EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

Příloha č. 2 a

Smlouva o dílo

uzavřená v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, v souladu se zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů

Číslo smlouvy zhotovitele RCH-250049

Číslo smlouvy objednatele .....

I.
Smluvní strany

Objednatel	**Zdravotnická záchranná služba Královéhradeckého kraje**
	Příspěvková organizace zapsaná v obchodním rejstříku pod spisovou značkou Pr 829 vedená u Krajského soudu v Hradci Králové
IČO	48145122
se sídlem	Hradecká 1690/2A, 500 12 Hradec Králové
zástupce	MUDr. Libor Seneta, ředitel
bankovní spojení	Komerční banka, a.s., pobočka Hradec Králové
číslo účtu	37237511/0100

dále jako „objednatel" a

Zhotovitel	**Aricoma Systems a.s.**
	společnost zapsaná v obchodním rejstříku vedeném Krajským soudem v Ostravě pod spisovou značkou B 11012
se sídlem	Hornopolní 3322/34, 702 00 Ostrava
IČO	04308697
DIČ	CZ04308697
zástupce	Jaroslav Dvořák, člen představenstva
	Tomáš Ječmínek, člen představenstva
bankovní spojení	Česká spořitelna a.s.
číslo účtu	6563752/0800

dále jako *„zhotovitel"*; objednatel a zhotovitel společně také jako *„smluvní strany"*

II.

Základní ustanovení a účel smlouvy

1. Smluvní strany prohlašují, že údaje uvedené v čl. I této smlouvy jsou v souladu s právní skutečností v době uzavření smlouvy. Smluvní strany se zavazují, že změny dotčených údajů oznámí bez prodlení písemně druhé smluvní straně. Při změně identifikačních údajů smluvních stran včetně změny účtu není nutné uzavírat ke smlouvě dodatek.
2. Je-li zhotovitel plátcem DPH, prohlašuje, že bankovní účet uvedený v čl. I odst. 2 této smlouvy je bankovním účtem zveřejněným ve smyslu zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „zákon o DPH"). V případě změny účtu zhotovitele je zhotovitel povinen doložit vlastnictví k novému účtu, a to kopií příslušné smlouvy nebo potvrzením peněžního ústavu; je-li zhotovitel plátcem DPH, musí být nový účet zveřejněným účtem ve smyslu předchozí věty.
3. Zhotovitel prohlašuje, že je odborně způsobilý k zajištění předmětu plnění podle této smlouvy
4. Smluvní strany určují následující osoby jako kontaktní osoby pro plnění této smlouvy:
   - Za objednatele: [redacted]
   - Za zhotovitele: [redacted]

   Změní-li se kontaktní osoba jedné ze smluvních stran, je tato strana povinna sdělit jméno nové kontaktní osoby druhé smluvní straně nejpozději do dvou dní ode dne, kdy došlo ke změně (v tomto případě postačuje forma e-mailu).
5. Tato smlouva je uzavírána smluvními stranami na základě výsledku zadávacího řízení veřejné zakázky zadávané objednatelem a nazvané **„Kybernetická bezpečnost informačních a komunikačních technologií ZZS KHK - Bezpečnostní technologie pro ZZS KHK**, která byla uveřejněna ve Věstníku veřejných zakázek pod evidenčním číslem Z2025-**009793** (dále jen „veřejná zakázka"), a to za účelem poskytování služeb v souvislosti s přípravou a realizací projektu s názvem **„Kybernetická bezpečnost IS Zdravotnické záchranné služby Královéhradeckého kraje**", reg. číslo CZ.06.01.01/00/22_003/0000037.

Odpovědné veřejné zadávání

6. Zhotovitel dále prohlašuje, že po celou dobu realizace této smlouvy zajistí:
   a) plnění veškerých povinností vyplývající z právních předpisů České republiky, zejména pak z předpisů pracovněprávních, předpisů z oblasti zaměstnanosti a bezpečnosti ochrany zdraví při práci, a to vůči všem osobám, které se na plnění veřejné zakázky podílejí; plnění těchto povinností zajistí i u svých poddodavatelů;
   b) sjednání a dodržování smluvních podmínek se svými poddodavateli srovnatelných s podmínkami sjednanými v této smlouvě, a to v rozsahu výše smluvních pokut a délky záruční doby;
   c) řádné a včasné plnění finančních závazků svým poddodavatelům, kdy za řádné a včasné plnění se považuje plné uhrazení poddodavatelem vystavených faktur za plnění poskytnutá k plnění veřejné zakázky, ve sjednaných termínech a zcela v souladu se smluvními podmínkami uzavřeného smluvního vztahu s poddodavatelem;
   d) minimální produkci všech druhů odpadů, vzniklých v souvislosti s realizací předmětu smlouvy a v případě jejich vzniku bude přednostně a v co největší míře usilovat o jejich další využití,

recyklaci a další ekologicky šetrná řešení, a to i nad rámec povinností stanovených zákonem č. 541/2020 Sb., o odpadech.

