1.9 Dvoufaktorová autentizace administrátorských VPN přístupů

Pro řešení požadavků na dvoufaktorovou autentizaci nabízíme řešení firmy ESET: „ESET Secure Authentication“ licencováno pro 20 uživatelů s zárukou na funkčnost, podpora a aktualizace po dobu min. 5 let, které plně splňuje požadavky ZD.

ESET Secure Authenticationse skládá ze serverové a klientské části, jež má podobu mobilní aplikace a není tak třeba další zařízení nebo token. Nabízené řešení je plně integrovatelné s prostředím ZZS:

- FireWall Cisco ASA
- Firemní VPN a OWA
- Remote Desktop protokol

- Přihlášení do operačního systému
- VMware Horizon View
- Služby založené na RADIUS

Push autentifikace – autentifikaci je možné provést s pomocí jednoduchého potvrzení na mobilním telefonu bez nutnosti přepisovat jednorázové heslo (podporuje iOS, Android i Windows Mobile).

Produkt je kompatibilní se všemi telefony, které umožňují přijímat SMS a podporuje široké spektrum mobilních operačních systémů. Přístup do aplikace je chráněn kódem PIN. ESET Secure Authentication podporuje doručení jednorázového hesla nejen přes mobilní aplikaci, push notifikaci, hardwarové tokeny a SMS, ale i vlastní cestou (např. e-mailem).

ESET Secure Authentication

Jde o autentifikační metodu, která k heslu, co zná jen uživatel, přidává něco, co uživatel fyzicky vlastní (např. kreditní kartu, USB token nebo klíč), případně něco, čím je charakteristický. Ideální situace nastává v případě, kdy je druhý faktor vyřešený softwarově, takže jako token slouží mobilní zařízení s instalovanou aplikací, která generuje jednorázová hesla (OTP).

Jednorázová hesla jsou generována náhodně, takže je nelze předvídat ani znovu použít. Výhody tohoto řešení jsou zřejmé: uživatel se nemusí starat o další zařízení, ale využívá své mobilní zařízení, které má po většinu dne stále v dosahu.

ESET Secure Authentication podporuje doručení jednorázového hesla nejen přes mobilní aplikaci, push notifikaci, hadrwarové tokeny a SMS, ale i vlastní cestou (např. e-mailem).

Produkt lze spravovat prostřednictvím webové konzole nebo Microsoft Management Console (MMC). Funguje s Active Directory i jako samostatný produkt v prostředí bez domény Windows.

ESET Secure Authentication nativně podporuje služby Virtual Private Networks (VPN), Remote Desktop Protocol (RDP), Outlook Web Access (OWA), VMware Horizon View a RADIUS.

Podporované operační systémy Windows server 2008 - 2019

ESET Secure Authentication podporuje webové a cloudové služby typu Google Apps a Microsoft ADFS 3.0 (včetně Office 365).

I když hardwarové tokeny nejsou potřeba, produkt podporuje všechny standardní typy (HOTP, OATH).

Podporované VPN, Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet FortiGate, Juniper, Palo Alto, SonicWall.

1.1.10 Nástroje pro bezpečnostní audit a penetrační testy

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

Pro realizaci požadavku na dodávku nástroje pro periodické testování bezpečnostních zranitelností interních systémů i systémů, které komunikují s externími subjekty i jako součást penetračních testů (nástroj budou využity v rámci Bezpečnostní audit a penetrační testy) nabízíme produkt firmy Tenable Nessus Professional, který splňuje zcela požadavky ZD.

Společnost Tenable je renomovaným dodavatelem systémů pro detekci, hodnocení a správu bezpečnostních zranitelností.

Nessus Professional (dále jen „Nessus“) je řešení pro vyhledávání a analýzu zranitelností, které poskytuje kompletní přehled o zabezpečení IT infrastruktury. Skenování neslouží pouze k identifikaci zranitelností, ale také k objevení malwaru nebo špatně nakonfigurovaných systémů.

Nessus nabízí více než desítku šablon pro jednoduché vytváření nových skenů. Mezi ty nejpoužívanější patří:

- Host Discovey,
- Basic Network Scan,
- Credentialed Patch Audit,
- Web Application Tests,
- Policy Compliance Auditing.

Kromě základních šablon pro skenovaní umožňuje Nessus vytvořit sken podle požadavků uživatele pomocí pokročilého skenování. To nabízí tyto možnosti konfigurace:

- Host Discovery – metody vyhledávání aktivních strojů;
- Port Scanning – možnost nastavit skenované porty;
- Service Discovery – možnost nastavit jakým způsobem hledá běžící služby;
- Assessment Options – možnost nastavit jak získávat určité informace během skenování;
- Brute Force Options – nastavení testování Brute Force Attack;
- SCADA Options – možnost nastavit skenování SCADA zařízení;
- Web Applications Options – možnost nastavit skenování webových aplikací;
- Windows Scan Options – možnost nastavit Windows SMB;
- Malware Feature – možnost nastavit skenování za účelem detekce malwaru;
- Scan Report Options – možnost nastavit jaké informace mají být obsaženy v reportu;
- Authentication Options – nastavení možnosti autentizace při skenování.

1.1.11 Bezpečnostní audit a penetrační testy

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

Nabízené řešení je v souladu s požadavky dle zadávací dokumentace c.12 – bezpečnostní audit a penetrační testy.

1.1.11.1 Bezpečnostní audit / bezpečnostní analýza

Bezpečnostní analýza bude provedena na základě požadavků zákona 181/2014 Sb., ve znění pozdější novelizace a s vyhláškou 82/2018 Sb.

Průběh analýzy:

1. Zahajuje se zaslání dokumentace ze strany Zadavate.
   Tzn. veškeré:
   - bezpečnostní a provozní politiky
   - definice aktiv
   - analýza rizik
   - zápisi z řídícího výboru KB

- plány kontinuity
- organizační struktura
- topologie sítě
- atd.

2. Po nastudování dokumentace následuje úvodní workshop.
   Zde je předmětem:
   - Seznámení se s obecným fungováním organizace
   - Seznámení se s cíly a podstatou činnosti organizace.
   - Předání informací ohledně členění IT, topologií a zodpovědností.
   - Vydefinování majitelů a provozovatelů jednotlivých aktiv
   - Vydefinování specializovaných workshopů podle technologií, aplikací, lokalit apod.
   - Zadavatel přiřadí zodpovědné osoby za jednotlivá aktiva z pohledu majitelů a provozovatelů
3. Po úvodním workshopu následují dílčí technické workshopy podle specializací.
   a) Pohovory s majiteli aktiv (většinou non-IT osoby). Upozorňujeme, že budem potřebovat hovořit i s řadou osob, které se ZKB na první pohled nesouvisí. Tj. HR, finanční oddělení, top management … Seznam detailně určujeme podle dodané organizační struktury.
   b) Pohovory s provozovateli aktiv (obvykle s IT oddělením). Do této části patří i externí dodavatelé.
4. Na základě získaných informací dojde k sepsání auditní zprávu a hodnotící zprávy dle požadavků v zadávací dokumentaci.

5. Získávání informací do auditní a hodnotící zprávy
   - je skrze diskuzi s majiteli a provozovateli aktiv
   - v případě potřeby se některé informace kontrolně ověřují
   - Používá se vzorková metoda. Tzn. pokud je nutné prověřit konfigurace aplikací, zařízení, koncových systémů …,kdy jich je větší množství (např. WAN směrovače), tak se neprochází všech zařízení, ale jenom určitého vzorku (např. 1 zařízení od každého modelu).
6. V případě, že v organizační části auditu jsou nedostatečné vstupy u definice aktiv, analýze rizik a v plánu zvládání rizik atd. tak:
   - provedeme orientační identifikaci potřebných vstupních informací
   - v případě potřeby aplikujeme kvalifikovaný odhad
   - upozorňujeme, že úroveň těchto kroků nejsou náhradou analýzi rizik, metodikou pro určování aktiv, mapování zavislostí primárních a podpůrných aktiv, plánem zvládání rizik

<u>Součinnost:</u>

1. Zajištění součinnosti majitelů majitelů a provozovatelů aktiv a to včetně externích subjektů.
2. Aktivní účast na workshopech majitelů majitelů a provozovatelů aktiv a to včetně externích subjektů dle dohodnutého harmonogramu.

3. Poskytnutí vstupů pro technické hodnocení.
4. Dodání dokumentace
    a. kompletní ISMS dokumentaci
    b. kompletní dokumentaci k ZKB
    c. technickou a provozní dokumentaci k síťovým prvkům, serverům, aplikacím apod.
5. Zajištění všech požadovaných vstupních informací v úvodních týdnech od zahájení GAP analýzi. Pokud se to nepodaří, tak to znamená časový posun v termínu dokončení díla.

Auditní zpráva

- U každého opatření se vyhotový popis aktuálního stavu.
- Bude provedeno hodnocení z pohledu požadavků aktuální prováděcí vyhlášky KB
- V případě, že to bude potřebné, tak dojde k hodnocení i z pohledu dobré praxe.
- Každé opatření bude popsáno minimálně v požadovaném rozsahu ½ A4
- Celková délka auditní zprávy je orientačně přes 50 stran A4. Finální rozsah je dán množstvím zkoumaných primárních a podpůrných aktiv. Případně složitostí prostředí.
- Obsahem zprávy jsou veškeré paragrafy obsažené v prováděcí vyhlášce ZKB
- Organizace se zkoumá z pohledu:
    - organizační opatření
    - technických opatření
    - fyzické bezpečnosti

Hodnocení stavu

- Dojde k vytvoření přehledového excelu s výpočetní logikou, který bude hodnotit výsledek GAP analýzy pro
    - Technické role
    - Manažerské role (zaměřeno na přehledové informace pro manažersky)

Obecný návrh nápravných opatření

- Nebudou se hodnotit veškeré možné technické varianty nápravných opatření, ale dojde k určení orientační výše nákladů pro zajištění souladu se ZKB a dojde k určení druhu technologie.
- V případě, že se jedná o úpravu nastavení stávajících zařízení nebo softwarů, tak předpokládáme, že si zajistí Zadavatele cenu těchto úprav od nasmlouvaných dodavatelů. Poskytujeme pouze součinnost pro definici rozsahu.
- V případě, že se bude jednat o úpravy, bez dodání zařízení a licencí, dodávaného řešení bude toto řešeno v rámci servisních služeb na základě dohody se Zadavatele.

Hodnocení rozsahu bude obsahovat položky dle požadavku P.106 a případně jiné mandatorní části dle ZKB.

Součástí není:

- Jednání s NBÚ

- Úprava dokumentace
- Průzkum trhu
- Analýza aktiv dalších částí, které nemají přímou souvislost se ZKB
- Vytváření metodik nebo směrnic pro ZKB

1.1.11.2 Penetrační testování a testy zranitelností

Testy zranitelností

Budou provedeny provedeny z vnější sítě. Tyto skeny se zaměří na požadované aplikace dle zadávací dokumentace (Systémy IS ZOS a elektronickou poštu) a případné perimetrové prvky.

Cílem skenu bude:

- rozpoznání aktivních zařízení
- detekování otevřených portů
- rozpoznání aktivních služeb
- sken webových aplikací
- zjistění známých zranitelností pro publikované služby a sytémy

Penetrační testy

Budou zaměřeny na aplikace Endpoint NIS IZS a SOSView. Cílem testů bude odhalení nedostatků, oproti požadavkům §25 vyhlášky 82/2018 Sb. Požadavky §25 budou vnímány v kontextu bezpečnostní strategie čí dalších dokumentů Zadavatele.

Vlastnímu penetračnímu testu bude předcházet detekce zranitelností pomocí speciálního nástroje.

Metodické rámce

Penetrační testy budou provedeny:

- dle platné verze OWASP Testing Guide (OTG)
- v souladu s metodikou OSSTMM

Budeme reflektovat závěry dle OWASP Top 10 a tyto informace použijeme pro směřování testů

Penetrační testy se zaměří výhradně na aplikace Endpoint NIS IZS a SOSView a nebudou prováděny na jiných podpůrných aktivech. Penetračním testováním nebudou ověřovány další SW komponenty, které nemají přímou souvislost s testovanými aplikacemi.

Auditní zpráva

Součástí závěrečné zprávy bude kompletní seznam provedených testů. Ka každému testu bude informace ohledně odhalených zranitelností a to včetně navrhu realizace pro zajištění nápravy.

V případě požadavku jsme schopni poskytnout součinnost při odstraňování zranitelnost A to buď formou vlastní realizace, nebo konzultací.

1.1.12 Bezpečnostní požadavky

Nabízené řešení bude splňovat uvedené bezpečnostní požadavky ZD.

Systém bude chránit osobní údaje pacientů a bude v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob (GDPR) v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Vybavení plní podmínky zákona č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Přičemž dodávané systémy nepořizují primárně osobní data, ale zpracovávají informace o přístupech uživatelů jak k systémům, tak datům. Poptávané a nabízené systémy tak neobsahují osobní údaje o pacientech.

Nabízené systémy splňují požadavky:

- Autorizace: Poskytnutí přístupu autentizovaného uživatele k aktivu systému (data, aplikace), odpovídající pracovnímu zařazení uživatele a přidělené roli (rolím) v systému.
- Systém umožní řídit přístupová oprávnění jednotlivých subjektů jen k údajům, ke kterým mají a mohou mít přístup.
- Zabránění vstupu neautorizovaného subjektu do systému – zamezení možnosti přístupu neoprávněného subjektu.
- Zajištění šifrované komunikace mezi všemi součástmi systému a pracovišti uživatelů, případně zajištění komunikace v odděleném síťovém prostředí.
- Evidence přístupů všech uživatelů do systémů a technologií (logování) včetně časových údajů.
- Veškeré přístupy k datům a aktivita uživatelů v rámci dodávaných systémů a technologií budou logovány tak, aby byly zřejmé přístupy k jednotlivým údajům a zpětná kontrola těchto údajů.
- Veškeré logy budou dostupné pro externí Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí.

1.1.13 Implementační a provozní požadavky

Nabízené řešení plně splňuje implementační a provozní požadavky dle ZD. Řešení je nabízeno na produktech renomovaných firem s předpokladem provozu 24x7x365 (non-stop) a plně koresponduje s požadavky na jeho dostupnost, uvedenými v servisní smlouvě.

Předmětem zakázky jsou i veškeré služby související s dodávkou – doprava, instalace, implementace do stávající infrastruktury, konfigurace a zprovoznění komunikace, nastavení datových toků, seznámení s obsluhou a správou systému, testování, bezplatné preventivní prohlídky v rámci poskytování servisních služeb. Veškeré seznámení s obsluhou bude probíhat v prostorách objednatele a v českém jazyce. Instalace bude provedena do prostředí objednatele a v rámci implementace bude zajištěn plnohodnotný provoz dodávaného řešení současně s provozem stávajících systémů a technologií. To vše s minimálním omezením provozu. Realizace předmětu zakázky se přizpůsobí podmínkám objednatele.

Veškeré technologie budou mít nastavenu synchronizaci času všech zařízení s time serverem (doporučujeme NIS) nebo zprostředkovaně přes centrální systém.

Součástí nabídkové ceny jsou i veškeré práce či činnosti, které v této zadávací dokumentaci nejsou explicitně uvedeny, ale které musí dodavatel s ohledem na jím nabízený předmět veřejné zakázky a jeho řádnou a úplnou realizaci provést k dosažení objednatelem požadovaného cílového stavu.

2 DETAILNÍ POPIS FUNKČNÍCH VLASTNOSTÍ

V této kapitole je uveden detailní popis funkčních vlastností nabízeného plnění ve struktuře a rozsahu uvedených v kapitole 3 Přílohy č.1 - Technická specifikace dodávky.

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v této kapitole.

2.1 POŽADAVKY NA DODÁVKY

V této kapitole jsou uvedeny požadavky na dodávky.

2.1.1 Obecné a společné požadavky

V této kapitole jsou uvedeny obecné požadavky na požadované řešení:

#	Požadavek
P.1	Dodávané technologie musí svojí architekturou splňovat obecné zásady informační bezpečnosti v míře, odpovídající charakteru užití a kategorii zpracovávaných dat (GDPR).
P.2	Veškeré nabízené SW i HW prvky musí být plně kompatibilní se stávajícími systémy a technologiemi **ZZS JMK**.
P.3	Součástí implementace musí být i veškeré potřebné licence a služby nezbytné pro dodávku a provoz dodávaných technologií minimálně po dobu účinnosti servisní smlouvy.
P.4	Zaručená perspektiva rozvoje a podpory je minimálně po dobu dalších 6 let od uvedení do provozu.
Legislativa a další normy	
P.5	Soulad s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob (GDPR – General data protection regulation) v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
P.6	Soulad se Zákonem č. 181/2014 Sb., o kybernetické bezpečnosti v aktuálním znění a vyhláškou Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti v aktuálním znění.
P.7	Soulad s prováděcím nařízením Komise (EU) 2018/151 ze dne 30. ledna 2018, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný (dále jen "PNK").
P.8	Soulad se Zákonem č. 239/2000 Sb. o integrovaném záchranném systému a o změně některých zákonů v aktuálním znění.
P.9	Soulad se Zákonem č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů v aktuálním znění.
Ostatní obecné požadavky	
P.10	Zajištění jednotného času na všech technologiích a zařízeních (synchronizace s time serverem) .

Tabulka 2: Obecné požadavky

Pro konkrétní oblasti jsou uvedeny specifické požadavky samostatně v dílčích podkapitolách.

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce.

2.1.2 FireWall s IPS pro ZZOS

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.11	Dodávka firewallu s IPS pro řízení bezpečného přístupu mezi vnějšími sítěmi (Internet, NIS IZS, PČR atd.) a vnitřní sítí ZZOS a ZOS.

P.12	Dodávka FireWallu pro záložní ZOS:
	• FireWall bude oddělovat externí sítě připojené v rámci záložního ZOS (internet apod.)
	• Stavový aplikační firewall jako samostatné HW zařízení, který musí nabízet
	  ○ Dynamický a statický NAT/PAT (překlad IP adres)
	  ○ Podporu dynamických směrovacích protokolů RIP, OSPF, BGP a Policy based Routing
	  ○ Plnou podporou protokolu IPv6
	  ○ Podpora redundance pro případ výpadku ve formě Active/Active failover, Active/Standby failover (redundantní prvek není součástí dodávky)
	  ○ Podpora filtrace IPv4, IPv6 a filtrace podle identity uživatele nebo jeho skupiny definované v AD
	• Aplikační firewall
	  ○ Pokročilá hloubková analýza dat na aplikačních vrstvách ISO modelu
	  ○ Podpora pasivního monitorování (TAP režim)
	  ○ Rozeznávání a kategorizace aplikací, geografických lokalit, uživatelů
	  ○ Možnost rozšíření o identifikace a zamezení přístupu na nedůvěryhodné či škodlivé webové stránky – filtrace podle reputace serverů
	  ○ Security Inteligence database – známé adresy anonymních proxy, otevřených mail relay, uzly botnet sítí
	  ○ Možnost integrovat vlastní reputační databáze
	• IPS senzor, který musí nabízet
	  ○ Možnost definovat typ provozu předávaný k inspekci do IPS
	  ○ Možnost obejití IPS funkcí při zahlcení nebo nedostupnosti
	  ○ IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií
	  ○ Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s reputací
	  ○ IPS musí umět detekovat a blokovat útoky průzkumných aktivit
	  ○ IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS
	  ○ IPS musí umět detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host“ jako je spyware, phishing nebo Botnet C&C
	  ○ aktuálních databázích AV dodavatelů
	  ○ Ochrana před malware typu „zero day attack“ které nelze detekovat tradičními antiviry
	  ○ Retrospektivní ochrana prostředí – pokud SW kód je později detekován jako malware, je na to IPS schopna reagovat
	  ○ Podpora databází reputací adres v internetu (Security Intelligence)
	• VPN koncentrátor
	  ○ Zakončení „full-tunnel“ IPSec nebo SSL VPN pro alespoň 300 současné připojených uživatelů – licence pro 25 uživatelů
	  ○ Možnost rozšíření (licence apod.) „odlehčené“ SSL VPN pro uživatele formou zabezpečeného přístupu na webový portál bez nutnosti tlustého klienta
	  ○ Zakončení alespoň 300 současně připojených site-to-site IPsec tunelů

#	Požadavek
	○ Implementace IPsec musí podporovat protokoly IKEv1 i IKEv2 a šifrovací standardy 3DES/AES a algoritmy nové generace popsané ve standardu NSA Suite-B • Výkonnostní parametry a provedení ○ Minimální propustnost NGFW (hloubková inspekce) 850 Mbps ○ Minimální propustnost NGFW (hloubková inspekce + IPS modulem) minimálně 450 Mbps. ○ Minimální propustnost pro IPsec VPN komunikaci (šifrování 3DES/AES) 250 Mbps ○ Formát zařízení Appliance v provedení do racku max 2RU ○ Samostatný port pro management ○ Minimální 8 portů pro data 10/100/1000 BaseT Ethernet ○ Podporovaný počet VLAN min. 100 Součástí dodávky je implementace (montáž, instalace, konfigurace, zaškolení a seznámení s funkcionalitami a obsluhou, dokumentace) Podpora na 5 let typu NBD, oprava v místě instalace zařízení včetně aktualizací v šech signatur a SW komponent včetně jejich funkčnosti.
P.13	Umístění firewallu s IPS do DC v rámci záložního zdravotnického operačního střediska.
P.14	Nastavení pravidel pro kontrolu přístupu do segmentů IS ZOS a ZZOS z externích sítí a kontrolovat ho před případnými externími i interními útoky. Konfigurace FireWallu bude realizována na základě požadavků ZZS s přihlédnutím ke konfiguraci stávajících oprávnění v rámci centrálního FireWallu v ZOS. Nastavení bude umožňovat bezproblémový chod IS OŘ ze ZZOS (stávajících technologií) včetně využití připojení k externím sítím v ZZOS (Internet apod.). Pro konfiguraci přístupu vzdálených uživatelů v rámci VPN bude využito stejné konfigurace jako v primární lokalitě ZOS v době implementace FW (centrální RADIUS serverů), tak aby byla umožněna jednotná konfigurace těchto přístupů bez ohledu na lokalitu přístupu. *Konfigurace stávajících firewallů a nastavení sítě budou poskytnuty v rámci implementační analýzy.*
P.15	Výchozí nastavení pravidel pro alertování upozorňující na bezpečnostní události detekované na tomto bezpečnostním prvku. *Bezpečnostní alerty v rámci IS ZOS budou definovány a konfigurovány na základě požadavků ZZS v rámci implementační analýzy.*
P.16	Napojení a předávání alertů a logů do Systému analýzy bezpečnostních logů (viz kap. 2.1.6). Včetně specifikace korelace kritických bezpečnostních alertů z tohoto bezpečnostního prvku týkajících se IS ZOS.
P.17	Dodávka FireWallu jako kompaktního zařízení, tj. HW včetně vnitřního SW zajišťujícího všechny požadované funkcionality. Pro případný podpůrný SW sloužící pro instalaci, konfiguraci a aktualizace FW ZZS umožní využití stávající virtualizační infrastruktury ZZS za předpokladu, že nepřesáhne požadavek na jeden server (4 vCPU, 8 GB RAM a 500 MB vHD, OS MS Windows Server 2016 Standard nebo Linux). V případě vyšších požadavků na server dodavatel dodá i nezbytný HW a systémový SW včetně licencí pro běh podpůrného SW (HW ve verzi rack mount).
P.18	Možnost aktivace/deaktivace izolace systému IS ZOS od externích sítí nebo i od interních LAN/WAN segmentů ze systému IS OŘ (viz kap. 2.1.8 – Úpravy IS ZOS). Vlastní izolace bude provedena na firewallech v rámci ZOS (součinnost poskytne ZZS) a ZZOS (součástí dodávky).

#	Požadavek
P.19	Bude proveden detailní záznam událostí izolace systému IS ZOS včetně jejich časové souslednosti, případně o uživatelích, kteří opatření realizovali, a to jak do logu IS OŘ, tak do Systému analýzy bezpečnostních logů (viz kap. 2.1.6).

Tabulka 3: FireWall s IPS pro ZZOS

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce

2.1.3 FireWall pro ochranu segmentu ZOS

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.20	Dodávka Firewallu pro ochranu segmentů ZOS v primární lokalitě.
P.21	FireWall pro ochranu segmentu ZOS musí plnit min. parametry stejné jako FireWall s IPS pro ZZOS s výjimkou že nejsou požadovány vlastnosti VPN koncentrátoru. Dále jsou požadovány následující výkonnostní parametry: • Minimální propustnost NGFW (hloubková inspekce) 2 000 Mbps • Minimální propustnost NGFW (hloubková inspekce + IPS modulem) 800 Mbps.
P.22	Umístění firewallu do DC v rámci primárního zdravotnického operačního střediska.
P.23	Implementace v pasivním módu s možností implementace fyzického oddělení segmentu IS ZOS
P.24	Výchozí nastavení pravidel pro alertování upozorňující na bezpečnostní události detekované na tomto bezpečnostním prvku. *Bezpečnostní alerty v rámci IS ZOS budou definovány a konfigurovány na základě požadavků ZZS v rámci implementační analýzy.*
P.25	Napojení a předávání alertů a logů do Systému analýzy bezpečnostních logů (viz kap. 2.1.6). Včetně specifikace korelace kritických bezpečnostních alertů z tohoto bezpečnostního prvku týkajících se IS ZOS.
P.26	Dodávka FireWallu jako kompaktního zařízení, tj. HW včetně vnitřního SW zajišťujícího všechny požadované funkcionality. Pro případný podpůrný SW sloužící pro instalaci, konfiguraci a aktualizace FW ZZS umožní využití stávající virtualizačí infrastruktury ZZS za předpokladu, že nepřesáhne požadavek na jeden server (4 vCPU, 8 GB RAM a 500 MB vHD, OS MS Windows Server 2016 Standard nebo Linux). V případě vyšších požadavků na server dodavatel dodá i nezbytný HW a systémový SW včetně licencí pro běh podpůrného SW (HW ve verzi rack mount).

Tabulka 4: FireWall pro ochranu segmentu ZOS

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce

2.1.4 L3 switche pro ZZOS

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.27	Dodávka centrálního L3 switche ZZOS složeného ze dvou vzájemně propojených switchů pro segmentaci LAN sítí ZZOS.
P.28	L3 switche musí plnit následující min. parametry (každý jeden switch): 1. provedení rack mount 2. ethernetový spravovatelný přepínač vrstvy 3

#	Požadavek
	3. min. 24x 10/100/1000Mbs portů a min. 4x 10Gb SFP/SFP+ na jeden switch 4. propojení switchů do jednoho stacku (přepínače se chovají jako jeden z pohledu managementu i připojených zařízení – včetně automatického loadbalancingu) vysokorychlostním redundantním propojením min. 80Gbps. 5. software podporující CLI (Telnet/SSH), SNMP management, včetně omezení přístupu na management z definovaných adres a subnetů, 6. podpora Jumbo Frames, min. 9 kB, podpora agregace portů (LACP) s využitím dvou switchů ve stacku (jedna agregace pře dva switche), 7. access listy (access control lists – ACL) aplikovatelné na IP L2 a L3 pro filtrování provozu; podpora globálních ACL, VLAN ACL, port ACL, a podpora IPv6 ACL, 8. bezpečnost – port security a implementace 802.1X, automatické zařazování do VLAN 802.1x – RADIUS server Windows AD, 9. šifrování na L2 dle IEEE 802.1AE (min. uplink porty), 10. podpora IPv4 a IPv6, 11. implementace (montáž, instalace, konfigurace, seznámení s funkcionalitami a obsluhou, dokumentace) 12. záruka 5 let.
P.29	Umístění L3 switchů do DC v rámci záložního zdravotnického operačního střediska.
P.30	Propojení do stávající infrastruktury, která zajišťuje propojení lokalit ZOS a ZZOS.
P.31	Napojení a předávání alertů a logů do Systému analýzy bezpečnostních logů (viz kap. 2.1.6). Včetně specifikace korelace kritických bezpečnostních alertů z tohoto aktivního prvku týkajících se IS ZOS.

Tabulka 5: L3 switche pro ZZOS

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce

2.1.5 Aplikační firewall pro IS ZOS

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.32	Dodávka webového aplikačního firewallu pro zabezpečení webových služeb (web services) v rámci externí komunikace IS ZOS. Minimálně následující aplikace: • Endpoint NIS IZS (SOS5) – publikováno do sítě NIS IZS • SOSView a SOSnow služby – publikováno do sítě Internet Jedná se o služby IS ZOS dostupné z externích sítí.
P.33	Funkcionalita webového aplikačního firewallu (WAF) bude poskytovat ochranu webových aplikací před kybernetickými útoky s využitím pozitivní i negativní bezpečnostní logiky v bezpečnostních politikách (detekci a ochranu před známými útoky a povolení explicitního legitimního provozu s minimální propustností 200Mbps. K těmto základním bezpečnostním politikám požadujeme implementaci dalších dodatečných bezpečnostních vlastností, jako je ochrana před útoky prolomením logovacích URL hrubou silou (Brute Force útoky) s možností eskalace a potlačení technologií CAPTCHA v případě podezření, že je aplikace pod útokem.

#	Požadavek
P.34	Je požadováno, aby WAF obsahoval technologie pro detekci a potlačení robotických (nelidských) uživatelů s možností výjimek (např. pro legitimní robotické klienty). WAF také zajistí ochranu před únosy HTTP relací. WAF musí podporovat SSL terminaci.
P.35	Aplikační firewall musí plnit následující min. parametry: 1. Ochrana proti aplikačním DoS a DDoS útokům (SlowLoris, R.U.D.Y, ApacheKiller, SSL útoky, SYN flood, HTTP flood aj.) 2. Ochrana proti "forcefull browsing", XSS, SQL-INJ, CSRF, remote command execution a ostatním útokům podle OWASP Top 10 3. Ochrana proti manipulaci s cookies 4. Ochrana parametrů webové aplikace 5. Session Management – ochrana proti únosům relací 6. Brute Force Ochrana – ochrana před prolomení hrubou silou 7. Detekce a potlačení robotických uživatelů aplikace 8. Ochrana AJAX a JSON aplikací, zabezpečení XML komunikace 9. Možnost rozšíření o detekci a ochranu před robotickými klienty pro nativní mobilní aplikace IOS a Android 10. Blokování požadavků z podezřelých prohlížečů (proaktivní ochrana proti botnetům) 11. Automatická instalace a aktualizace databáze pro detekci útoků, botnetů nebo kampaní kybernetických útoků 12. Blokování útočníků na základě geolokace 13. Podpora různých typů reportů – PCI, geolokační reporty, OWASP Top 10 14. Identifikace zařízení a potlačení škodlivých zařízení v bezpečnostní politice (fingerprinting) 15. Podpora rozkládání zátěže na více než 3 servery a podpora různých typů mechanismů rozkladu zátěže, minimálně kruhová metoda (round-robin), vážená kruhová metoda s (weighted round-robin) podle počtu spojení 16. Podpora zajištění konektivity uživatelů k serveru (persistence) na základě IP adresy, HTTP cookie 17. Podpora REST API pro správu a monitoring zařízení 18. Možnost doprogramovat filtrovací pravidla pro aplikace 19. Ochrana proti L7 DDoS útokům, web scrapingu a útokům pomocí hrubé síly (brute force), mitigace DDoS útoků založená na behaviorální analýze 20. Podpora SSL (šifrování a dešifrování) 21. Povoleni jednotlivých HTTP metod pro jednotlivá URL 22. Detekce anomálií a podezřelých operacích na aplikační vrstvě 23. implementace (instalace, konfigurace, seznámení s funkcionalitami a obsluhou, dokumentace) 24. záruka a aktualizace SW apod. na 5 let.
P.36	Implementace WAF na externě dostupné aplikace IS ZOS včetně jejich optimalizací a nastavení pravidel optimalizovaných pro chod těchto aplikací/rozhraní s ohledem na jejich funkčnost a dostupnost s detailní znalostí těchto aplikací/rozhraní.
P.37	Pro chod aplikačního FW je možné využít jak HW, který bude součástí dodávky řešení (viz kap. 2.1.7) nebo i stávající virtualizační infrastruktury ZZS za předpokladu, že nepřesáhne požadavek na jeden server (4v CPU, 8 GB RAM a 100 GB HD, OS MS Windows Server 2016 Standard nebo Linux). V případě vyšších požadavků na server dodavatel dodá i nezbytný HW a systémový SW včetně licencí pro běh FW (HW ve verzi rack mount).

#	Požadavek
P.38	Umístění aplikačního firewallu do DC v rámci primárního zdravotnického operačního střediska. S možností migrace do ZZOS v případě plné aktivace ZZOS (s možností využití stávající virtualizační platformy ZZOS).
P.39	Napojení a předávání alertů a logů do Systému analýzy bezpečnostních logů (viz kap. 2.1.6). WAF musí podporovat logování ve formátu minimálně Syslog, a případně s navrženým logovacím systémem (viz kap. 2.1.6). Součástí předávání logů do Systému analýzy bezpečnostních logů musí být veškeré kritické bezpečnostní události související s chráněnými aplikacemi ZOS a případných útocích na ně vedených. Součástí předávaných logů musí být také varování před nestandartními stavy jako jsou anomální nárůsty požadavků, pokusy o přístup do nepublikovaných částí aplikací apod. WAF musí dále předávat logy o veškerých přístupech (úspěšné i neúspěšné) do managementu WAF a informace o změnách konfigurací WAF.

Tabulka 6: Aplikační firewall pro IS ZOS

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce

2.1.6 Systém analýzy bezpečnostních logů (SW)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.40	Dodávka SW nástroje pro sběr dat (logů, alertů a dalších vstupů) a vyhodnocení kybernetických bezpečnostních událostí ze zabezpečovaných informačních systémů, infrastruktury, HW, systémového SW a technologií včetně IS ZOS a systému elektronické pošty. Systém bude sdružovat záznamy o událostech z jednotlivých aplikačních modulů IS ZOS, elektronické pošty a z okolí uvedených systémů (to je ze všech důležitých zařízení, systémů, sítě LAN/WAN a navazujících aplikací). Tyto záznamy bude ukládat a bude tyto záznamy dávat do souvislostí – korelovat a zajistí tak okamžitou detekci nebezpečného, případně nestandardního chování právě v IS ZOS, systému elektronické pošty nebo jejich infrastruktury.
P.41	Pro sběr dat z OS a DB serverů IS ZOS a elektronické pošty požadujeme minimálně následující události: • Přihlášení • Odhlášení • Neúspěšné pokusy o přihlášení Ukládání sesbíraných dat do úložiště nástroje pro následnou analýzu.
P.42	Zpracování (korelace) záznamů s cílem detekce nebezpečného, případně nestandardního chování v zabezpečovaných IS infrastruktury, infrastruktury, HW, systémového SW a technologií.
P.43	Zpracování bezpečnostních logů z IS ZOS a jeho komunikačních modulů/aplikací a elektronické pošty tak, aby bylo možné jej využít k identifikaci a korelaci bezpečnostních incidentů, a to nejenom na úrovni přístupů, včetně možnosti zablokování, ale i chování uživatele v rámci aplikace,
P.44	Minimální požadavky na systém analýzy bezpečnostních logů: 1. podporované protokoly: Syslog, Windows Events Collection (WinRM/RPC), FTP, S/TP/SCP, SNMP, ODBC/JDBC, CP-LEA, SDEE, 2. bezagentový sběr logů (sběr bez nutnosti instalovat agenta na cílový systém), 3. licence pro zpracování 300 EPS (událostí za sekundu) s možností rozšíření až na 5000 EPS, 4. možnost řešení jak prostřednictvím VirtualAppliance nebo samostatným HW, 5. počet zdrojů pro sběr logů minimálně 150,

#	Požadavek
	6. možnost sběru logů samostatným lokálním kolektorem s přeposíláním do centrálního systému, 7. možnost záložního uložení logů (rozšiřitelné úložiště neodpovídá tomuto požadavku), 8. centrální management všech komponent a administrativních funkcí ve webovém uživatelském rozhraní, 9. možnost definovat uživatelům systému přístup k jednotlivým zařízením, jejich skupinám či síťovým segmentům, 10. automatická identifikace systémů – zdrojů logů, 11. podpora šifrované komunikace mezi zdroji logů a systémem analýzy bezpečnostních logů, 12. integrace s adresářovým systémem (LDAP, Active Directory) pro potřeby autentifikace uživatelů, 13. minimální administrace /výběr zařízení ze seznamu od výrobce/pro připojení dalších zdrojů událostí (servery Windows, Unix/Linux, přepínače, routry, FW apod.), 14. Log Management s minimální postimplementační administrací. /agregace událostí dle typů, analýza, vyhodnocování/ pro případy, jako je zavedení nového zdroje událostí, nastavení pravidel pro sběr dat a archiv událostí, 15. definice základních korelačních pravidel v návaznosti na IS ZOS s důrazem na jeho bezpečnost a případné pokusy o zneužití, a to vše s korelací získávaných informací z okolí systému (provoz, aktivní prvky, OS atd.), 16. podpora sběru síťových toků (NetFlow, JFLow, Sflow) z navržených infrastrukturních prvků (switche, routery, NetFlow sondy), 17. řešení musí umožňovat automatické aktualizace, 18. webové uživatelské rozhraní pro management, analýzu a reporting, 19. poskytování automatického backup/recovery procesu, 20. poskytovat interní kontroly stavu zařízení (healthcheck) a upozornění uživatele v případě problému, 21. možnost integrovaného managementu rizik na základě síťových toků a konfigurace aktivních prvků do GUI, 22. poskytování analytických a korelačních funkcí bez dalších zásahů a činností (out-of-the-box), 23. řešení musí být dodáno jako all-in-one appliance (vAppliance), 24. sběr logů z dalších bezpečnostních a síťových systémů (např. FlowMon, AFW f5, FW Cisco, AV Symantec, IronPort Cisco) a prvků navržených v rámci tohoto projektu, 25. výkonová rozšiřitelnost – přidání nových zařízení, lokací, aplikací, 26. možnost rozšíření výběrů o uživatelské položky z obsahu logů, 27. zajištění integrity nasbíraných dat, 28. umožnění nárůstu zdrojů událostí bez nutnosti pořizování dalšího hardware (v případě fyzického HW), 29. Near-real-time analýza událostí, 30. analýza dlouhodobých trendů událostí, 31. řešení musí být hodnocené v segmentu „leaders“ v GartnerMagicQuadrantu za minulé dva roky, 32. pokročilé "drill-down" dohledávání v případě potřeby, 33. možnost agregace události z logů i podle položek které nejsou standardně zahrnuty v řešení,