III.

Předmět smlouvy

1. Předmětem smlouvy je závazek zhotovitele provést níže specifikované dílo, a to v souladu se všemi závaznými právními předpisy a sjednanými podmínkami, a současně závazek objednatele převzít řádně provedené dílo a zaplatit zhotoviteli za řádně a včas provedené dílo cenu ve výši a za podmínek sjednaných touto smlouvou. Dílem se pro účely smlouvy rozumí 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 Objednatelem.

2. Zdravotnická záchranná služba Královéhradeckého kraje 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) a komunikační systémy (KS) ZZS KHK a došlo by tedy k omezení, případně znemožnění plnění úkolů ZZS KHK.

3. Předmětem plnění je:

   - Informační systém zdravotnického operačního střediska ZZS KHK – jedná se o primární IS sloužící pro hlavní činnost ZZS KHK, tj. poskytování PNP na území Královéhradeckého kraje.
   - Elektronická pošta – jedná se o hlavní informační systém (IS) zajišťující komunikaci mezi zaměstnanci a podporu výkonu jejich činností.
   - Pagingová síť – jedná se o radiovou komunikační síť (KS) pro komunikaci dispečinku ZOS s výjezdovými skupinami v rámci řízení poskytování PNP posádkami v terénu, tedy podporu výkonu jejich činností, konkrétně předávání výzev jednotlivým posádkám.

   Předmětem smlouvy jsou také další dodávky a služby, které nejsou výslovně uvedené v tomto článku, ale jsou nezbytné pro splnění předmětu smlouvy.

4. Účelem smlouvy je zabezpečení uvedených informačních systémů, čímž 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 KHK s využitím těchto IS.
5. 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 KHK vyplývajících z projevů kybernetických rizik (kybernetických bezpečnostních událostí).
6. 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).

7. Předmět plnění (dále také „dílo") bude realizován dle detailního popisu uvedeného v příloze č. 1 – Technická specifikace a v příloze č. 2 Technická specifikace nabízených technologii této smlouvy.

IV.

Místo a doba plnění

1. Realizace předmětu plnění bude probíhat na pracovištích objednatele, která jsou uvedena v příloze č. 1 této smlouvy.
2. Zhotovitel se zavazuje provést dílo dle čl. II. smlouvy nejpozději v termínech dle harmonogramu provádění díla dle přílohy č. 1 smlouvy – Technická specifikace.

V.

Cena

1. Cena za dílo činí:

   25 981 400,00 Kč bez DPH

   DPH 21 % ve výši 5 456 094,00 Kč

   31 437 494,00 Kč včetně DPH

   Podrobný rozpis ceny za dílo je uveden v příloze č. 3 této smlouvy nabídková cena.

2. Cena za dílo zahrnuje veškeré náklady zhotovitele spojené se splněním jeho závazku z této smlouvy, tj. cenu díla včetně dopravného, odměny za poskytnutí licence, veškerých instalačních prací, zprovoznění, zkušebního provozu, zaškolení správců a zpracování dokumentace. Cena za dílo je stanovena jako nejvýše přípustná a není ji možno překročit.
3. Je-li zhotovitel plátcem DPH, odpovídá za to, že sazba daně z přidané hodnoty bude stanovena v souladu s platnými právními předpisy; v případě, že dojde ke změně zákonné sazby DPH, je zhotovitel k ceně díla bez DPH povinen účtovat DPH v platné výši. Smluvní strany se dohodly, že v případě změny ceny díla v důsledku změny sazby DPH není nutno k smlouvě uzavírat dodatek. V případě, že zhotovitel stanoví sazbu DPH či DPH v rozporu s platnými právními předpisy, je povinen uhradit objednateli veškerou škodu, která mu v souvislosti s tím vznikla.

VI.