#	Požadavek
	34. podpora a normalizace časových značek z různých časových zón, 35. sběr textových logů ze souborů, 36. sběr logů z databází pomocí JDBC/ODBC, 37. sběr log záznamů z prostředí Windows a Linux/Unix/AIX. Sběr Windows EVT záznamů i z Windows Server, a navržených OS v rámci SOBD, 38. rozčlenění vyhledaných dat (Drilldown): Vyhledávací rozhraní systému správy logů musí nabízet možnost rozčlenění vyhledaných dat až na detailní úroveň, IP adresa, typ události, protokol, port atd., 39. způsob zadávání vyhledávání: vyhledávací rozhraní systému správy logů musí poskytovat podporu jak pro zadání dotazu s použitím Booleovy logiky, tak pro regulární výrazy, 40. poskytování alertů na detekované anomálie, změny chování sítě a změny v generování logů a událostí, a to i v návaznosti na aplikaci operačního řízení, 41. kombinované hledání v indexovaných i neindexovaných datech v systému správy logů s použitím regulárních výrazů a fulltextového vyhledávání v nestrukturovaném textu současně, 42. korelační modul musí poskytovat již po instalaci (out-of-the-box) metody korelačních pravidel, která automatizují zjišťování incidentů a související workflow procesy, 43. korelace mezi zařízeními již po instalaci (out-of-the-box). Zjišťování chyb autentizace, chování perimetru a výskytu infiltrací (červů apod.) bez potřeby specifikovat typy sledovaných zařízení, 44. řešení musí poskytnout alerting vycházející z detekovaných bezpečnostních hrozeb od monitorovaných zařízení a aplikace operačního řízení, 45. alerting založený na vypozorovaných anomáliích a změnách chování sítě (analýza síťových toků). Řešení musí poskytovat NBAD (Network Behavior Anomaly Detection) funkcionalitu, 46. řešení musí poskytnout alerting porušení bezpečnostních pravidel, založený na stanovené bezpečnostní politice (např. IM provoz je zakázán), 47. vykonávání akcí v závislosti na přijatém logu jako např. zaslat email, 48. schopnost pracovat s IP geolokacemi (botnet kanály atp.), 49. generování alertu při výpadku logů z konkrétního zařízení, 50. vestavěný mechanismus na klasifikaci systémů podle typu (např. mail server vs. databázový server), 51. vyhodnocení chybějících sekvencí (např. služba přestala běžet), 52. schopnost monitorovat historii útoků (typů událostí) na kritické komponenty a historii útoků jednotlivých uživatelů, 53. schopnost korelovat události DHCP, VPN a Active Directory a sledovat průběh uživatelské relace (session) v rámci celé instituce (přesná identifikace uživatele), 54. schopnost korelovat data o událostech se statickými a dynamickými seznamy označujícími položky, které mají či nemají být v síti povoleny (tj. seznam nezabezpečených protokolů), 55. poskytování rozhraní pro reporting, pomocí kterého lze vytvářet nové sestavy bez nutnosti sestavovat SQL dotazy, 56. nezměněná funkcionalita reportingu i při změně nebo náhradě některé technologie jako např. firewallu nebo IDS, 57. přístup k datům skrze otevřené REST API pro integraci s dalšími systémy,

#	Požadavek
	58. postupné doplňování funkcionalit pro log management a security intelligence (rozšíření o další analytické moduly by mělo mít minimální dopad přidávání komponent třetích stran a mělo by být primárně umožněno jen licenčním klíčem), 59. řešení musí být schopno pracovat s interními překrývajícími se rozsahy adres, 60. řešení si musí pasivně budovat tabulku zařízení v síti z informací obsažených v již příchozích zdrojích (flows), 61. schopnost agregovat záznamy o síťovém provozu z obou stran datového toku do jedno záznamu, 62. provádění deduplikace záznamů o síťovém provozu v případě identických záznamů z různých zařízení, 63. podpora korelace dat proti výsledkům scanům zranitelností třetích stran, 64. uchovávání logů i flows jak v normalizovaném formátu, tak i „raw“ formátu, 65. řešení nebude licenčně omezeno počtem používaných korelačních pravidel a nebude licenčně omezeno počtem generovaných reportů, 66. možnost nasazení High Availability režimu v jakékoliv fázi životního cyklu řešení bez nutnosti reinstalace řešení.
P.45	Záruka 5 let, 5x8, garantovaná doba opravy do následujícího pracovního dne na místě včetně update SW a všech modulů.
P.46	Součástí dodávky musí být instalace a konfigurace řešení, včetně součinnosti při konfiguraci jednotlivých zařízení a aplikací a nastavení notifikací, a to včetně seznámení s funkcionalitami a obsluhou. Dále je požadováno za měsíc a za 3 měsíce vyhodnocení provozu a doladění korelačních pravidel na základě získaných dat během provozu implementovaného systému a dle požadavků Zadavatele.
P.47	Implementace notifikací s využitím stávajících notifikačních nástrojů ZZS a to včetně implementace napojení na svolávací systém. Notifikace budou prováděny následujícími nástroji: • Email • SMS • Hlasová zpráva (text-to-Speech) • Push aplikace na mobilní zařízení • Využití záložního svolávacího systému (jiná ZZS) *Pro notifikaci emailem bude využíván protokol SMTP, rozhraní stávajícího svolávacího systému bude poskytnuto v rámci implementační analýzy.*
P.48	Sběr logů z aplikačních, bezpečnostních a síťových systémů využívaných v rámci ZZS nebo dodávaných v rámci dodávky.
P.49	Nástroje/rozhraní pro logování z IT infrastruktury: 1. Aktivní prvky (sítě) 2. Informační systémy – IS ZOS/ZZOS a systém elektronické pošty 3. Databáze (ORACLE, MS SQL) 4. Operační systémy (MS Windows, Linux) – servery, pracoviště ZOS/ZZOS V případě, že se bude jednat o jeden nástroj zajišťující všechny uvedené služby, musí nástroj umožnit samostatný přístup k různým službám pro různé osoby na základě oprávnění definovaného správcem a možnost instalace na oddělený samostatný server.
P.50	Dodávka a implementace nástroje na logování z IT infrastruktury, IS ZOS a elektronické pošty, tzn. aktivní prvky, aplikace, operační systémy apod. ve kterém bude možnost plošně prohledávat sesbíraná data a mít k dispozici statistiku a analytické funkce – přičemž zdrojem dat může být stávající syslog systém a bude rozšířen o následující funkce:

#	Požadavek
	1. Schopnosti provádět korelace přes více datových zdrojů a hledání specifických vzorů 2. Dlouhodobé retence dat (minimálně 3 měsíce, optimálně 6 měsíců) 3. Předpokládaný objem logovaných dat do 5 GB za den 4. Jeden společný datový sklad pro všechna indexovaná data – jeden dotaz nebo report může zahrnout všechna indexovaná data 5. Není třeba vytvářet datové schéma nebo připravit vyhledávací dotazy ještě před indexováním 6. Možnost využití nestrukturovaných souborů a datového skladu bez pevného schématu (bez relační databáze s pevným schématem) 7. Schopnost indexovat a připravit pro vyhledávání všechna originální data bez jakékoliv modifikace (bez normalizace/redukce dat) 8. Automatická komprese indexovaných dat pro redukci nároků na úložný prostor 9. Flexibilní nastavení uchování dat s možností odstupňování řízení toho, co se stane s postupně stárnoucími daty. Neaktuální data mohou být přesunuta na externí (levnější) datové úložiště k archivaci a (nebo) smazána. 10. Flexibilní kontrola přístupu na základě rolí pro řízení přístupu uživatelů a přístupů přes API. 11. Integrace autentizace a autorizace s Microsoft Active Directory, případně samostatný oddělený systém pro auditní účely (mimo stávající systém AD). 12. Generování hashe pro každou událost v době indexování tak aby umožnilo při vyhledávání zjistit, zda s daty nebylo manipulováno 13. Monitoring své vlastní konfigurace a využití s cílem udržet si kompletní, digitálně podepsané auditní záznamy o tom, kdo přistupuje k systému, jaké dotazy spouští, na jaké reporty se dívá, jaké konfigurační změny provádí a další. 14. Řešení by mělo umožnit snadné vytváření široké palety vizualizací (nejen pevně dané, předpřipravené reporty) 15. Dostupné vizualizace by měly zahrnovat: čárový graf, časový graf, plošný graf, sloupcový graf vertikální, sloupcový graf horizontální, jediná hodnota s trendem (růst, pokles), koláčový graf, bodový graf, bublinový graf, ciferníkový (budíkový) ukazatel, graf typu teploměr (zobrazení hodnoty ve vztahu k rozsahu), geolokační mapa, graf zobrazující rozložení hodnot v geografických regionech, kruhový graf, výplňový graf, tabulky (vč. doplňkových funkcí jako jsou automatické sumy, procentuálních vyjádření, číslování řádků, atd.)
P.51	Implementace nástroje na logování bude obsahovat nejenom zprovoznění a základní nastavení systému ale vytvoření i reportů a dashboardů (náhledů) na jednotlivé komponenty IT infrastruktury a IS ZOS. Minimálně následující náhledy: 1. Aktivní prvky (LAN/WAN/FW) – přihlášení, změny konfigurací, chyby atd. 2. FW/VPN – přístupy (oprávněné a neoprávněné) včetně geolokace (zobrazení na mapě a v tabulce) 3. Operační systémy a databáze IS ZOS – přihlášení, chyby atd. 4. Emailová komunikace – přístupy (oprávněné a neoprávněné) včetně geolokace, chyby systému atd.
P.52	Je požadována realizace jednotného bezpečnostního portálu pro správce a management ZZS, který bude zahrnovat dodané technologie v rámci projektu. Minimální požadavky na přehledový bezpečnostní portál:

#	Požadavek
	1. Webové rozhraní 2. Autentizace/autorizace uživatelů proti Microsoft Active Directory 3. Zobrazení posledních incidentů na základě analýzy bezpečnostních logů 4. Zobrazení VPN připojení (úspěšné i neúspěšné) 5. Zobrazení přihlášení do aplikací IS ZOS (úspěšné i neúspěšné) 6. Zobrazení přehledu emailové komunikace ZZS (chyby, vytížení apod.) 7. Možnost dalšího rozvoje dle požadavků ZZS – otevřený systém
P.53	Systém analýzy bezpečnostních logů (SW) bude provozován na infrastruktuře (HW a systémový SW) požadovaný a dodávaný dle kap. 2.1.7 – Infrastruktura (HW) a systémový SW pro systém analýzy bezpečnostních logů.

Tabulka 7: Systém analýzy bezpečnostních logů (SW)

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce

2.1.7 Infrastruktura (HW) a systémový SW pro systém analýzy bezpečnostních logů

V této kapitole jsou uvedeny požadavky na infrastrukturu (HW) a nezbytný systémový SW pro provoz dodávaných technologií – Systém analýzy bezpečnostních logů (SW).

Zadavatel nepředepisuje technologii, jen principy a požadavky na řešení. Technologie bude navržena dodavatelem v nabídce v rámci veřejné zakázky.

HW a SW infrastrukturu není možné v této dokumentaci dostatečně specifikovat, protože jsou závislé na zvolené technologii v rámci řešení konkrétního uchazeče. Zde jsou stanoveny limitní podmínky, které musí uchazeč splnit, tj. nejen technologické podmínky v DC, technologie využívané zadavatelem, ale i požadavky na min. doby pro ukládání dat a v návaznosti na splnění těchto podmínek a potřeb technologie, uchazeč navrhne a dodá vhodnou HW a SW infrastrukturu.

#	Požadavek
P.54	Dodávka min. 1 ks následujících serverů s min. konfigurací: 1. provedení Rack mount (včetně potřebných montážních komponent a ramene pro kabeláž) pro až 28 disků velikosti 2,5“, maximální velikost 2U, pro přístup ke všem komponentám serveru bez použití nářadí 2. minimálně jeden šestnácti jádrový procesor s hodnotou dle SPECint_rate2006 base min. 1700 bodů a dle SPECfp_rate2006 base min. 1300 pro 2 CPU konfiguraci (údaje musí být k dispozici na www.spec.org) 3. min. 192 GB RAM (min. 32GB moduly 2666MHz) s celkem 24 DIMM pozicemi 4. min. 14x 900GB SAS 15K v raid 5 pro data 5. hw řadič s min. 2GB cache a podporou raid 0, 1, 5, 6, 50 6. min. 4x 1Gbase-T ethernet síťové porty s podporou IPv4, IPv6 7. min. 2x 10Gbit SFP+ ethernet síťové porty s podporou TOE, IPv4, IPv6 včetně dvou SFP+ DA kabelů pro připojení do stávající infrastruktury 8. 2 redundantní síťové napájecí zdroje min. 750W 9. management serveru nezávislý na operačním systému s dedikovaným USB či SD úložištěm (data na úložišti musí být dostupná i v případě výpadku interních disků a musí být možné ji rozdělit na několik nezávislých partition s možnosti volby boot sekvence) poskytující management funkce a vlastnosti: webové rozhraní a dedikovaná IP adresa,

#	Požadavek
	sledování hardwarových senzorů (teplota, napětí, stav, chybové senzory); podpora virtuální mechaniky 10. vyžadována je schopnost monitorovat a spravovat server out-of-band bez nutnosti instalace agenta do operačního systému 11. management musí podporovat dvou faktorovou autentifikaci, filtrování přístupu na základě IP adres (IP blocking) a AD/LDAP 12. Záložní BIOS v dedikované ROM s možností manuální/automatické obnovy 13. požadujeme vestavěné GUI s podporou HTML5 a možnost komunikace pomocí: HTTPS, CLI, IPMI, WSMAN, REDFISH 14. certifikace pro aktuální verze VMware ESX, vSphere, Windows Server 2016, Red Hat Enterprise Linux a SUSE 15. součástí je licence MS Windows Server 2016 Datacenter pro min. 16 jader (odpovídající nabízenému procesoru) 16. podpora na 5 let typu NBD, oprava v místě instalace zařízení Server bude předán v místě plnění po základní instalaci HW v místě plnění, konfiguraci a instalaci SW (virtualizační platforma) včetně aktualizace firmware a ověření funkčnosti kupujícím.
P.55	Dodávka a instalace systémového SW: 1. Požadujeme dodávku systémového SW pro všechny nabízené systémy. Jedná se o minimálně následující systémový SW: o Operační systémy serverů, kde požadujeme dodávku všech licencí potřebných operačních systémů a mimo to požadujeme jako součást HW dodávaných serverů (viz požadavek na dodávku serveru výše) licenci Windows Datacenter. o Databáze pro dodávané systémy dle jejich požadavků o Pro virtualizaci dodávaných serverů požadujeme kompatibilní řešení se stávající virtualizací tak, aby bylo možné zařadit do jedné konfigurační konzole – Minimálně licence na dodávaný počet CPU (VMware vSphere 6 Standard for CPU) s podporou výrobce na 5 let. 2. V případě, že nabízené řešení vyžaduje další nespecifikovaný systémový SW tak musí být součástí nabídky.
P.56	Součástí dodávky je integrace dodávaných technologií do stávajícího monitorovacího nástroje (WhatsUp firmy Ipswitch), který není součástí dodávky tohoto projektu. Monitoring musí jednoznačně identifikovat chod jednotlivých komponent.
P.57	Součástí dodávky není strukturovaná kabeláž.
P.58	Dodávka, zapojení, instalace technologií, instalace a zprovoznění dodávaných technologií a prvků na dodaných technologiích.

Tabulka 8: Infrastruktura (HW) a systémový SW pro systém analýzy bezpečnostních logů

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce

2.1.8 Úpravy IS ZOS

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
Napojení na Systém analýzy bezpečnostních logů (SW) (viz kap. 2.1.6)	

#	Požadavek
P.59	Je požadována úprava systémů IS ZOS pro zaznamenávání činností v rámci operací těchto systémů do externích systémů pro následné zpracování a analýzy – Systém analýzy bezpečnostních logů (SW) (viz kap. 2.1.6).
P.60	**IS OŘ:** Předávání logů z IS OŘ do systému analýzy bezpečnostních logů v následujícím rozsahu: 1. Přihlášení a odhlášení do systémů a modulů 2. Chybná přihlášení do systému a modulů 3. Operace s daty (pořízení, modifikace a zobrazení) 4. Možnost předávání logů s anonymizovanými položkami – dle druhu informace a účelu jejího pořízení – na základě konzultace a požadavků ZZS
P.61	**GIS:** Předávání logů z GIS do systému analýzy bezpečnostních logů v následujícím rozsahu: 1. Přihlášení a odhlášení do systému 2. Chybná přihlášení do systému Logy jsou ukládány na diskové úložiště, odkud mohou být automatizovaně zpracovávány Systémem analýzy bezpečnostních logů. V případě využití této možnosti je součástí dodávky parsování logů, jejich analýza a ukládání do Systému analýzy bezpečnostních logů.
P.62	**EKP/MZD:** Předávání logů z EKP/MZD do systému analýzy bezpečnostních logů v následujícím rozsahu: 1. Přihlášení a odhlášení do systémů a modulů 2. Chybná přihlášení do systému a modulů 3. Operace s daty (pořízení, modifikace a zobrazení) 4. Možnost předávání logů s anonymizovanými položkami – dle druhu informace a účelu jejího pořízení – na základě konzultace a požadavků ZZS
P.63	**IS Pojišťovna:** Předávání logů z IS Pojišťovna do systému analýzy bezpečnostních logů v následujícím rozsahu: 1. Přihlášení a odhlášení do systémů a modulů 2. Chybná přihlášení do systému a modulů 3. Operace s daty (pořízení, modifikace a zobrazení) 4. Možnost předávání logů s anonymizovanými položkami – dle druhu informace a účelu jejího pořízení – na základě konzultace a požadavků ZZS
P.64	**Systém sledování vozidel (AVL):** Předávání logů z AVL do systému analýzy bezpečnostních logů v následujícím rozsahu: 1. Přihlášení a odhlášení do systému 2. Chybná přihlášení do systému 3. Informace odeslání informací k dané události do technologie AVL ve voze 4. Možnost předávání logů s anonymizovanými položkami – dle druhu informace a účelu jejího pořízení – na základě konzultace a požadavků ZZS Logy jsou ukládány na diskové úložiště, odkud mohou být automatizovaně zpracovávány Systémem analýzy bezpečnostních logů. V případě využití této možnosti je součástí dodávky parsování logů, jejich analýza a ukládání do Systému analýzy bezpečnostních logů.
P.65	**Svolávací systém** využívá data IS OŘ a jeho volání je vždy z IS OŘ, tj. data budou sbírána cestou IS OŘ.
P.66	**Telefonní ústředna** je integrována s IS ZOS prostřednictvím API serveru. Vlastní přístup na server určený pro API rozhraní je logován v rámci systémových prostředků OS. Data jsou tedy sbírána na systémové úrovni. Součástí dodávky parsování logů, jejich analýza a ukládání do Systému analýzy bezpečnostních logů.

#	Požadavek
P.67	**Záznamový systém (REDAT)** je uzavřené řešení pro nahrávání hovorů. Dispečeři ZOS mají přístup k nahrávkám prostřednictvím systému IS OŘ, který loguje přístupy k aplikačnímu serveru systému REDAT v rámci IS OŘ. Tyto informace jsou tak předávány v rámci přeposílání logů IS OŘ. Součástí dodávky parsování logů z IS OŘ je jejich analýza a ukládání do Systému analýzy bezpečnostních logů.
P.68	**Integrace telefonie a radiofonie** je vázaná na dané dispečerské pracoviště a informace o přihlášení a přístupu uživatele budou brány z IS OŘ dle toho, který dispečer na daném pracovišti pracoval (vlastní integrace nevyužívá speciální přístupy a ovládá komunikační prostředky na daném pracovišti). Vlastní přístup na server určený pro integraci je logován v rámci systémových prostředků OS. Data jsou tedy sbírána na systémové úrovni. Součástí dodávky parsování logů z IS OŘ je jejich analýza a ukládání do Systému analýzy bezpečnostních logů.
P.69	**Záložní IS ZOS (ZZOS):** ZZOS využívá v současné době repliku systému IS OŘ. Je požadováno, aby pro tento systém byla sbíraná data stejná v primární i záložní lokalitě.
P.70	Aplikační SW na pracovištích ZOS/ZZOS: Vlastní přístup do OS na pracovištích ZOS a ZZOS bude logován v rámci systémových prostředků operačního systému. *Sbíraná data z operačních systémů a dalších technologie na pracovištích ZOS/ZZOS budou sbírána na systémové úrovni.*
Napojení IS OŘ na FireWall s IPS pro ZZOS (viz kap. 2.1.2)	
P.71	V rámci IS OŘ bude možné přijímat i alerty upozorňující na bezpečnostní události a to nejenom z uvedených bezpečnostních prvků ale všech komponent zabezpečení. Bude se jednat o alerty bezpečnostních událostí relevantních k provozu centrálního dispečinku a celého IS ZOS s kritickou důležitostí. Bezpečnostní alerty v rámci IS ZOS budou definovány a konfigurovány na základě požadavků ZZS v systémech analýzy a sběru bezpečnostních logů, který tyto alerty bude předávat do IS OŘ – dispečerského pracoviště. Tak bude aktivně informován provoz centrálního dispečinku ZOS o vážných bezpečnostních událostech.
P.72	Oprávněné osoby centrálního dispečinku budou mít možnost pomocí rozhraní v IS ZOS (IS OŘ) na základě vzniklých bezpečnostních událostí a jejich průběhu rozhodnout o možnosti aktivace (a následné deaktivace) izolace systému IS ZOS od externích sítí nebo i od interních LAN/WAN segmentů. Vlastní izolace bude realizována na uvedených bezpečnostních prvcích (ZOS/ZZOS). Oprávněný uživatel bude před vlastní aktivací daného typu izolace informován o rozsahu izolace a z toho plynoucích omezení centrálního dispečinku a IS ZOS. O těchto událostech bude proveden detailní záznam událostí včetně jejich časové souslednosti a uživatelích, kteří taková opatření realizovali a neprodleně automaticky informováni definovaní pracovníci ZZS v rámci stávajícího svolávacího systému ZZS.
Autentizace uživatelů operačního řízení prostřednictvím AD	
P.73	V rámci sjednocení ověřování identity uživatelů v rámci IT a operačního řízení je požadováno využití stávající domény v rámci Microsoft Active Directory. Pro tyto účely požadováno rozšíření stávajícího IS ZOS o možnost autentizace a autorizace v rámci struktury Active Directory.
P.74	**IS OŘ:** Správce IS OŘ bude pak schopen zvolit způsob autentizace jednotlivých uživatelů dle potřeb ZZS a typu modulů/subsystémů. Je požadováno, aby bylo možné plně využít pro autentizaci a autorizaci uživatelů IS OŘ jednotných účtů v rámci MS Active Directory. Autorizace uživatelů pro jejich oprávnění pak bude spočívat v příslušnosti k dané skupině uživatelů.
P.75	**EKP/MZD:** EKP/MZD musí umožňovat autentizaci a autorizaci uživatelů jak interní (stávající stav) nebo v rámci MS Active Directory. Správce IS v návaznosti na okolní systémy bude schopen zvolit způsob autentizace EKP/MZD dle požadavku ZZS. Autorizace uživatelů pro jejich oprávnění pak bude spočívat v příslušnosti k dané skupině uživatelů.
Integrace s personálním systémem	

#	Požadavek
P.76	IS OŘ a EKP/MZD musí umožnit využití integrace s personálním systémem, a to jak při zakládání uživatele a případně jejich základní role v rámci personálního systému (která se promítne do AD) využití zneplatnění účtů uživatelů, u kterých bude ukončen pracovní poměr (zneplatnění/vymazání účtu v AD). Tím bude zajištěna maximální aktuálnost uživatelských účtů zaměstnanců ZZS.
Monitoring a reporting a přístupů	
P.77	Pro správu a reporting oprávnění bude dodán i samostatný portál pro správu uživatelů IS OŘ a přiřazování jejich rolí. Tento portál bude sloužit pro vedoucí pracovníky OŘ, kteří budou tato oprávnění spravovat a kontrolovat a monitorovat.
P.78	Součástí dodávky bude nástroj pro reportingu všech změn provedených jednotlivými uživateli/administrátory v rámci Microsoft Active Directory (AD) ZZS, tak aby bylo možné kontrolovat změny oprávnění, které byly v rámci AD provedeny. Je požadováno reportovat minimálně: • Vytvoření nového uživatele nebo skupiny • Vymazání uživatele nebo skupiny • Zneplatnění (disable) uživatele • Přidání člena skupiny • Vymazání člena skupiny
Infrastruktura (HW) a systémový SW pro úpravy IS ZOS	
P.79	Stávající infrastruktura (HW) a systémový SW pro běh IS ZOS po realizaci úprav zůstane beze změny, tj. nedojde ke změně konfigurace, parametrů, licencí systémového SW využívaných pro běh IS ZOS.

Tabulka 9: Úpravy IS ZOS

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce

2.1.9 Konfigurace systému elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.80	Napojení na Systém analýzy bezpečnostních logů (SW) a předávání následujících dat ze systému elektronické pošty: • Úspěšná a neúspěšná připojení k systému dostupnými protokoly • Využívání systému elektronické pošty jednotlivými uživateli • Dostupné bezpečnostní logy používaného systému • Dostupné chybové a provozní logy používaného systému Předávání veškerých logů systému do nástroje/rozhraní pro logování.
P.81	Toto nastavení realizovat pro všechny komponenty systému elektronické pošty.
P.82	Předávání logů systému online prostřednictvím syslog služby.
P.83	Součinnost při konfiguraci FireWallu ZOS a konfigurace FireWallu ZZOS pro získávání informací o bezpečnostních událostech na prvcích FireWall, týkajících se systému elektronické pošty. Minimálně: • Odepření přístupu z dané IP adresy na systém (reputace dynamický ACL apod.) • IPS a AntiMalware události

#	Požadavek
	• Identifikace chyb v protokolu
P.84	Systém dynamických ACL na základě parametrického vyhodnocení bezpečnostních logů systému. Dynamický ACL bude vytvářen prostřednictví analýzy logů na základě neoprávněného přístupu k systému. Pro vytváření dynamických ACL bude možné systémově nastavovat následující parametry: • Počet špatných přihlášení k danému protokolu • Minimální čas od posledního výskytu špatného přihlášení Publikace dynamického ACL pro systém elektronické pošty bude pro účely aktualizace pravidel FireWallu realizována web serverem jako standardní textový soubor s výčtem (list) IP adres (jedna IP na jednom řádku).
P.85	Nástroj/rozhraní pro logování bude zpracovávat i uvedený dynamický ACL pro systém elektronické pošty a zobrazovat časový průběh počtu IP adres obsažených v listu a upozorňovat na enormní nárůst.
P.86	Provedení konfigurace FireWallu ZZOS (kap. 2.1.2) a součinnost pro konfiguraci FireWallu ZOS pro implementaci dynamického ACL – aktualizace listu IP adres

Tabulka 10: Úpravy elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce

2.1.10 Dvoufaktorová autentizace administrátorských VPN přístupů

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.87	Pro autentizaci administrátorských VPN přístupů je požadován systém dvoufaktorové autentizace. Minimální požadavky: 1. Integrace se stávajícím FireWallem ZOS a autentizačním serverem 2. Správa pomocí webové konzole nebo Microsoft Management Console (MMC) 3. Bez potřeby dalšího zařízení nebo tokenu 4. Kompatibilní se všemi telefony, které umožňují přijímat SMS 5. Jednorázové heslo nejen přes mobilní aplikaci, push notifikaci, hardwarové tokeny a SMS, ale i vlastní cestou (např. e-mailem). 6. Push autentifikace – možnost autentifikace potvrzením v aplikaci na mobilním telefonu, bez nutnosti přepisovat jednorázové heslo (podpora iOS, Android i Windows Mobile). 7. Podpora Virtual Private Networks (VPN) – Cisco ASA, Remote Desktop Protocol (RDP) a RADIUS.
P.88	Licence pro 20 min. uživatelů.
P.89	Je požadována záruka na funkčnost, podpora a aktualizace po dobu min. 5 let.

Tabulka 11: Dvoufaktorová autentizace administrátorských VPN přístupů

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce

2.1.11 Nástroje pro bezpečnostní audit a penetrační testy

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.90	Je požadována dodávka nástroje/nástrojů pro periodické testování bezpečnostních zranitelností interních systémů i systémů, které komunikují s externími subjekty i jako součást penetračních testů (nástroj/nástroje budou využity v rámci kap. 2.1.12 – Bezpečnostní audit a penetrační testy.
P.91	Minimální rozsah: externí testy, interní testy a testy zranitelností operačních systémů, databází a informačních systémů (aplikací). Jedná se minimálně o: 1. Host Discovery – vyhledávání aktivních strojů; 2. Port Scanning – skenování portů; 3. Service Discovery – vyhledání běžící služby; 4. Web Applications – skenování webových aplikací;
P.92	Je požadováno, aby nástroj/nástroje umožňoval: 1. Vzdálené privilegované a neprivilegované skeny 2. Neomezené množství koncových IP adres 3. Pravidelné aktualizace signatur/detekčních metod (cca 1xtýdně)
P.93	Předmětem dodávky není periodické provádění testů zranitelností (nad rámec testů v rámci vedlejších aktivit), ale zajištění nástrojů pro provádění a vyhodnocování uvedených testů.
P.94	S ohledem na vysokou citlivost zpracovávaných dat musí být dodaný nástroj možné kompletně instalovat na server/počítač umístěný v lokální síti, která je pod správou Zadavatele. Výstupy z testů/skenů musí být rovněž zpracovávány lokálně, bez zasílání do cloudu. Dodaný nástroj musí umožňovat ovládání s pomocí webového GUI.
P.95	Instalaci nástroje musí být možné realizovat na prvky s operačními systémy Microsoft Windows 7 a vyšší, Microsoft Windows Server 2008 a vyšší, macOS i Linux. Součástí dodávky nebude HW, OS ani další aplikační vybavení nutné pro provoz nástroje. Předpokládá se instalaci na prostředky Zadavatele (virtuální server nebo testovací PC/notebook).
P.96	Dodané řešení musí podporovat realizaci vzdálených bezagentských privilegovaných i neprivilegovaných skenů neomezeného počtu zařízení/IP adres a musí být schopné realizovat bezpečnostní skeny webových aplikací.
P.97	Řešení musí být schopné identifikovat chybějící záplaty/zranitelné služby a aplikace běžící na skenovaných systémech.
P.98	Součástí dodávky bude licence relevantního nástroje s podporou a funkčností po dobu 5 let, instalace a aktivace jednoho skeneru v prostředí Zadavatele a úvodní zaškolení administrátorů a uživatelů.

Tabulka 12: Nástroje pro bezpečnostní audit a penetrační testy

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce

2.1.12 Bezpečnostní audit a penetrační testy

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.99	Bezpečnostní analýza stávajícího prostředí z pohledu souladu se zákonem 181/2014 Sb., ve znění pozdější novelizace a s vyhláškou 82/2018 Sb.
P.100	Hodnocení stávajícího rozsahu řízení bezpečnosti informací: 1. Politiky

#	Požadavek
	2. Metodiky a. Metodika identifikace a hodnocení aktiv b. Metodika analýzy rizik 3. Proces a výstupy hodnocení aktiv 4. Proces a výstupy hodnocení rizik 5. Revize primárních a podpůrných aktiv, jejich vzájemné vazby, určení jejich hodnoty a hodnocení jejich správy garanty 6. Plán zvládání rizik 7. Prohlášení o aplikovatelnosti bezpečnostních opatření 8. Zajištění zpětné vazby 9. Plán rozvoje bezpečnostního povědomí 10. Strategie řízení kontinuity 11. Pravidla řešení kybernetických bezpečnostních incidentů 12. Pravidla řízení provozu ICT 13. Hodnocení definice kontextu organizace, hodnocení jeho rozdělení na vnitřní a vnější kontext a hodnocení SLA mezi těmito 2 kontexty
P.101	Přezkoumání implementace technických opatření do praxe. Technické ověření souladu implementace primárních a podpůrných aktiv dle požadavků ZKB: 1. Aplikace 2. Operační systémy 3. Síťové prvky 4. Bezpečnostní prvky 5. Fyzická bezpečnost 6. Zálohování 7. Apod.
P.102	Výsledkem auditu bude: 1. Zpráva z přezkoumání stávajícího prostředí Zadavatele s následujícím obsahem: a. Pro každé opatření bude uveden popis aktuálního stavu b. Zhodnocení z pohledu požadavků prováděcí vyhlášky KB (ZKB) c. Případné zhodnocení z pohledu „best practice“, pokud bude takovéto doporučení žádoucí. d. Každé opatření bude popsáno minimálně v rozsahu ½ A4. e. Obsahem zprávy jsou veškeré paragrafy obsažené v prováděcí vyhlášce ZKB, tzn. Že se organizace zkoumá z pohledu organizační opatření, technických opatření i fyzické bezpečnosti. 2. Hodnocení stavu a. Přehledový dokument s výpočetní logikou, který bude hodnotit výsledek pro ▪ Technické role ▪ Odděleně a s menší mírou detailu pro manažerské role b. Hodnocení bude provedeno jednotlivě pro každý požadavek paragrafů ZKB 3. Obecný návrh nápravných opatření a. Cílem není hodnotit veškeré možné technické varianty nápravných opatření, ale určit orientační výši nákladů pro zajištění souladu se ZKB a určit druh technologie. 4. Prezentace výsledků projektu pro projektový tým a. PT prezentace a diskuze s týmem

#	Požadavek
	5. Prezentace výsledků projektu pro vrcholový management
P.103	Provedení penetračních testů a testů zranitelnosti: 1. Provedení penetračních testů a testů zranitelnosti pro IS ZOS, IS ZZOS a systému elektronické pošty. 2. Pro systémy IS ZOS, IS ZZOS a Elektronickou poštu budou provedeny závěrečné testy zranitelnosti z externí sítě. V zájmu ověření korektního fungování webového aplikačního firewallu (WAF) a zajištění vysoké úrovně bezpečnosti provozovaných webových aplikací je požadováno provedení jednorázových penetračních testů.
P.104	Závěrečné testy zranitelnosti budou provedeny z externí sítě na IS ZOS, IS ZZOS a Elektronickou poštu. Jedná se tedy o testy zranitelnosti realizované přes bezpečnostní prvky – perimetry (FireWall) implementované v ZOS a ZZOS. Tyto testy musí obsahovat min.: 1. Host Discovery – vyhledávání aktivních strojů; 2. Port Scanning – skenování portů; 3. Service Discovery – vyhledání běžící služby; 4. Web Applications – skenování webových aplikací; Účelem těchto testů je ověření konfigurace perimetrů a nalezení zranitelností publikovaných služeb/systémů.
P.105	Součástí bezpečnostního auditu budou i penetrační testy, které musí splňovat minimálně: 1. Penetrační testy se budou týkat uvedených aplikací provozovaných zadavatelem a jejich účelem bude identifikovat případné nedostatky v nastavení nasazeného WAF a odhalit případné zranitelnosti ve výše uvedených aplikacích, které jsou jím chráněny, a zajistit tak jejich bezpečnost v rámci plnění požadavků §25 vyhlášky 82/2018 Sb. V souladu s bezpečnostní strategií a dalšími dokumenty zadavatele. 2. Součástí testů nebude vyhledávání zranitelností v síťové ani jiné infrastruktuře, virtualizačních platformách ani dalším SW vybavení serverů provozujících uvedené aplikace, které s provozem daných aplikací přímo nesouvisí. Před vlastními penetračními testy bude proveden test zranitelnosti nástrojem uvedeným v kapitole 3.4.11. viz předcházející požadavek. 3. Testy budou realizovány dle aktuální verze OWASP Testing Guide (OTG) a v souladu s metodikou OSSTMM a budou primárně zaměřeny na odhalování zranitelností dle platné verze OWASP Top 10. Využito při tom bude automatizovaných nástrojů i manuálního testování.
P.106	Výstupem testů zranitelnosti a penetračních testů musí být: 1. Závěrečná zpráva, která bude obsahovat soupis provedených testů a jejich výsledků, detailní popis odhalených zranitelností, ohodnocení jejich nebezpečnosti včetně konkrétního postupu umožňujícího jejich odstranění. 2. Doporučení řešení odhalených zranitelností – konkrétní postupy umožňující jejich odstranění u oblastí/technologií, které nejsou součástí dodávky. 3. Realizace opatření k odstranění odhalených zranitelností ve formě nastavení a implementace u oblastí, které jsou součástí dodávky.

Tabulka 13: Bezpečnostní audit a penetrační testy

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce

2.1.13 Bezpečnostní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.107	Systém bude chránit osobní údaje pacientů a bude v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob (GDPR) v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
P.108	Vybavení musí plnit podmínky zákona č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
P.109	Autorizace: Poskytnutí přístupu autentizovaného uživatele k aktivu systému (data, aplikace), odpovídající pracovnímu zařazení uživatele a přidělené roli (rolím) v systému. Systém umožní řídit přístupová oprávnění jednotlivých subjektů jen k údajům, ke kterým mají a mohou mít přístup.
P.110	Zabránění vstupu neautorizovaného subjektu do systému – zamezení možnosti přístupu neoprávněného subjektu.
P.111	Zajištění šifrované komunikace mezi všemi součástmi systému a pracovišti uživatelů, případně zajištění komunikace v odděleném síťovém prostředí.
P.112	Evidence přístupů všech uživatelů do systémů a technologií (logování) včetně časových údajů.
P.113	Veškeré přístupy k datům a aktivita uživatelů v rámci dodávaných systémů a technologií budou logovány tak, aby byly zřejmé přístupy k jednotlivým údajům a zpětná kontrola těchto údajů.
P.114	Veškeré logy budou dostupné pro externí Systém analýzy bezpečnostních logů (SW).