Předání díla, vlastnické právo k předmětu díla a nebezpečí škody

1. Za účelem předání částí díla blíže specifikovaných v čl. III této smlouvy budou mezi smluvními stranami sepsány předávací protokoly, ve kterých bude jednoznačně specifikováno, které části díla objednatel přebírá a dále zde bude uvedena specifikace případných nedodělků včetně způsobu a termínu pro jejich odstranění.
2. Po řádném předání všech částí díla a na základě předávacích protokolů, případně po odstranění nedodělků v termínech uvedených v předávacích protokolech, bude mezi smluvními stranami sepsán akceptační protokol, ve kterém objednatel prohlásí, zda dílo přejímá či nikoli. Bude-li dílo vykazovat jakékoli vady či nedodělky nebude objednatelem převzato, a tyto vady či nedodělky budou uvedeny v akceptačním protokolu spolu se lhůtou k jejich odstranění. Po odstranění vad bude zhotovitelem opětovně sepsán akceptační protokol ve smyslu tohoto článku smlouvy.
3. Předávací protokol bude podepsán oprávněnými zástupci obou smluvních stran uvedenými v čl. II odst. 4 této smlouvy.
4. Předávací protokol a akceptační protokol musí obsahovat mimo jiné tyto náležitosti:
   a) číslo předávacího/akceptačního protokolu a datum jeho vyhotovení;
   b) číslo smlouvy a datum jejího uzavření, včetně čísel a dat uzavření jejích případných dodatků, číslo veřejné zakázky;

c) označení předmětu plnění nebo jeho části v souladu s uvedením etap dle čl. III odst. 2 této smlouvy vč. soupisu dodaných jednotlivých položek a provedených prací na díle, odpovídající jednoznačně jak obsahem, tak formátem technickým podmínkám a specifikacím dle členění této smlouvy;

d) název, sídlo, IČO a DIČ objednatele a zhotovitele;

e) název projektu, registrační číslo projektu a informaci, že se jedná o projekt **„Kybernetická bezpečnost IS Zdravotnické záchranné služby Královéhradeckého kraje"**, reg. číslo CZ.06.01.01/00/22_003/0000037,

f) datum zahájení a dokončení plnění příslušné části díla/celého díla;

g) podrobné vymezení rozsahu provedených prací a dodávek
   - pro HW bude minimálně uveden:
     - název a typ zařízení
     - jeho konfigurace
     - výrobní / sériové číslo
     - seznam veškerých softwarových licencí, jsou-li dodávány jako součást daného hardware;

h) seznam příloh;

i) prohlášení objednatele, že plnění (jeho část) přejímá (nepřejímá), a to včetně uvedení případných vad a nedodělků a termínu jejich odstranění, podpis oprávněné osoby objednatele;

j) jméno a vlastnoruční podpis osoby, která předávací/akceptační protokol vystavila, včetně kontaktního telefonu a e-mailu.

5. Vlastnické právo k věcem, které jsou předmětem díla a nebezpečí škody na nich přechází na objednatele dnem převzetí díla bez vad a nedodělků objednatelem dle odst. 2 tohoto článku smlouvy.

VI.

Platební a fakturační podmínky

1. Úhrada ceny za provedení díla dle čl. V odst. 1 této smlouvy bude provedena, bezhotovostním převodem na účet zhotovitele na základě daňového dokladu – faktury. Zálohové platby nejsou přípustné a zhotovitel není oprávněn je požadovat.
2. Právo na úhradu cen za provedení díla dle přílohy č. 2 této smlouvy – nabídková cena zhotoviteli vzniká po ukončení díla dle harmonogramu provádění díla, přičemž za den ukončení se považuje den protokolárního předání a převzetí díla.
3. Faktura – daňový doklad musí splňovat veškeré náležitosti dle zákona č. 563/1991 sb., o účetnictví, ve znění pozdějších předpisů a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.
4. Faktura musí kromě zákonem stanovených náležitostí pro daňový doklad obsahovat také:

   a) číslo a datum vystavení faktury,

   b) číslo smlouvy objednatele a datum jejího uzavření, číslo veřejné zakázky,

   c) název a registrační číslo projektu: **„„Kybernetická bezpečnost IS Zdravotnické záchranné služby Královéhradeckého kraje"**, reg. číslo CZ.06.01.01/00/22_003/0000037,

   d) předmět plnění a jeho přesnou specifikaci ve slovním vyjádření (nestačí pouze odkaz na číslo uzavřené smlouvy),

   e) označení banky a číslo účtu, na který musí být zaplaceno (pokud je číslo účtu odlišné od čísla uvedeného v této smlouvě, je zhotovitel povinen o této skutečnosti informovat objednatele),

f) číslo a datum akceptačního protokolu podepsaného zástupci obou smluvních stran. (Akceptační protokol bude přílohou faktury),

g) lhůtu splatnosti faktury,

h) název, sídlo, IČO a DIČ objednatele a zhotovitele,

i) jméno a vlastnoruční podpis osoby, která fakturu vystavila, včetně kontaktního telefonu a e-mailu.