Tabulka 14: Bezpečnostní požadavky

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce

2.1.14 Implementační a provozní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.115	Všechny komponenty musí být připraven na provoz 24x7x365 (non-stop).
P.116	Počet uživatelů informačních systémů se nezmění.
P.117	Předmětem zakázky jsou i veškeré služby související s dodávkou – doprava, instalace, implementace do stávající infrastruktury, konfigurace a zprovoznění komunikace, nastavení datových toků, seznámení s obsluhou a správou systému, testování, bezplatné preventivní prohlídky v rámci poskytování servisních služeb. Veškeré seznámení s obsluhou bude probíhat v prostorách objednatele a v českém jazyce. Součástí nabídkové ceny musí být i veškeré práce či činnosti, které v této zadávací dokumentaci nejsou explicitně uvedeny, ale které musí dodavatel s ohledem na jím nabízený předmět veřejné zakázky a jeho řádnou a úplnou realizaci provést k dosažení objednatelem požadovaného cílového stavu.
P.118	Instalace do prostředí objednatele uvedeného v kap. 6.4 – Stav ostatních informačních a komunikačních technologií a kap. 6.2 – Informační a komunikační systémy k zabezpečení (číslování dle ZD).
P.119	V rámci implementace musí dodavatel zajistit plnohodnotný provoz dodávaného řešení současně s provozem stávajících systémů a technologií. To vše s minimálním omezením provozu. Dodavatel je povinen přizpůsobit realizaci předmětu zakázky podmínkám objednatele.

#	Požadavek
P.120	Dodávka OS na servery, včetně instalace do prostředí objednatele, vč. Potřebných licencí, pokud se jedná o licencovaný OS.
P.121	Všechny dodávané nebo upravované součástí systémů (OS, DB, IS, klientské aplikace) musí logovat svou činnost do logů s možností nastavit úroveň logování pro potřeby diagnostiky.
P.122	Zálohování – dodávaný systém (virtualizace, OS) a DB musí být schopny a připraveny na zálohování systémem objednatele, tj. pro virtualizaci, OS a DB musí existovat agenti umožňující zálohování ze strany objednatele. Informace k zálohovacímu systému objednatele jsou uvedeny v kapitole 6.4.1 – Datové centrum, HW infrastruktura, systémový SW (čílováno dle ZD).
P.123	Zajištění administrátorských aplikací, konzolí pro všechny součástí systému (OS, DB, IS, …) pro zajištění konfiguračního managementu systému anebo jeho součástí.
P.124	Dohled – dodávané systémy a technologie musí předávat informace o svém stavu na žádosti SNMP GET. Zhotovitel poskytne parametry, podmínky a součinnost při nastavení dohledu dodaného řešení.
P.125	Architektura řešení celého systému musí korespondovat s požadavky na jeho dostupnost, uvedenými v servisní smlouvě.
P.126	Synchronizace času všech zařízení s time serverem nebo zprostředkovaně přes centrální systém.

Tabulka 15: Provozní požadavky

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce

2.2 POŽADAVKY NA SLUŽBY

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v této kapitole a všech podkapitolách.

2.2.1 Realizace předmětu plnění

Součástí předmětu plnění je zajištění služeb souvisejících s realizací předmětu plnění minimálně v následujícím rozsahu:

1) Objednatel požaduje před zahájením implementačních prací zpracování **Implementační analýzy včetně návrhu řešení** (konkretizace implementačního postupu, přesné konfigurace a instalačního a montážního návrhu řešení z nabídky), která bude zahrnovat informace pro všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění. Implementační analýza včetně návrhu řešení musí být před zahájením prací schválena objednatelem. Implementační analýza včetně návrhu řešení musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu a musí obsahovat minimálně tyto části:
   a) Implementační analýza – zjištění týkající se prostředí objednatele, bude obsahovat alespoň následující:
      i) Seznam technologií, které mají vliv/dopad na dodávku
      ii) Identifikace zdrojů dat využitých pro dodávku
      iii) Evaluace bezpečnosti systému a rizikových faktorů
      iv) Implementační upřesnění specifikace požadavků
      v) Výstupy z analýzy okolí – sběr a analýza informací vztahujících se k dodávce (např. součinnosti apod.)
   b) Detailní popis cílového stavu (instalační a montážní upřesnění návrhu řešení z nabídky)

Popis bude obsahovat alespoň:

i) Rozpracování návrhu řešení z nabídky zhotovitele z pohledu instalací a montáže dle informací z implementační analýzy

ii) Upřesnění rozhraní pro integraci na IS a technologie třetích stran (v případě nutnosti)

iii) Způsob zajištění projektového řízení na straně zhotovitele pro realizaci předmětu plnění (harmonogram, projektový tým, koordinační mechanismy apod.)

iv) Detailní návrh a popis postupu implementace, instalace a montáže předmětu plnění

v) Detailní popis zajištění bezpečnosti systému a informací

Detailní harmonogram projektu včetně uvedení kritických milníků. Kritické milníky jsou termíny dosažení určitých fází projektu, které jsou pro naplnění cílů projektu klíčové. Kritické milníky budou obsahovat minimálně aktivity vedené v kapitole 3 – Harmonogram, s uvedením konkrétních termínů, zhotovitel vhodným způsobem může rozšířit kritické milníky o další aktivity, které mohou být pro projekt klíčové.

vi) Detailní popis navrhovaného seznámení s funkcionalitami, obsluhou dodávaných technologií a budoucím provozem.

Uchazeč zpracuje Implementační analýzu včetně návrhu řešení (dále jen Analýza) dle požadavků uvedených v této kapitole a na základě dlouholetých zkušeností s navrhováním, vývojem a implementací informačních systémů a technologií obdobného rázu jako předmět plnění této veřejné zakázky.

Akceptace Analýzy ze strany Zadavatele je základním podmínkou pro započetí implementačních prací ze strany Uchazeče.

2) **Zajištění projektového vedení/řízení** realizace předmětu plnění ze strany zhotovitele a jeho případných subdodavatelů.

Popis řešení:

Jelikož Uchazeč disponuje týmem vysoce kvalifikovaných projektových manažerů a pracovníků na úrovni vedených řešitelských týmů s dlouholetými zkušenostmi s realizací obdobných projektů v podobném rozsahu jako předmět plnění této veřejné zakázky, garantuje uchazeč zajistit projektové vedení realizace předmětu plnění dle standardních metodik projektového řízení a v souladu s požadavky výzvy č. 10 IROP.

3) **Vývoj, implementace a nastavení** informačních a komunikačních technologií odpovídající schválenému návrhu řešení uvedenému v Implementační analýze a příprava pro ověření ze strany objednatele, alespoň v následujícím rozsahu:

a) Vývoj na straně zhotovitele – vývoj jednotlivých systémů, úpravy existujících produktů, jejich parametrizace a nastavení, vývoj a ověřování integračních rozhraní, součinnost se třetími stranami v souvisejících oblastech.

b) Instalace a implementace do prostředí objednatele v testovacím režimu.

c) Interní ověření na straně zhotovitele a příprava podkladů pro ověření na straně objednatele (dokumentace, organizace testování a další).

d) Příprava a naplnění základních dat – z integračních úloh, číselníky, uživatelé a další.

Provedením těchto činností bude zajištěna připravenost pro ověření ze strany objednatele.

Uchazeč zajistí splnění požadavků uvedených v této kapitole a to na základě dlouholetých zkušeností s vývojem, implementací a nasazováním obdobných informačních systémů a technologií a v souladu se standardy metodik vývoje IS a projektového řízení.

4) **Dodávka předmětu plnění**. Součástí dodávky musí být instalace, upgrade a sestavení předmětu zakázky včetně:

a) Instalace, upgrade a zahoření HW na místě,
b) Instalace a nastavení HW a SW budou provedeny kvalifikovanými osobami pro dané typy zařízení
c) Nastavení HW a aplikací

Popis řešení:

Uchazeč zajistí splnění požadavků uvedených v této kapitole a to na základě dlouholetých zkušeností s vývojem, implementací a nasazováním obdobných informačních systémů a technologií včetně zajištění služeb instalace, nastavení virtuálních strojů a migrace dat a aplikací.

5) **Zajištění instalace všech součástí dodávky** v určených lokalitách a prostorách objednatele.

Popis řešení:

Uchazeč zajistí splnění požadavků uvedených v této kapitole a to na základě dlouholetých zkušeností s nasazováním obdobných zařízení a technologií včetně připojení technickým prostředkům zajištěných Zadavatelem.

6) **Zajištění instalace a připojení** k zařízením a technickým prostředkům zajištěným objednatelem.

Popis řešení:

Uchazeč zajistí splnění požadavků uvedených v této kapitole a to na základě dlouholetých zkušeností s nasazováním obdobných zařízení a technologií včetně připojení technickým prostředkům zajištěných Zadavatelem.

7) **Realizace pilotního provozu** k ověření funkčnosti systému na menším obejmu dat, s menším počtem uživatelů a na menším počtu zařízení.

Popis řešení:

Uchazeč zajistí splnění požadavků uvedených v této kapitole a to na základě dlouholetých zkušeností s vývojem, implementací nasazováním obdobných informačních systémů a technologií a v souladu se standardy metodik vývoje IS a projektového řízení.

8) **Převedení systémů do zkušebního provozu** a plná podpora uživatelů v rámci zkušebního provozu včetně technické podpory. V této etapě budou realizována požadovaná seznámení s funkcionalitami, obsluhou dodávaného zařízení a budoucím provozem.

Popis řešení:

Uchazeč zajistí splnění požadavků uvedených v této kapitole a to na základě dlouholetých zkušeností s vývojem, implementací nasazováním obdobných informačních systémů a technologií a v souladu se standardy metodik vývoje IS a projektového řízení

9) **Zpracování dokumentace skutečného provedení, systémové a provozní dokumentace** – součástí předmětu plnění je zajištění systémové a provozní dokumentace související s realizací předmětu plnění minimálně v následujícím rozsahu:

Název	Popis
Uživatelská dokumentace	Bude popisovat konkrétní funkčnost z pohledu uživatele tak, aby byl uživatel schopen práce s informačním systémem a pochopil význam jednotlivých částí systému a vazeb mezi nimi. V uživatelské příručce bude popisován způsob práce s jednotlivými částmi systému, vazby mezi nimi včetně popisu součástí jednotlivých částí systému. K usnadnění práce bude sloužit popis jednotlivých obrazovek, ovládacích prvků na

Název	Popis
	obrazovkách a jejich významů, který bude uveden v rámci uživatelské dokumentace.
Dokumentace skutečného provedení a systémová/provozní dokumentace	Obsahuje popis informačního systému (rozhraní a služby) včetně popisu správy informačního systému, definování uživatelů, jejich oprávnění a povinností a detailní popis údržby systému.
Bezpečnostní dokumentace	Účelem bezpečnostní dokumentace je definovat závazná pravidla pro zajištění informační bezpečnosti včetně stanovení bezpečnostních opatření. Součástí této dokumentace bude uveden seznam, který bude obsahovat seznam všech externích zdrojů, ke kterým se jednotlivé servery (součásti systému) připojují, včetně uvedení síťových protokolů, pomocí kterých se s daným externím zdrojem komunikuje. V případě, že na servery (součásti systému) existuje vzdálený přístup, musí být tento přístup jasně specifikován (vzdálené zařízení, síťový protokol) a popsán zdůvodnění takovéhoto přístupu (dohled, správa DB atd.)
Disaster & Recovery Plan	Plán řešení situací v případě výpadků a obnovy funkčnosti systému. Součástí je plán a způsob provádění zálohy a případného způsobu obnovy a obnovy funkčnosti i v případě jiných technických výpadků. Dokument bude vytvářen v součinnosti s objednatelem.
Projektová dokumentace	Smluvní dokumentace, harmonogram realizace projektu, analýzy a prováděcí projekty, zápisy z jednání, protokoly (předávací, akceptační)

Tabulka 16: Dokumentace – požadavky na zpracování

Dokumentace bude dodána v relevantním rozsahu na všechna místa plnění projektu.

Dokumentace bude v souladu se zákonem č. 365/2000 Sb. O informačních systémech veřejné správy a prováděcích právních předpisů, v platném znění.

Dokumenty budou zpracovávány v následujících programech elektronicky a uloženy v následujících formátech:

- MS Office 2010 (MS Word 2010, MS Excel 2010, MS PowerPoint 2010)
- MS Project 2010
- WinZip (formát .zip)
- Portable Document Format (formát .pdf).

Preferovaná forma předávaných dokumentů, které nebudou vyžadovat podpisy konkrétních osob je elektronicky, a to na elektronických nosičích (CD, DVD, flash disk, atp.). K předávání a k archivaci souborů se používají média s možností pouze zápisu, nikoliv přepisovatelná.

Veškerá dokumentace bude podléhat schvalování (akceptaci) při převzetí ze strany objednatele.

Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána ve 2x kopiích v elektronické formě ve standartních formátech (MS Office a PDF) používaných objednatelem na datovém nosiči a 1x kopii v papírové formě.

Popis řešení:

Uchazeč zajistí splnění požadavků na zpracování dokumentace uvedených v této kapitole a to na základě dlouholetých zkušeností s vývojem, implementací nasazováním obdobných

informačních systémů a technologií a v souladu se standardy metodik vývoje IS a projektového řízení.

Dokumentace bude vždy zpracovávána v úzké součinnosti Zadavatele a bude podléhat jeho akceptaci/schválení.

10) **Provedení akceptačních testů.** Zhotovitel je povinen kompletně připravit podklady pro akceptaci dodaného řešení. Součástí akceptace bude akceptační protokol a kompletní předávací dokumentace.
11) **Uvedení systému do produkčního provozu**, zajištění potřebných nastavení a přístupů pro všechny pracovníky objednatele, minimalizace dopadů na provoz objednatele při přechodu a zvýšená podpora bezprostředně po přechodu do produkčního provozu.

    Popis řešení:

    Uchazeč připraví podklady pro akceptační testování (akceptačních testy, evidence provedených testů).

    Zároveň uchazeč připraví akceptační protokoly včetně kompletní předávací dokumentace. Vlastní průběh akceptačních testů bude Uchazečem a Zadavatelem domluven a vzájemně odsouhlasen před provedením akceptačních testů.

    Na základě výsledků akceptačního testování bude předmět plnění předán Zadavateli (=Zadavatelem akceptován).

12) Zhotovitel dle svého uvážení doplní v nabídce další služby, které jsou dle jeho názoru nezbytné pro úspěšnou realizaci zakázky.

    Popis řešení:

    Uchazeč v rámci plnění předmětu této veřejné zakázky zajistí dodání odborných analytických a konzultačních služeb nezbytných pro plnění zakázky.

13) Veškeré náklady na zajištění služeb souvisejících s realizací předmětu plnění musí být zahrnuty v ceně odpovídající části předmětu dodávky.

    Popis řešení:

    Uchazeč garantuje, že veškeré náklady na zajištění služeb souvisejících s realizací předmětu plnění jsou zahrnuty v ceně odpovídající části předmětu díla.

2.2.2 Seznámení s funkcionalitami, obsluhou dodávaných technologií

V této kapitole jsou uvedeny požadavky na seznámení s funkcionalitami, obsluhou dodávaných technologií a jejich budoucím provozem:

1) Zhotovitel proškolí pracovníky objednatele se všemi typy dodaných zařízení a aplikací a problematikou jejich užití, provozu a obsluhy. Zhotovitel se zavazuje poskytnout informace minimálně k následujícím tématům v dostatečném detailu pro porozumění činnosti zařízení a způsobu provozu:
    a) Základní produktové seznámení s jednotlivými dílčími technologickými celky.
    b) Celkové schéma součinnosti jednotlivých zařízení a jejich návaznosti.
    c) Obsluha jednotlivých dílčích modulů, aplikací a technologických celků
    d) Použitá nastavení zařízení, detailnější rozbor použitých konfigurací.
    e) Základní kroky správy, diagnostiky a elementární postupy pro řešení problémů.

2) Poskytnuté informace zajistí seznámení pracovníků objednatele se všemi podstatnými částmi dodávky v rozsahu potřebném pro obsluhu, provoz, údržbu a identifikaci nestandartních stavů systému a jejich příčin.
3) Vše uvedené bude probíhat v prostorách objednatele s využitím vybavení dodaného v rámci této veřejné zakázky, případně zajištěné ze strany objednatele.
4) Konkrétní termíny určí objednatel dle postupu v rámci realizace projektu a dostupnosti zainteresovaných osob.
5) Seznámení s funkcionalitami, obsluhou dodávaných technologií se týká klíčových uživatelů, ostatní uživatelé budou proškoleni klíčovými uživateli.

Veškeré náklady na zajištění těchto činností musí být zahrnuty v ceně odpovídající části předmětu dodávky.

2.3 ZÁRUKY

Popis řešení:

Nabízené řešení splňuje veškeré požadavky na záruky uvedené v této kapitole.

V této kapitole jsou uvedeny požadavky na záruky dodávky jako celku, případně specificky dílčích částí dodávky.

Objednatel požaduje záruku na veškeré dodané technologie včetně nezbytných provozních a servisních služeb v délce trvání minimálně:

a) 60 měsíců na informační systém(y), aplikace a služby spojené s realizací projektu,
b) 36 měsíců – u HW infrastruktury a systémového SW, pokud není u konkrétního vybavení uvedeno jinak. Delší záruka je uvedena jen u částí, kde je na trhu běžné poskytování delší záruky v pořizovací ceně.
c) 12 měsíců na spotřební materiál, případně drobné vybavení podléhající rychlému opotřebení. Případný spotřební materiál musí být explicitně označen v nabídce a smlouvě a musí být prokázáno, že splňuje tento charakter.

Záruka začíná běžet od okamžiku předání do ostrého (produkčního) provozu. Veškeré opravy po dobu záruky budou bez dalších nákladů pro provozovatele (objednatele). Veškeré komponenty, náhradní díly a práce budou poskytnuty bezplatně v rámci záruky. Zhotovitel ve své nabídce výslovně uvede všechny podmínky záruk.

a) Po dobu záruky na části dodávky musí zhotovitel nebo výrobce všech zařízení garantovat běžnou dostupnost náhradních komponentů a dostupnost servisu.
b) Součástí záruky je i shoda dodávaných systémů s platnou legislativou.
c) Max. doba na odstranění vady díla je 30 dnů od prokazatelného oznámení dodavateli.
d) Zhotovitel uvede provozní služby požadovaného předmětu plnění veřejné zakázky včetně parametrů, které budou předmětem dodávek v rámci záruky systému a v rámci poskytování servisních služeb.

Poskytovatel zajistí HelpDesk pro hlášení vad.

Popis řešení:

Zhotovitel akceptuje všechny požadavky Objednatele, co se týče podmínek záruky, reklamačního řízení a odstraňování vad. V následujícím textu Zhotovitel uvádí doplňující informace pro záruky v rámci ZD.

Zhotovitel poskytne záruku na veškeré dodané technologie včetně nezbytných provozních a servisních služeb v délce uvedené v bodě a)-c) úvodní části této kapitoly (není-li u konkrétní technologie uvedeno jinak – toto je uvedeno u konkrétních částí předmětu nabídky) od okamžiku předání do provozu.

Podmínky záruky jsou následující:

- *Bude poskytován bezplatný záruční servis na objednatelem reklamované vady předmětu díla vzniklé v době trvání záruční doby.*
- *Záruka se vztahuje jen a pouze na technologie a poskytnuté služby, které jsou předmětem dodávky Zhotovitele, případně na části, které Zhotovitel autorizoval. Zhotovitel tedy neručí za vady hmotných i nehmotných komponent, které nedodával a za vady díla, které byly vyvolány vadou těchto komponent.*
- *Záruka končí uplynutím záruční doby bez nutnosti jejího formálního ukončování.*
- *Záruční opravy budou při splnění záručních podmínek pro Objednatele zdarma tj. veškeré komponenty, náhradní díly a práce budou poskytnuty bezplatně.*
- *Reakční doba a doba odstranění vad díla v rámci záruky je uvedena ve Smlouvě o dílo.*
- *Záruka se nevztahuje na případy, kdy není zajištěna nezbytná součinnost, která povede k rozdílům v rozhraních, funkčnosti celků třetích stran, změny technologií nebo nejsou dodrženy podmínky provozu a využívání dodaných celků.*
- *Záruka se nevztahuje na vady, které byly způsobeny vnějšími okolnostmi nebo zařízeními a systémy, která nebyla dodána podle této smlouvy a nezpůsobil je zhotovitel nebo osoby, s jejichž pomocí zhotovitel plnění prováděl*
- *Záruka se nevztahuje na vady vzniklé v důsledku:*
  - *použití zařízení pro účely, pro něž není určeno; užívání v rozporu s předanou dokumentací*
  - *chybného provádění obsluhy;*
  - *živelních pohrom*
  - *přemístění zařízení bez souhlasu zhotovitele;*
  - *připojení jiných nebo dalších zařízení nebo systémů než předpokládá smlouva;*
  - *vady kvality elektrické energie, nebo pokud podmínky prostředí neodpovídají specifikacím dle technologického projektu;*
  - *vady elektrické instalace jakož i datových a sdělovacích rozvodů;*
  - *neoprávněně provedených změn, opravárenských prací nebo zásahů do programového vybavení ze strany objednatele nebo třetí osoby;*
  - *kolizí vyvolaných stavem počítačové sítě ZZS;*
  - *kolizí aplikačního programového vybavení systému se softwarovými produkty objednatele, resp. konečného uživatele, nainstalované do systému po předání díla objednateli;*
  - *zavirování systému v důsledku používání neověřených aplikací a přenosných médií uživatelem;*
  - *vad způsobených vadami technologií a služeb třetích stran či částmi zajišťovanými Objednatelem v rámci součinnosti*
- *Zhotovitel neručí za nové pořízení dat, pokud jejich ztrátu nezavinil, dále v případě, že objednatel nezajistil, aby bylo data možno opět pořídit z materiálů ve strojově čitelné podobě bez dodatečných nákladů*

Popis služby Helpdesk

1. *Služba bude poskytována nepřetržitě v režimu 24h x 7 dní.*

2. *Veškeré servisní požadavky budou hlášeny a spravovány výhradně přes YOUR SYSTEM Helpdesk pomocí smluvně dohodnutých komunikačních kanálu.*
3. *Pouze požadavky nahlášené pomocí YS Helpdesk jsou považovány za platné prokazatelně nahlášené.*
4. *Pouze požadavky, jejichž řešení jsou zaznamenány v YS Helpdesk jsou považovány za platné prokazatelně vyřešené.*
5. *Poskytovatel se zavazuje, že bude vždy dostupný minimálně jeden ze smluvních komunikačních kanálů.*
6. *Je-li jedním z komunikačních kanálů webové rozhraní YS Helpdesk, zavazuje se poskytovatel ke zřízení přístupových údajů nejpozději v den zahájení poskytování služby.*
7. *Servisní požadavky jsou hlášeny výhradně smluvně dohodnutými oprávněnými osobami Objednatele.*
8. *V rámci hlášení servisního požadavku bez ohledu na jeho charakter budou poskytovatelem vždy požadovány a odběratelem vždy poskytnuty základní identifikátory pro co nejrychlejší a nejefektivnější řešení:*
    - *Příjmení a jméno oprávněné osoby*
    - *Telefonické spojení na oprávněnou osobu*
    - *E-mailová adresa na oprávněnou osobu*
    - *Kontaktní údaje na další zainteresované osoby*
    - *Datum a hodina vzniku závady (jedná-li se o závadu)*
    - *Druh technologie nebo typ zařízení, kterého se požadavek týká*
    - *Lokalita*
    - *Přesný popis požadavku nebo závady*
9. *V rámci servisních požadavků může být vyžadována neomezená telefonická asistence v režimu 24x7. V rámci této asistence mohou být závady řešeny ihned, případně je domluvena závazná doba pro zpětné volání od vzniku požadavku. YS Helpdesk zajistí telefonickou asistenci s konkrétním pracovníkem pro danou technologii či typ zařízení.*
10. *Správa platného požadavku:*
    - *Registraci požadavku interním informačním systému (apl. YS Helpdesk) provádí:*
        - *Oprávněná osoba pomocí webového rozhraní aplikace*
            - *Helpdesk provede vyhodnocení relevantnosti požadavku, následně provede jeho klasifikaci a kategorizaci*
            - *V případě chybějících údajů, neprodleně kontaktuje oprávněnou osobu, která požadavek zaregistrovala, pro jejich doplnění*
        - *Operátor YS Helpdesk*
            - *YS Helpdesk zajistí získaní všech potřebných a dostupných údajů pro co nejrychlejší a nejefektivnější řešení*
            - *Helpdesk provede vyhodnocení relevantnosti požadavku, následně provede jeho klasifikaci a kategorizaci a požadavek zaregistruje*
    - *Po zaregistrování platného požadavku je oprávněné osobě, případně dalším zainteresovaným osobám, automaticky vygenerována e-mailová notifikace s potvrzením přijetí požadavku*
    - *Helpdesk předá požadavek kompetentnímu pracovníkovi technické podpory*

- *Po přidělení je pracovníkovi TP vygenerována automatická e-mailová notifikace o přiděleném případu k řešení. V případě požadavků/závad s vysokou prioritou jsou tyto potvrzeny pracovníkovi technické podpory zároveň telefonicky*
- *Helpdesk průběžně monitoruje stav řešení a na vyžádání o něm informuje oprávněné osoby*
- *Helpdesk hierarchicky nebo funkčně eskaluje požadavky, které nejsou řešeny v dohodnutých termínech nebo kde se blíží konec dohodnutého termínu*
- *Je-li požadavek ze strany oprávněné osoby, která požadavek nahlásila, urgován nebo doplněn o nové skutečnosti, Helpdesk provede aktualizaci požadavku, o čemž je oprávněná osoba, další zainteresované osoby a příslušný pracovník TP informován formou e-mailové notifikace.*
  Aktualizace, urgence, případně storno požadavku je možné provést pomocí veškerých smluvních komunikačních kanálů.
- *Po vyřešení požadavku Helpdesk informuje osobu, která požadavek nahlásila, o jeho vyřešení.*
  - *Telefonicky*
    - *Po ověření a odsouhlasení řešení je případ uzavřen a automaticky vygenerována e-mailová notifikace o uzavření požadavku*
    - *Při neakceptování je požadavek vrácen zpět k řešení kompetentnímu pracovníkovi TP*
  - *Automaticky generovanou e-mailovou notifikací o vyřešení požadavku*
    - *Při akceptování řešení (libovolným smluvním komunikačním kanálem) Helpdesk požadavek uzavře.*
    - *Při neakceptování řešení (libovolným smluvním komunikačním kanálem) je požadavek vrácen zpět k řešení kompetentnímu pracovníkovi TP*
    - *Neobdrží-li Helpdesk do 5 pracovních dnů reakci na vyřešení požadavku, je řešení požadavku automaticky považováno za odsouhlasené a je požadavek je uzavřen.*
    - *Při uzavření požadavku je automaticky vygenerována e-mailová notifikace o uzavření požadavku*

Komunikační kanály

- *Placená telefonní linka 277 775 555*
- *Placená faxová linka 277 775 501*
- *Záložní mobilní spojení 737 203 233*
- *Elektronická pošta helpdesk@ys.cz*
- *Webové rozhraní https://yourdesk.ys.cz*

3 HARMONOGRAM

Následující tabulka obsahuje požadovaný časový harmonogram realizace dodávky (T ~ datum účinnosti smlouvy o dílo):

#	Fáze	Doba trvání od zahájení	Doplňující informace
1	Zahájení realizace	0	Zahájení realizace bude dnem podpisu smlouvy na dodávku.
2	Analýza a návrh řešení	45	Zpracování analýzy a návrhu řešení pro potřeby upřesnění podmínek realizace.
3	Dodávka, implementace, instalace, konfigurace HW a SW infrastruktury.	140	Dodávka a implementace HW, SW a síťové infrastruktury.
4	Vývoj a implementace úprav SW, dodávka dokumentace k SW.	140	Vlastní vývoj a implementace úprav IS dle analýzy a návrhu řešení.
5	Ověření funkčnosti dodaných technologií a systémů.	150	Otestování funkčnosti technologií a systémů a ověření jejich plné funkčnosti.
6	Seznámení s funkcionalitami, obsluhou dodávaných technologií	150	Seznámení s funkcionalitami, obsluhou dodávaných technologií
7	Dodávka dokumentace dodaného systému a jeho částí.	150	Min. uživatelská dokumentace, dokumentace skutečného provedení, systémová dokumentace, projektová dokumentace.
8	Převedení do zkušebního provozu.	150	Převedení do zkušebního provozu, odstranění všech vad a nedodělků, dokončení realizace a převedení do ostrého provozu.
9	Bezpečnostní audit a penetrační testy	180	Zpracování a předání bezpečnostního auditu a penetračních testů. *Pozn.: zpracování bezpečnostního auditu bude zahájeno při zahájení realizace. Jedná se o termín předání a akceptace výstupů.*
10	Ukončení realizace dodávky.	180	Součástí je zahájení doby provozu dodaného systému a poskytování servisních služeb.

Tabulka 17: Harmonogram

Doplňující informace:

- Pod pojmem „den“ je míněn kalendářní den.
- Zhotovitel má možnost definovat kratší termíny plnění (v rámci dodávky), nelze zkrátit dobu zkušebního provozu, která musí být min. 30 dnů.
- Zkrácení zkušební doby je možné pouze na základě písemné dohody se Zadavatelem v rámci dodávky.

4 MÍSTA PLNĚNÍ

Realizace předmětu plnění bude probíhat v následujících místech plnění:

Místo	Adresa	Předmět realizace
Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace	Kamenice 798/1d, Brno PSČ: 625 00	Primární datové centrum ZZS JMK – dodávky v návaznosti na technologie umístěné v tomto DC a dodávka částí technologie. Primární lokalita, kde je provozován IS ZOS a kde je primární ZOS. Současně se jedná o primární lokalitu IS elektronická pošta. Sídlo ZZS JMK – místo předání výstupů projektu.
Záložní zdravotnické operační středisko ZZS JMK a záložní datové centrum	HZS Lidická 61 602 00 Brno	Záložní zdravotnické operační středisko ZZS JMK (ZZOS) a záložní datové centrum pro toto ZZOS, kde bude umístěna dodaná technologie ZZOS a které bude propojeno s primárním datovým centrem ZZS JMK.

Tabulka 18: Místa plnění

5 POŽADAVKY NA SOUČINNOST

Požadavky na součinnost

Předpokladem úspěšné realizace je zajištění těchto základních součinností:

#	Požadovaná součinnost	Poznámky
1	Zajištění souhlasu majitele nemovitosti (pokud je třeba) s instalací technologií	Nelze efektivně realizovat projekt ZZS JMK KB.
2	Zajistit delegování bezpečnostního garanta ZZS JMK - zajištění kontaktní osoby na straně Objednatele. Zajištění součinnosti majitelů majitelů a provozovatelů aktiv a to včetně externích subjektů. Aktivní účast na workshopech majitelů a provozovatelů aktiv a to včetně externích subjektů dle dohodnutého harmonogramu.	Nesoulad implementace s bezpečnostními požadavky ZZS. Nemožnost dodat část projektu (Bezpečnostní audit, Penetrační testy, GAP analýza…)
3	Poskytnutí vstupů pro technické hodnocení a Zajištění všech požadovaných vstupních informací v úvodních týdnech od zahájení GAP analýzy.	Nemožnost dodat část projektu (Bezpečnostní audit, Penetrační testy,…)
4	Dodání dokumentace o kompletní ISMS dokumentaci o kompletní dokumentaci k ZKB o technickou a provozní dokumentaci k síťovým prvkům, serverům, aplikacím apod.	Nemožnost dodat část projektu (Bezpečnostní audit, Penetrační testy, GAP Analýza…)
5	Delegování administrátorů – zajistit delegování IT pracovníků zodpovědných za správu HW a síťové infrastruktury nutné pro běh systému. Zajištění odpovědné osoby, která bude technicky schopná spolupracovat při implementaci řešení a začlenění do stávající infrastruktury Zajištění pracovníka, který bude spolupracovat na instalaci HW a SW pro zajištění výsledku projektu	Nezajištěná administrace systémů, problematická instalace a testování dodávky HW a systémového SW.
6	Přístup do prostředí ZZS JMK - zřízení přístupů pro konzultanty Zhotovitele do budov, sítě, případně systémů Objednatele/Zadavatele. jištění pracovníka	Nelze efektivně realizovat projekt ZZS JMK KB. Součinnost po celou dobu realizace.

#	Požadovaná součinnost	Poznámky
	pro přístup do jednotlivých prostor pro instalaci služby	
7	Delegování a alokace pracovníků Objednatele pro potřeby realizace projektu - jmenování pracovníků Objednatele do projektových struktur na všech úrovních (Řídící výbor, HTP, Pracovní týmy), alokace jejich času a disponibilita pro plnění úkolů na projektu s cílem realizovat projekt v daném rozsahu, čase a kvalitě.	Nemožnost zahájit a realizovat projekt. Při zahájení projektu.
8	Zajištění prostor pro jednání projektových týmů - zajištění prostor pro jednání týmů na všech úrovních projektového řízení. Včetně WC a napájení 230V.	Organizační komplikace, možnost vzniku vícenákladů na projekt. Při zahájení projektu.
9	Zajistit akceptační proceduru na straně Objednatele/Zadavatele pro zajištění akceptace poskytovaných služeb/jednotlivých dílčích plnění převzetí jednotlivých dodávek.	Zpoždění v projektu, nemožnost zahájit případné návazné etapy projektu. Při zahájení projektu.
10	Součinnost při školení – pro zdárný průběh školení poskytnout potřebnou infrastrukturu: zajištění školící místnosti, počítačového vybavení a projektoru po celou dobu školení. Delegovat osobu zodpovědnou za organizaci školení na straně Objednatele/Zadavatele. Delegovat pracovníky na školení a zajistit jejich rozdělení do skupin.	Neproškolení uživatelů, nemožnost používat systém autorizovanými pracovníky. 1 týden před započetím školení.
11	Součinnost v rámci Zkušebního a testovacího provozu – delegovat osoby Objednatele (testery) a zajistit organizaci zkušebního provozu (kdo, kdy bude prověřovat výstupy projektu) / Zkušební, jaká funkcionalita a jak dlouhou dobu bude prověřována)	Riziko na straně Objednatele/Zadavatele – aplikace není ověřena v živém provozu. 1 měsíc před předáním do zkušebního provozu) / V příslušné etapě.
12	Plnění operativních úkolů - realizovat a zabezpečovat operativní úkoly stanovené na jednotlivých úrovních řízení (na základě zápisů z jednání, rozhodnutí Řídícího výboru a vyplývající z ostatní projektové dokumentace). Zajištění reakční doby v souladu s úkoly zadanými v rámci projektových činností	Nedodržení harmonogramu, zpoždění v projektu. V rámci realizace projektu průběžně.
13	Zadavatel zajistí po celou dobu instalace a zprovozňování systému přístup pro pracovníky uchazeče do prostor budování ZZS JMK KB	Organizační problémy při zahájení instalace, ztížené podmínky.

#	Požadovaná součinnost	Poznámky
	(dispečerský sál, technologická místnost a přilehlé prostory) a dále zajistí uzamykatelný prostor za účelem uložení montážního a instalačního materiálu a dočasné šatny pracovníků. Zajištění přístupových cest pro vozidla s dodávkou technologie, volné stěhovací trasy do místa určení, výtah. Zajištění možnosti provádět implementační práce v době od 8:00-18:00.	V rámci realizace projektu průběžně.
14	Zajištění dostatečného prostoru (RACK), napojení na infrastrukturu a zálohovaného napájení pro instalace dodávaných technologií	Nelze efektivně realizovat projekt.
15	Zajištění konfigurací, součinnosti a přístupů k navazujícím technologiím (FireWall, AD apod.)	Nemožnost realizace projektu
16	Pro zrychlení řešení případných problémů uživatelů s klientskou částí systému IS OŘ a pro zvýšení efektivity při poskytování telefonických konzultací navrhujeme umožnit vzdálený přístup pracovníků podpory na plochu koncové stanice operátora; přístup bude umožněn pouze na vyžádání ze strany uživatele. - Vzdálený přístup ke klientským pracovištím a serverům pro IT dodavatele - Zajistit vzdálený přístup pro instalační práce - Zajištění přístupových účtů a oprávnění k provádění záručního servisu - Vzdálený přístup pro realizaci zásahů v rámci záruky	Zpomalení řešení případných problémů se systémem na koncových stanicích operátorů, nemožnost podpořit telefonické konzultace sdílením obrazovky. Před termínem s požadovaným přístupem uživatele.
17	Součinnost stávajícího dodavatele personálního systému ZZS JMK (VEMA) při využití integrace se systémy IS OŘ a EKP/MZD tak, aby mohl dodavatel naplnit požadavek P.76 dle zadávací dokumentace.	Nemožnost realizace části projektu

Tabulka 19: Požadavky na součinnost

Příloha č. 5: Kalkulace nabídkové ceny

Položka ceny	Cena v Kč bez DPH	DPH v Kč	Cena v Kč s DPH
Celková nabídková cena za dodávky dle vzorové Smlouvy o dílo	11 050 000,00 Kč	2 320 500,00 Kč	13 370 500,00 Kč
Celková nabídková cena za servisní služby dle vzorové Servisní smlouvy	2 820 000,00 Kč	592 200,00 Kč	3 412 200,00 Kč
Celková nabídková cena za plnění této VZ (dodávky i servisní služby)	**13 870 000,00 Kč**	**2 912 700,00 Kč**	**16 782 700,00 Kč**

Ozn.	Položka rozpočtu	Počet jednotek	Cena za dodávku (v Kč bez DPH)	Cena za dodávku (v Kč s DPH)	Cena za servisní služby / 1 rok (v Kč bez DPH)	Cena za servisní služby / 4 roky (v Kč bez DPH)	Cena za servisní služby / 4 roky (v Kč s DPH)
1	FireWall s IPS pro ZZOS	1 ks	480 000,00 Kč	580 800,00 Kč			
2	FireWall pro ochranu segmentů ZOS	1 ks	550 000,00 Kč	665 500,00 Kč			
3	L3 switche pro ZZOS	2 ks	220 000,00 Kč	266 200,00 Kč			
4	Aplikační firewall pro IS ZOS	1 ks	795 000,00 Kč	961 950,00 Kč			
5	Systém analýzy bezpečnostních logů (SW)	1 soubor	3 130 000,00 Kč	3 787 300,00 Kč			
6	Infrastruktura (HW) pro systém analýzy bezpečnostních logů (HW)	1 soubor	850 000,00 Kč	1 028 500,00 Kč			
7	Systémový SW pro systém analýzy bezpečnostních logů (SW)	1 soubor	450 000,00 Kč	544 500,00 Kč	705 000,00 Kč	2 820 000,00 Kč	3 412 200,00 Kč
8	Úpravy IS ZOS	1 soubor	3 090 000,00 Kč	3 738 900,00 Kč			
9	Konfigurace systému elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů	1 soubor	50 000,00 Kč	60 500,00 Kč			
10	Dvoufaktorová autentizace administrátorských VPN přístupů	1 soubor	135 000,00 Kč	163 350,00 Kč			
11	Nástroje pro bezpečnostní audit a penetrační testy	1 soubor	400 000,00 Kč	484 000,00 Kč	---	---	---
12	Bezpečnostní audit a penetrační testy	1 soubor	900 000,00 Kč	1 089 000,00 Kč	---	---	---
Celkem			**11 050 000,00 Kč**	**13 370 500,00 Kč**	**705 000,00 Kč**	**2 820 000,00 Kč**	**3 412 200,00 Kč**

Příloha č. 4 Smlouvy o dílo – Servisní smlouva

Servisní smlouva

podle § 2586 a násl. zák. č. 89/2012 Sb., občanského zákoníku, v platném znění (dále jen „občanský zákoník“)

Číslo smlouvy objednatele:

Číslo smlouvy poskytovatele: S-JAKA-000221

Objednatel:	**Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace**
Se sídlem:	Kamenice 798/1d 625 00 Brno
Zastoupený:	MUDr. Hana Albrechtová, ředitelka
IČ:	00346292
DIČ:	CZ 00346292
Bankovní spojení:	……..
Číslo účtu:	……

na straně jedné (dále jen „**Objednatel**“)

a

Poskytovatel:	**YOUR SYSTEM, spol.s r.o.**
Se sídlem:	Türkova 2319/5b, Praha 4, PSČ 149 00
Zastoupený:	RNDr. Martin Nehasil, jednatel
IČ:	00174939
DIČ:	CZ 00174939
Plátce DPH:	ANO
Bankovní spojení:	UniCredit Bank Czech Republic, a.s.
Číslo účtu:	381610004/2700

Zapsaný v OR vedeném Městským soudem v Praze, 18. července 1990, oddíl C, vložka č. 72

na straně druhé (dále jen „**Poskytovatel**“)

1. Předmět smlouvy

1.1. Smluvní strany shodně prohlašují, že mezi sebou uzavřely dne …….. Smlouvu o dílo č. ……., (č. smlouvy zhotovitele S-JAKA-000220) na komplexní dodávku a implementaci technologií, dodávky SW, HW a infrastruktury pro realizaci technických bezpečnostních opatření dle § 5 odst. 3) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů pro zabezpečení IS provozovaných Objednatelem, kterým je Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace. Poskytovatelem

bude Objednateli dodáno dílo v souladu s přílohou č. 4 Smlouvy o dílo (dále jen „Dílo“). Tato smlouva je uzavírána a je přílohou předmětné Smlouvy o dílo.