5. Lhůta splatnosti faktury je dohodou stanovena na **30 kalendářních dnů** ode dne jejího doručení objednateli. Faktura bude doručena doporučenou poštou nebo osobně oprávněnému zaměstnanci objednatele proti písemnému potvrzení.

6. Nebude-li faktura obsahovat zákonem či touto smlouvou stanovené náležitosti nebo bude chybně vyúčtována cena nebo DPH, je objednatel oprávněn fakturu před uplynutím lhůty splatnosti vrátit druhé smluvní straně k provedení opravy s vyznačením důvodu vrácení. Zhotovitel provede opravu vystavením nové faktury. Dnem odeslání vadné faktury zhotoviteli přestává běžet původní lhůta splatnosti a nová lhůta splatnosti běží znovu ode dne doručení nové a řádně vystavené faktury objednateli.

7. Faktura bude vystavena tak, aby byla doložena její účelovost.

8. Daňový doklad je považován za proplacený datem odepsání příslušné finanční částky z účtu objednatele ve prospěch čísla účtu zhotovitele.

9. Zhotovitel dále prohlašuje a potvrzuje, že k datu podpisu této smlouvy není označen správcem daně za nespolehlivého plátce a současně prohlašuje a zavazuje se za to, že veškeré bankovní účty jím uváděné při smluvním styku s objednatelem, již byly správci daně řádně oznámeny a jsou řádně zveřejněny v Registru plátců DPH v souladu se zákonem o dani z přidané hodnoty (dále jen „spolehlivý bankovní účet").

10. V případě, že se účet zhotovitele ukáže být jiným než spolehlivým bankovním účtem, nejedná se v případě vystavení faktury dle dohody smluvních stran o řádně vystavený daňový doklad ve smyslu této smlouvy a objednatel je oprávněn takový daňový doklad odeslat zpět zhotoviteli k vystavení nového řádného dokladu.

11. Zhotovitel se zavazuje v případě, kdy nastane či se projeví jakákoli změna v prohlášení uvedeném v předchozích odstavcích a/nebo nastane či se projeví jakákoli okolnost zakládající potenciální riziko ručení objednatele za zhotovitelem nezaplacenou daň ve smyslu zákona o DPH, bez zbytečného odkladu o takovéto skutečnosti písemně informovat objednatele a dále se zavazuje zjednat co možná nejdříve nápravu tak, aby správce daně objednatele z titulu ručení nevyzval k poskytnutí plnění za zhotovitele.

12. Smluvní strany se dohodly, že pokud nastane jakákoli okolnost zakládající riziko vzniku ručení za nezaplacenou daň zhotovitele předpokládaná zákonem o dani z přidané hodnoty, zejména že zhotovitel bude označen v Registru plátců DPH správcem daně jako nespolehlivý plátce či zhotovitel bude žádat splnění závazku na jiný než spolehlivý bankovní účet, objednatel je oprávněn nikoli však povinen využít institutu zvláštního způsobu zajištění daně ve smyslu ust. § 109a zákona o dani z přidané hodnoty (či jakéhokoli jiného shodného či obdobného nahrazujícího institutu obsaženého v budoucích změnách příslušného právního předpisu) a zaplatit část svého závazku odpovídající výši daně z přidané hodnoty z konkrétního zdanitelného plnění na příslušný depozitní účet správce daně zhotovitele. Postup dle tohoto odstavce se považuje za řádné splnění závazků objednatele uhradit sjednanou smluvní cenu a souvisejících plnění dle této smlouvy.

VII.