1.2. Plnění této servisní smlouvy je součástí projektu „Kybernetická bezpečnost Zdravotnické záchranné služby Jihomoravského kraje“ (dále jen „Projekt“), registrační číslo projektu CZ.06.3.05/0.0/0.0/15_011/0006960 (dále jen „Projekt“), který je spolufinancován z výzvy č. 10 Integrovaného regionálního operačního programu (IROP) s názvem „KYBERNETICKÁ BEZPEČNOST“, prioritní osy PO 3: Dobrá správa území a zefektivnění veřejných institucí, specifického cíle SC 3.2: Zvyšování efektivity a transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality systémů IKT.

1.3. Předmětem této servisní smlouvy (dále jen „Smlouva“) je zajištění služeb servisní podpory Poskytovatelem Objednateli (dále jen „Služby“). Podrobný popis Služeb a podmínek jejich poskytování je uveden v Příloze č. 1 této Smlouvy.

1.4. Objednatel se touto Smlouvou zavazuje zaplatit Poskytovateli za Služby poskytnuté jím na základě této Smlouvy a v souladu s jejími podmínkami cenu dle této Smlouvy.

2. Rozsah a místo plnění Smlouvy

2.1. Plnění Poskytovatele dle této Smlouvy se vztahuje pouze k Dílu.

2.2. Místem plnění je Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace, Kamenice 798/1d, 625 00 Brno a Záložní zdravotnické operační středisko ZZS JMK a záložní datové centrum, HZS Lidická 61 602 00 Brno.

3. Cena služeb

3.1. Cena Služeb dle této Smlouvy je stanovena a podrobně rozepsána v Příloze č. 2 této Smlouvy.

3.2. Ceny v Kč bez DPH, uvedené v Příloze č. 2, jsou ceny konečné a obsahují veškeré přímé a nepřímé náklady nezbytné k řádnému provedení požadovaných služeb. K cenám bude připočtena DPH v zákonné výši. Ceny je možné změnit dodatečně v případě, že v průběhu realizace plnění dojde ke změnám daňových nebo jiných legislativních předpisů, které mají vliv na cenu. V důsledku změny sazby DPH není nutno ke Smlouvě uzavírat dodatek.

4. Platební a fakturační podmínky

4.1. Cena za Služby dle této Smlouvy bude účtována čtvrtletně zpětně na základě Výkazu služeb za uplynulé kalendářní čtvrtletí podepsaného oprávněnými osobami dle odst. 7.4 této Smlouvy. Výkaz musí obsahovat všechny povinné služby a jejich čerpání v daném kalendářním čtvrtletí (viz Příloha č. 1).

4.2. Faktury za plnění poskytnuté Poskytovatelem Objednateli na základě této Smlouvy v uplynulém kalendářním čtvrtletí vystavené Poskytovatelem budou Poskytovatelem zasílány na adresu sídla Objednatele nebo elektronicky do podatelny Objednatele (E-mail:info@zzsjmk.cz). V případě, že služby nebyly poskytovány po celé kalendářní čtvrtletí (první a poslední čtvrtletí v návaznosti na datum uzavření a ukončení smlouvy), bude účtována alikvotní část ceny za Služby v daném čtvrtletí.

4.3. Za den uskutečnění zdanitelného plnění se považuje poslední den příslušného kalendářního čtvrtletí. Splatnost faktury se sjednává na 30 kalendářních dnů od data doručení faktury na adresu sídla Objednatele, resp. elektronicky do podatelny Objednatele. Připadne-li doba splatnosti na den pracovního klidu (tzn. na státní svátek nebo ostatní svátek, sobotu či neděli)nebo na den, který není bankovním pracovním dnem, posouvá se doba splatnosti na nejbližší následující pracovní den.

4.4. Došlá faktura musí být vystavena v souladu se zákonem č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění. Dále musí obsahovat ve vztahu k plnění věcně správné údaje a musí na ní být uvedeno číslo této Smlouvy a informace, že se jedná o projekt Integračního regionálního operačního programu a označení registračním číslem projektu uvedeném v úvodním ustanovení této smlouvy.

4.5. V případě, že faktura nebude obsahovat některou ze zákonných nebo v této Smlouvě sjednaných náležitostí, nebo nebude obsahovat věcně správné údaje, má Objednatel právo vrátit ji zpět Poskytovateli k opravě. Oprávněným vrácením faktury se ruší původní lhůta její splatnosti a doručením opravené faktury Objednateli začíná běžet nová lhůta splatnosti.

4.6. K vyrovnání závazku Objednatele dojde odepsáním částky z jeho účtu ve prospěch účtu Poskytovatele.

5. Sankce

5.1. Při nedodržení lhůty pro odstranění závady definované v Příloze č. 1 této Smlouvy je Objednatel oprávněn účtovat Poskytovateli smluvní pokutu ve výši 1 % z měsíční ceny Služeb (cena za zajištění služeb za kalendářní čtvrtletí/3) za každou hodinu prodlení a za každou jednotlivou závadu spadající do kategorie poruch A. U závad kategorie poruch B je Objednatel oprávněn účtovat Poskytovateli smluvní pokutu ve výši 1 % ze čtvrtletní ceny Služeb za každý den prodlení. Nárok na smluvní pokutu bude Objednatel uplatňovat písemně na Výkazu služeb za uplynulé čtvrtletí dle odst. 4.1 této Smlouvy. Objednatel má právo započíst takto vzniklou pohledávku na úhradu ceny Služeb za odpovídající kalendářní čtvrtletí. Maximální celková výše všech smluvních pokut, které může Objednatel nárokovat v jednom kalendářním čtvrtletí, není omezena.

6. Omezení výše nároku na náhradu škody

6.1. Každá ze smluvních stran nese odpovědnost za škody způsobené porušením povinností dle Smlouvy v souladu s platnými právními předpisy, není-li ve Smlouvě stanoveno jinak. Smluvní strany budou vyvíjet maximální úsilí k předcházení škodám a k minimalizaci vzniklých škod.

6.2. Poskytovatel neodpovídá Objednateli za škody vzniklé poskytnutím chybných dat ze strany Objednatele, chybnou obsluhou, neodborným zacházením, či užíváním v rozporu s doporučením Poskytovatele, neoprávněným zákrokem, mechanickým poškozením, pokud tyto skutečnosti nevznikly vinou Poskytovatele.

6.3. Maximální celková výše nároku na náhradu škody, prokazatelně způsobené Poskytovatelem Objednateli v souvislosti s plněním Smlouvy, bude shora omezena částkou 15.000.000 Kč (slovy: dvacet milionů korun českých). Nárok na náhradu škody bude Objednatel uplatňovat u Poskytovatele písemně do 30 dnů od vzniku škodní události. Stanovení rozsahu škod jakož

i posouzení míry zavinění ze strany Poskytovatele náleží ve sporných případech příslušnému soudu.

7. Všeobecné smluvní povinnosti

7.1. Objednatel umožní Poskytovateli přístup k systému a také použití dalšího souvisejícího zařízení systému nebo paměťových medií dočasně nezbytných pro poskytnutí Služeb podle této Smlouvy. Při odstraňování problémů Objednatel poskytne Poskytovateli přiměřenou součinnost s přístupem k relevantním systémům Objednatele.

7.2. Objednatel bude udržovat vzdálené (např. internetové) spojení s hardware a Informačním systémem v souladu s pokyny Poskytovatele a ponese náklady spojené s provozem takového spojení.

7.3. Objednatel je povinen provádět veškerý uživatelský provozní servis systému podle uživatelské dokumentace výrobce nebo podle instrukcí Poskytovatele. Objednatel nebude provádět na systému žádné úpravy anebo opravy, které odporují uživatelské nebo jiné technické dokumentaci výrobce příslušného zařízení.

7.4. Objednatel určí kontaktní osoby z řad svých zaměstnanců, odpovědné za veškeré kontakty s Poskytovatelem ve věci poskytování služeb servisní podpory. Stejná povinnost platí pro Poskytovatele směrem k Objednateli. V případě změny kontaktních osob nebo jejich kontaktních údajů bude tato změna prokazatelně sdělena druhé smluvní straně. Každá ze smluvních stran ze seznamu kontaktních osob určí osobu, případně osoby, které budou oprávněny schválit a podepsat výkaz služeb dle odst. 4.1. této Smlouvy. Seznamy kontaktních osob budou vzájemně předány při podpisu smlouvy a společný seznam bude podepsán oběma smluvními stranami. Změna kontaktních osob bude následně oznamována druhé smluvní straně písemně a bude podepsaná statutárním orgánem oznamující smluvní strany.

7.5. Softwarový produkt bude používán v systému splňujícím minimální hardwarovou sestavu vymezenou v příslušném popisu programového produktu nebo v jiné obdobné technické dokumentaci.

7.6. Objednatel je odpovědný za fyzické uchování záložních kopií veškerého provozovaného systémového software podle pokynů Poskytovatele (provozní dokumentace systému) tak, aby byly přístupné v případě, že budou nutné pro poskytování služeb dle této Smlouvy. Náhradní díly pro záruční i mimozáruční servis včetně montážního a elektroinstalačního materiálu zajišťuje Poskytovatel. Veškeré náklady na opravy v rámci záručního servisu jdou k plné tíži Poskytovatele. Při pozáruční či mimozáruční opravě bude vadná komponenta Poskytovatelem nahrazena funkční součástí a Objednateli budou účtovány náklady na opravu vadné komponenty. Oprava komponenty se provádí pouze na základě pokynu Objednatele dle posouzení rentability opravy. Pokud takováto oprava není možná nebo bude nerentabilní, bude komponenta nahrazena Poskytovatelem jinou funkční komponentou. Záruční doba na opravenou nebo novou komponentu v záruce bude mít stejné datum ukončení záruky jako původní komponenta. Záruční doba na komponentu i jinou funkční součást mimo záruku je vždy 6 měsíců. Kategorie opravy

(záruční/pozáruční/mimozáruční) nemá vliv na lhůty pro odstranění závady podle Přílohy č. 1 této Smlouvy.

7.7. Vyhodnocení, zda se jedná o záruční, pozáruční nebo mimozáruční servis (vč. neoprávněných reklamací), bude provádět Poskytovatel zpětně po provedení servisního zásahu a odstranění nahlášené závady. Neoprávněné reklamace, stejně jako případné posouzení opravitelnosti vadné komponenty mimo záruku či po záruce, kdy je nutno provést detailní diagnostiku a/nebo odeslat vadnou komponentu na posouzení výrobci, může být účtováno jako služba nad rámec Smlouvy dle ceníku v Příloze č. 2. V případech mimozáručních servisů (násilné poškození, případně používání zařízení prokazatelně v rozporu s jeho určením či pokyny výrobce/dodavatele) může kromě ceny opravy Poskytovatel účtovat Objednateli prokazatelné náklady spojené s demontáží vadné komponenty a se zpětnou montáží nové nebo opravené komponenty.

7.8. Poskytovatel může po dohodě s Objednatelem vyřešit opravu poskytnutím jiné, typově a funkční ekvivalentní komponenty.

7.9. Poskytovatel prohlašuje, že má uzavřenou platnou smlouvu na pojištění odpovědnosti za škodu způsobenou třetí osobě ve výši minimálně 15.000.000,- Kč a že tuto smlouvu o pojištění bude udržovat v platnosti po celou dobu plnění této smlouvy.

8. Platné právo

8.1. Vztahy mezi smluvními stranami, které nebudou touto Smlouvou upraveny, se budou řídit příslušnými ustanoveními českých obecně závazných právních předpisů, zejména pak příslušnými ustanovení občanského zákoníku. Při rozhodování případných sporů, vzniklých ze závazkových vztahů založených na této Smlouvě, platí soudní příslušnost dle zákona č. 99/1963 Sb., občanského soudního řádu, ve znění pozdějších předpisů.

9. Trvání Smlouvy

9.1. Tato Smlouva se uzavírá na dobu neurčitou.

9.2. Smlouva může být ukončena:
- odstoupením od Smlouvy dle čl. 10. Smlouvy
- na základě písemné dohody obou smluvních stran.

9.3. Smlouva může být rovněž ukončena písemnou výpovědí učiněnou kteroukoliv ze smluvních stran i bez udání důvodů. Výpovědní lhůta činí 90 dnů a počíná běžet prvním dnem měsíce následujícího po doručení výpovědi druhé smluvní straně. Poskytovatel tak může učinit nejdříve po uplynutí 5 let ode dne účinnosti této smlouvy.

10. Odstoupení od Smlouvy

10.1. Za podstatné porušení Smlouvy, při kterém dotčená smluvní strana bude oprávněna od Smlouvy s okamžitou účinností odstoupit, budou chápat smluvní strany:

10.1.1. Prokazatelnou neschopnost Poskytovatele plnit své závazky (ztráta kvalifikace, vyhlášení úpadku společnosti apod.). Za takovou neschopnost bude považován stav, kdy nedodržení sjednané lhůty pro odstranění závady při řešení jednotlivých zásahů přesáhne20% závad nahlášených v rámci jednoho kalendářního měsíce, a to bez ohledu na délku jejich prodlevy a

kategorii jednotlivých závad. Odstoupením od smlouvy podle tohoto bodu nezaniká právo Objednatele na uplatnění sankce podle odst.5.1.této Smlouvy.

10.1.2. Porušování jiných smluvních povinností, pokud k jejich nápravě nedojde ani ve lhůtě 30 dnů od písemné výzvy druhé smluvní strany.

10.2. Objednatel je oprávněn odstoupit od smlouvy v případě, že nezíská účelovou dotaci na spolufinancování předmětu Smlouvy, a tedy nedojde k uzavření „Smlouvy o poskytnutí podpory z Integrovaného regionálního operačního programu“(nebo obdobné smlouvy nebo vydání rozhodnutí) nebo v případě, že Objednateli bude dotace krácena.

10.3. Odstoupit od Smlouvy je možné výhradně na základě písemného oznámení druhé smluvní straně řádně doručeného dle příslušných ustanovení této Smlouvy s účinky od doručení oznámení.

10.4. V případě odstoupení od Smlouvy nebude mít žádná ze smluvních stran nárok na vrácení plnění poskytnutého druhou smluvní stranou na základě Smlouvy nebo v souvislosti se Smlouvou. Odstoupení od Smlouvy se nebude týkat nároku kterékoli smluvní strany na peněžité plnění ze Smlouvy nebo v souvislosti se Smlouvou, jestliže nárok na takové peněžité plnění vzniknul před odstoupením od Smlouvy.

11. Doručování

11.1. Jakákoli oznámení nebo jiná sdělení vyžadovaná Smlouvou budou v písemné formě zaslána druhé smluvní straně, nebude-li stanoveno nebo mezi smluvními stranami dohodnuto jinak, a to kurýrem nebo poštovní zásilkou s doručenkou, a budou pro účely této Smlouvy považována za doručená a obdržená adresátem, jestliže se doručení provede kurýrem, pak v den, kdy bude potvrzeno převzetí příslušné zásilky adresátem a jestliže se doručení provede poštovní zásilkou, pak v den příjmu uvedený na doručence. V případě nevyzvednutí poštovní zásilky s doručenkou adresátem je za den doručení považován 15. den od oznámení uložení takové zásilky k vyzvednutí.

11.2. Smluvní strany mohou pro účely Smlouvy změnit svoji doručovací adresu výhradně na základě písemného sdělení doručeného jedním ze shora uvedených způsobů druhé smluvní straně. Smluvní strany se zavazují, že v případě změny své adresy budou o této změně druhou stranu informovat nejpozději do 3 (slovy: tří) dnů od takové změny a změna adresy bude zanesena do Smlouvy ve formě dodatku ke Smlouvě, který bude podepsán statutárními zástupci obou smluvních stran.

12. Utajení informací

12.1. Smluvní strany budou povinny zajistit utajení informací obsažených v podkladech způsobem obvyklým pro utajování takových informací, nebude-li výslovně sjednáno jinak.

12.2. Právo užívat, poskytovat a zpřístupnit důvěrné informace třetím osobám (včetně úřadů a soudů) budou mít smluvní strany v rozsahu a za podmínek nezbytných pro řádné plnění povinností vyplývajících ze zákona, právních předpisů a úředních rozhodnutí.

12.3. Objednatel má povinnost podle ust. § 219 zák. č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, zveřejnit Smlouvu (plný text) s Poskytovatelem včetně jejích změn a

dodatků na svém profilu zadavatele a uveřejnit Smlouvu v registru smluv. Poskytovatel je povinen poskytnout Objednateli potřebnou součinnost k podpisu této smlouvy podle ustanovení zák. č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, a podle zák. č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). Poskytovatel je seznámen se skutečností, že poskytnutí těchto informací se dle citovaných zákonů nepovažuje za porušení obchodního tajemství a s jejich zveřejněním tímto vyslovuje svůj souhlas. Uveřejnění smlouvy v registru smluv zajistí Objednatel.

13. Vyšší moc

13.1. Zpoždění plnění v důsledku vyšší moci (definované v Příloze č. 1této Smlouvy) smluvní strana, která se na tuto vyšší moc odvolává, druhé smluvní straně bezodkladně oznámí, a to písemně nebo elektronicky.

14. Závěrečná ustanovení

14.1. Omezení, rozšíření a jiné změny této Smlouvy jsou možné po předcházejícím souhlasu smluvních stran formou písemných vzestupně číslovaných dodatků, podepsaných k tomu oprávněnými zástupci obou smluvních stran. Dodatek ke Smlouvě musí být uzavřen v souladu se zák. č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění.

14.2. Smluvní strany se zavazují plně dodržovat ustanovení Nařízení (EU) 2016/679 (GDPR) vůči všem relevantním informacím získaným v rámci realizace této smlouvy a v rámci realizace této smlouvy.

14.3. Poskytovatel se zavazuje učinit veškeré nezbytné úkony a opatření vedoucí ke splnění všech podmínek IROP v rámci plnění svých povinností z této smlouvy, a to zejména:

14.3.1. uchovávat veškerou dokumentaci související s realizací projektu včetně účetních dokladů nejméně do konce roku 2029,

14.3.2. poskytovat požadované informace a dokumentaci související s realizací projektu zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, NKÚ, 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 projektu a poskytnout jim při provádění kontroly součinnost.

14.4. Smluvní strany prohlašují, že si tuto Smlouvu před podpisem přečetly, že byla uzavřena po vzájemném projednání, podle jejich pravé a svobodné vůle, určitě, vážně a srozumitelně, nikoliv v tísni za nápadně nevýhodných podmínek. Autentičnost této Smlouvy stvrzují svým podpisem.

14.5. Tato Smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem jejího uveřejnění prostřednictvím registru smluv postupem dle zákona č. 340/2015., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), v platném znění. Tuto povinnost zveřejnění smlouvy v registru smluv zajistí objednatel. Realizace této smlouvy nezačne dříve než po předání a akceptaci kompletního Díla dle Smlouvy o dílo č. .....(č. smlouvy zhotovitele S-JAKA-000220) .

14.6. Smluvní strany berou na vědomí, že tato smlouva, včetně jejích případných změn a dodatků, musí být uveřejněna podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) v registru smluv, vyjma údajů, které požívají ochrany dle zvláštních zákonů, zejména osobní a citlivé údaje a obchodní tajemství a berou za tuto povinnost odpovědnost.

14.7. Smlouva se vyhotovuje ve 2 stejnopisech, z nichž každý má hodnotu originálu, každá smluvní strana obdrží po jednom výtisku, a v jednom vyhotovení v elektronické podobě.

14.8. Nedílnou součástí této Smlouvy jsou tyto její přílohy:

Příloha č. 1 – Popis služeb servisní podpory (jedná se o dokument, který byl přílohou č. 4 zadávací dokumentace pro veřejnou zakázku s názvem „Kybernetická bezpečnost Zdravotnické záchranné služby Jihomoravského kraje“)
Příloha č. 2 – Kalkulace cen

V Brně, dne ……

Za Objednatele

……
Zdravotnická záchranná služba
Jihomoravského kraje, příspěvková organizace
MUDr. Hana Albrechtová, ředitelka

V …… dne ……

Za Poskytovatele

RNDr. Martin Nehasil
Digitálně podepsal RNDr. Martin Nehasil
Datum: 2019.11.12 10:35:17 +01'00'

……
YOUR SYSTEM, spol. s r.o.
RNDr. Martin Nehasil, jednatel

Příloha č. 1– Popis služeb servisní podpory

PŘÍLOHA Č. 4: TECHNICKÁ SPECIFIKACE SERVISNÍCH SLUŽEB

V této příloze jsou uvedeny výchozí podmínky a požadavky na servisní služby v rámci této veřejné zakázky.

OBSAH

SEZNAM PŘÍLOH

Nejsou.

VYUŽITÉ ZDROJE

[1] Technická specifikace

SEZNAM TABULEK

SEZNAM ZKRATEK A POJMŮ

Zkratka/pojem	Význam
365x7x24	Poskytování služeb 365 dní v roce, 24 hodiny denně, 7 dnů v týdnu
DB	Databáze
DC	Datové centrum
EU	Evropská unie
HW	Hardware
ICT	Informační a komunikační technologie
IROP	Integrovaný regionální operační program
IS	Informační systém
OS	Operační systém
PD	Projektová dokumentace
SF EU	Strukturální fondy Evropské unie
SLA	Úroveň a podmínky poskytování služeb technické a technologické podpory.
SoD	Smlouva o dílo
SW	Software
VŘ	Výběrové řízení
VZ	Veřejná zakázka
ZD	Zadávací dokumentace
ZOS	Zdravotnické operační středisko
ZVZ	Zákon o zadávání veřejných zakázek
ZZOS	Záložní zdravotnické operační středisko
ZZS JMK	Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace

Tabulka 1: Seznam zkratek a pojmů

1 PŘEDMĚT PLNĚNÍ

Předmětem plnění veřejné zakázky (dílem) je komplexní dodávka a implementace technologií, dodávky SW, HW a infrastruktury pro realizaci technických bezpečnostních opatření dle § 5 odst. 3) zákona č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB) pro zabezpečení IS provozovaných Zadavatelem, kterým je Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace. Součástí plnění VZ jsou dále servisní služby po dobu udržitelnosti projektu.

Předmětem plnění této smlouvy je poskytování dodaných úprav informačních systémů, technologií, SW, systémového SW, HW a komunikační infrastruktury a související vybavení dodaných v rámci díla realizovaného v rámci smlouvy o dílo (dále jen „SoD“) min. na dobu 5 let od dodání díla.

Předmět plnění je tedy následující:

1. Zajištění technické a technologické podpory a nezbytných servisních služeb KB ZZS JMK.
2. Uvedené služby jsou nad rámec záruky, jak je definována ve SoD.
3. Služby budou poskytovány v režimu 7x24x365 – služby systému a jeho částí budou k dispozici uživatelům nonstop, protože ZZS JMK poskytuje služby nonstop.
4. Součástí bude maintenance technologií a dodaného SW, technická a technologická podpora nad rámec záruky s kratšími SLA než v případě záruky – SLA jsou specifikována dále v tomto dokumentu.
5. Nezbytné úpravy systému vyplývající ze změn legislativy, vyhlášek, případně dalších závazných dokumentů.
6. Pozáruční servis HW a SW infrastruktury.

2 VÝCHOZÍ STAV

Výchozí stav díla pro poskytování servisních služeb je dán dodaným dílem v rámci Smlouvy o dílo.

Zahájení plnění dle této smlouvy je ode dne předání a akceptace díla dle smlouvy o dílo.

3 POŽADAVKY NA SERVISNÍ SLUŽBY

V této kapitole jsou uvedeny požadavky na servisní služby, tj. maintenance a základní podpora technologií a IS dodaných v rámci smlouvy o dílo.

3.1 POSKYTOVANÉ SLUŽBY

Jsou požadovány následující služby:

1. Poskytování služby Hotline včetně základní servisní technické podpory Systému při odstraňování závad Systému. Hotline bude k dispozici v režimu 24 x 7, nicméně služby budou poskytovány dle úrovně v kap. 4 – Úroveň požadovaných služeb.
2. Poskytování pravidelné profylaxe Systému vč. indikace a předcházení možných problémů při užívání Systému.
3. Poskytování aktualizací Softwarových produktů a technologií a opravných patchů.
4. Dokumentace k aktualizacím Softwarových produktů a technologií, aktualizace provozní dokumentace Systému tak, aby odpovídala aktuálnímu stavu provozovaného Systému.
5. Aplikace service packů a hotfixů nutných pro bezchybný chod systému, které byly identifikovány na základě profylaxe a jejich aplikace byla dohodnuta s Objednatelem.

Výčet Softwarových produktů a technologií, na které se vztahují servisní služby je v kap. 4 – Úroveň požadovaných služeb.

3.2 PODMÍNKY POSKYTOVÁNÍ SLUŽEB

Druhy poruch:

A. Porucha kategorie A – Urgentní – za Urgentní poruchu se považuje stav celkové nefunkčnosti systému a nemožnost využívat klíčové funkcionality řešení nadpolovičním počtem všech uživatelů.

B. Porucha kategorie B – Běžná – za Běžnou poruchu se považuje stav, který neodpovídá předávací dokumentaci, ale neohrožuje klíčové funkcionality řešení.

Řešení poruch:

1. V případě, že se jedná o poruchu na Systému dle této Smlouvy, vztahují se na ni SLA dle této Smlouvy.
2. V případě, že se jedná o poruchu integrovaného systému nebo HW a SW infrastruktury mimo tuto Smlouvu s dopadem na Systém uvedený v této Smlouvě, nevztahují se na tuto poruchu SLA dle této Smlouvy do doby odstranění poruchy integrovaného systému nebo infrastruktury.
3. V případě, že bude snížena závažnost poruchy, snižují se poměrně k tomuto SLA a lhůty ve vztahu k nové závažnosti poruchy.
4. Poskytovatel je oprávněn navrhnout nebo poskytnout náhradní řešení poruchy tak, aby došlo k eliminaci dopadů této poruchy na provoz ZZS (snížení závažnosti nebo omezení poruchy) do konečného systémového řešení.

Způsob ohlašování poruch:

Poruchy Objednatel (oprávněné osoby Objednatele) hlásí na kontaktní místo Poskytovatele (Hot-line) prostřednictvím helpdesk, telefonicky a/nebo elektronickou poštou. Poruchy kategorie A objednatel vždy hlásí telefonicky a doplňující informace poskytuje prostřednictvím helpdesk nebo elektronickou poštou. Kontaktní údaje a oprávněné osoby Objednatele jsou uvedeny v samostatné příloze smlouvy.

Reakce Poskytovatele:

Služba Hot-line Poskytovatele dle sjednané reakční doby potvrdí Objednateli (elektronickou poštou a/nebo faxem), že obdržela výzvu Objednatele k odstranění poruchy. V potvrzení uvede označení evidované poruchy a termín zahájení prací na odstraňování poruchy. Tyto informace doručí osobě, která problém za Objednatele nahlásila a pracovišti Helpdesku Objednatele.

Režimy

- 24 x 7 – poskytování služeb non-stop, tj. 24 hodin denně, 7 dní v týdnu, 365 dní v roce.
- 5 x 10 – poskytování služeb v pracovní dny, v pracovní době
  Pracovní dny: pondělí – pátek; vyjma státních svátků, pracovní doba v pracovních dnech od 7:00 do 17:00 h.

Lhůty

Porucha	Režim	Zahájení odstraňování poruchy (reakční doba)	Lhůta na odstranění poruchy
A	24 x 7	4 hodiny v pracovní době 12 hodin mimo pracovní dobu	12 hodin v pracovní době 36 hodin mimo pracovní dobu
	5 x 10	4 hodiny v pracovní době	2 pracovní dny
B	24 x 7	Následující pracovní den	5 pracovních dnů
	5 x 10	3 pracovní dny	5 pracovních dnů

V případě poruchy, která pominula, a není možné identifikovat při prvotním výskytu její příčinu (neexistují logy, nejsou podklady od Objednatele) a potřeby monitoringu v delším časovém úseku, bude zadaný incident na helpdesku po vzájemné dohodě mezi Poskytovatelem a Objednatelem převeden do specifické kategorie pro tento účel – kategorie „Odloženo“. V případě opakovaného výskytu bude incident znovu otevřen (k datu nahlášení) a řešen v souladu s dohodnutými SLA. Poskytovatel je povinen vyvinout aktivitu k identifikaci příčiny chyby již po prvním výskytu.

V případě poruch hardwarového zařízení, systémového software či informačního systému Objednatele je Poskytovatel povinen na žádost Objednatele poskytnout Objednateli veškerou asistenci při instalaci Systému a zálohovaných dat na záložní hardware v rámci paušální platby.

3.3 OSTATNÍ PODMÍNKY

Ostatní podmínky na poskytování základní podpory jsou:

1. Servisní výjezdy (práce a cestovní náklady) na území Jihomoravského kraje nebudou Poskytovatelem Objednateli účtovány (bezplatné plnění).
2. Legislativní úpravy systému v návaznosti na změny legislativy, vyhlášek a nařízení ČR a EU a zdravotních pojišťoven – v rámci paušální platby.

3. Poskytování součinnosti dalším poskytovatelům služeb zabezpečení provozu integrovaných systémů v rámci poskytování maintenance nebo základní podpory v rámci zabezpečení provozu.
4. V rámci provozu Systému bude v součinnosti Objednatele a Poskytovatele docházet k instalacím nových verzí SW, bezpečnostních a opravných balíčků systémového SW (OS, DB apod.) a obměna HW a komunikační infrastruktury („modernizované provozní prostředí“). Služby budou na Systém poskytovány i na modernizované provozní prostředí, pokud bude zajištěno ve vzájemné součinnosti s Poskytovatelem nebo nebudou v rozporu se standartními požadavky na chod Systému.

4 ÚROVEŇ POŽADOVANÝCH SLUŽEB

V následující tabulce je uvedena úroveň požadovaných služeb k jednotlivým částem dodávky:

Ozn.	Položka rozpočtu	Režim poskytování
1	FireWall s IPS pro ZZOS	10 x 5 V době, kdy ZZOS je primárním dispečinkem tak režim 24 x 7.
2	FireWall pro ochranu segmentů ZOS	10 x 5
3	L3 switche pro ZZOS	10 x 5 V době, kdy ZZOS je primárním dispečinkem tak režim 24 x 7.
4	Aplikační firewall pro IS ZOS	24 x 7
5	Systém analýzy bezpečnostních logů (SW)	10 x 5
6	Infrastruktura (HW) pro systém analýzy bezpečnostních logů (HW)	10 x 5
7	Systémový SW pro systém analýzy bezpečnostních logů (SW)	10 x 5
8	Úpravy IS ZOS	Pro lokalitu, ve které je aktuálně provozován systém IS ZOS (je primárním dispečinkem) režim 24 x 7. Pro záložní lokalitu, pokud v ní není provozován primární dispečink 10 x 5.
9	Konfigurace systému elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů	10 x 5
10	Dvoufaktorová autentizace administrátorských VPN přístupů	24 x 7

Tabulka 2: Úroveň požadovaných služeb

5 MÍSTA PLNĚNÍ

Realizace předmětu plnění bude probíhat v následujících místech plnění:

Místo	Adresa	Předmět realizace
Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace	Kamenice 798/1d, Brno PSČ: 625 00	Primární datové centrum ZZS JMK – návaznost na technologie umístěné v tomto DC a dodávka částí technologie. Poskytování servisních služeb pro dodané úpravy IS a technologie umístěné do této lokality.
Záložní zdravotnické operační středisko ZZS JMK a záložní datové centrum	HZS Lidická 61 602 00 Brno	Záložní zdravotnické operační středisko ZZS JMK a záložní datové centrum pro toto ZZOS, kde bude umístěna dodaná technologie ZZOS a které bude propojeno s primárním datovým centrem ZZS JMK. Poskytování servisních služeb pro dodané úpravy IS a technologie umístěné do této lokality.

Tabulka 3: Místa plnění

6 OSTATNÍ PODMÍNKY

Kvalita a záruky:

1. Kvalita služeb bude zcela odpovídat požadavkům kladeným na HW i SW ve shodě s touto Zadávací dokumentací.
2. Poskytovatel se bude zavazovat provádět služby v kvalitě odpovídající účelu této Smlouvy, obecně závazným předpisům a platným technickým normám.
3. Poskytovatel bude odpovídat za závady na HW produktu způsobené neodbornou obsluhou nebo údržbou pracovníky Poskytovatele, a to až do výše nákupní ceny produktu, na kterém vznikla škoda.
4. Poskytovatel nebude odpovídat za jakékoli škody vzniklé Objednateli, ani za neplnění nebo zpožděné plnění svých povinností vyplývajících ze Smlouvy, dojde-li k nim v důsledku působení vyšší moci. Působením vyšší moci se rozumí okolnosti vylučující odpovědnost podle Zákona č. 89/2012 Sb., občanského zákoníku, zejména pak negativní vliv takové škody v době platnosti Smlouvy, nepředvídatelné události (živelná pohroma, průmyslová katastrofa, ozbrojený konflikt, revoluce nebo obdobná změna státního režimu), jejichž výskyt a vliv podstatně působí na plnění Smlouvy, aniž by tomuto vlivu Objednatel a/nebo Poskytovatel mohli s použitím veškerých jim právně dostupných a rozumně požadovatelných prostředků účinně zabránit.

Obnova dat, bezpečnost a pravidla pro update aplikace:

1. Poskytovatel nebude odpovědný za ztrátu nebo změnu dat při provozu počítačového systému Objednatele způsobenou používáním systému v rozporu s projektovou dokumentací. Případnou obnovu dat bude provádět Poskytovatel ze záloh, předaných mu Objednatelem.
2. Poskytovatel upozorní Objednatele na případné změny v doporučených pravidlech pro zálohování a obnovu systému, která byla součástí projektové dokumentace Díla.
3. Objednatel se zaváže zachovat před provedením update serverové části aplikace předchozí funkční konfiguraci aplikace pro případ její opětovné potřeby.
4. Poskytovatel v plném rozsahu odpovídá za provádění patch-managementu serverů a mobilních zařízení.
5. Nové verze systému a aplikací budou Poskytovatelem předány Objednateli k ověření deklarované funkčnosti. Vlastní implementace nebo instalace bude provedena Poskytovatelem po odsouhlasení Objednatelem. Toto se netýká odstranění závad v rámci plnění základní podpory.

Servis vybavení prováděný pracovníky Objednatele:

1. Pracovníkům Objednatele bude umožněno provádět drobné opravy závad vybavení vlastními silami při dodržení všech závazných podmínek a ustanovení jakož i veškerých pracovních postupů a doporučení stanovených Poskytovatelem.
2. Pracovník Objednatele bude povinen vyžádat si souhlas Poskytovatele v každém případě, kdy nebude zcela jisté, zda bude oprávněn provést danou opravu vlastními silami a současně si vyžádat doporučení vhodného postupu provedení opravy. Souhlas Poskytovatele i jím doporučený pracovní postup musí být zaevidován v helpdesku, provozovaném Poskytovatelem.
3. Stejně tak veškeré informace o zjištěných závadách a provedených opravách (vč. sériových čísel měněných komponent) bude Objednatel povinen řádně evidovat prostřednictvím helpdesku, provozovaného Poskytovatelem.

4. Za opravy provedené pracovníky Objednatele neponese Poskytovatel žádnou zodpovědnost a na tyto opravy nebude poskytovat žádné záruky. Poskytovatel dále neponese žádnou zodpovědnost za jakékoli závady nebo škody, způsobené pracovníky Objednatele při provádění oprav vybavení. Tyto závady nebude možné považovat za chyby informačního systému a případné odstranění těchto závad Poskytovatelem bude placenou službou.

KONEC ZÁKLADNÍ ČÁSTI DOKUMENTU

Příloha č. 2 – Kalkulace cen

Položka	Cena v Kč bez DPH	DPH	Cena v Kč vč. DPH
Zajištění služeb servisní podpory za 1 kalendářní čtvrtletí	**176 250,- Kč**	**37 012,50 Kč**	**213 262,50 Kč**
Zajištění služeb servisní podpory za 1 kalendářní rok	**705 000,- Kč**	**148 050,- Kč**	**853 050,- Kč**
Cena celkem za zajištění služeb servisní podpory za 4 roky	**2 820 000,- Kč**	**592 200,- Kč**	**3 412 200,- Kč**