Záruční podmínky a vady díla

1. Zhotovitel prohlašuje, že předmět plnění není zatížen právními vadami.
2. Zhotovitel odpovídá za vady zjevné, skryté a právní, které projeví v době odevzdání objednateli i když se vada stane zjevnou i po této době a dále za ty vady, které se na zboží vyskytnou v záruční době uvedené v této smlouvě.
3. Rozsah, kvalita, technická specifikace, příslušenství a další související služby musí odpovídat požadavkům objednatele a vymezení uvedenému v této smlouvě. Jakékoliv odchylky od požadavků objednatele či vymezení uvedenému v této smlouvě jsou vadným plněním.
4. Zhotovitel poskytuje 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 části, 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.
5. 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)součásti 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.
6. Záruční doba se staví po dobu, po kterou nemůže objednatel dílo řádně užívat pro vady, za které nese odpovědnost zhotovitel.
7. Vady, na něž se vztahuje záruka, je objednatel oprávněn uplatnit nejpozději do konce záruční doby.
8. Zhotovitel je povinen odstranit vadu nejpozději ve lhůtě 30 kalendářních dnů od nahlášení vady objednatelem, pokud se smluvní strany v konkrétním případě nedohodnou jinak.
9. Počátkem lhůty pro zahájení odstranění vady je okamžik nahlášení vady objednatelem, avšak pouze za podmínky, že objednatel nahlásil vadu v pracovní den v době od 7:00 do 17:00 hodin. V případě, že objednatel vadu nahlásí v jiné době než v době uvedené v předchozí větě, má se za to, že objednatel nahlásil vadu nejbližšího následujícího pracovního dne v 7:00 hodin.
10. Nezajistí-li zhotovitel odstranění vady ve stanovené lhůtě, má objednatel právo zajistit odstranění vady jinou osobou a zhotovitel je povinen tyto náklady uhradit. Pokud zhotovitel prokáže, že za vadu neodpovídá, budou mu vynaložené náklady proplaceny objednatelem.
11. Požadavek na záruční servis bude přednostně ohlašován prostřednictvím rozhraní HelpDesk provozovaného zhotovitelem na adrese [redacted] přičemž přístup do HelpDesku bude objednateli zhotovitelem zřízen. V případě nedostupnosti HelpDesku či jiné závažné okolnosti bude požadavek na provedení servisní činnosti ohlašován:

    telefonicky na telefonní číslo: [redacted]

    nebo

e-mailem na e-mailovou adresu: [redacted]

12. Objednatel je v rámci provozu díla oprávněn provádět změny HW a SW, nastavení a konfigurace HW a SW, a to tak, aby byl zabezpečen chod díla a související infrastruktury.

13. V případě takových vad, které mohou ohrozit závažným způsobem majetek objednatele, je zhotovitel povinen vyvinout maximální úsilí k zajištění doby nástupu a poskytnutí záručního plnění i mimopracovní dny v co nejkratším čase.

VIII.

Práva a povinnosti smluvních stran

1. Není-li stanoveno touto smlouvou výslovně jinak, řídí se vzájemná práva a povinnosti smluvních stran příslušnými ustanoveními občanského zákoníku.

2. Zhotovitel je zejména povinen:
   a. provést dílo řádně a včas za použití materiálu a postupů odpovídajících právním předpisům a technickým normám ČR. Dílo musí odpovídat příslušným právním předpisům, normám nebo jiné dokumentaci vztahující se k provedení díla a umožňovat užívání, k němuž bylo určeno a zhotoveno.
   b. Informovat objednatele o jakýchkoliv skutečnostech, které mohou mít zejména vliv na plnění této smlouvy nebo na bezpečnost informací či vznik škody objednateli, neprodleně poté, co se o nich dozví.
   c. Umožnit objednateli kontrolu provádění díla kdykoliv v průběhu plnění smlouvy. Pokud objednatel zjistí, že zhotovitel neprovádí dílo řádně či jinak porušuje svou povinnost, poskytne zhotoviteli lhůtu k nápravě; neučiní-li tak zhotovitel ve stanovené lhůtě, je objednatel oprávněn od smlouvy odstoupit.
   d. při provádění díla zajistit, aby jednotlivé části díla na sebe plynule navazovaly tak, aby dílo bylo provedeno bez jakýchkoliv vad a nedodělků nejpozději ve lhůtách uvedených v čl. IV smlouvy.
   e. řídit se při provádění díla pokyny objednatele.
   f. odstranit zjištěné vady a nedodělky na své náklady.
   g. dbát při provádění díla dle této smlouvy na ochranu životního prostředí a dodržovat platné technické, bezpečnostní, zdravotní, hygienické a jiné předpisy, včetně předpisů týkajících se ochrany životního prostředí.
   h. postupovat při provádění díla s odbornou péčí.
   i. umožnit objednateli provést audit procesů a bezpečnostních opatření souvisejících se smlouvou.
   j. zajistit, aby veškerá komunikace související s předmětem plnění této smlouvy probíhala v českém jazyce.

3. Zhotovitel bere na vědomí a souhlasí s tím, že je, podle s § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, v platném znění (dále jen „zákon o finanční kontrole"), osobou povinou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů.

4. Zhotovitel je povinen nejméně po dobu 10 let od finančního ukončení projektu poskytovat požadované informace a dokumentaci související s realizací projektu zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu, poskytnout veškeré doklady vážící se k realizaci projektu, umožnit průběžné ověřování souladu údajů o realizaci projektu uváděných ve zprávách o realizaci projektu se skutečným stavem v místě jeho realizace a poskytnout součinnost všem osobám oprávněným k provádění kontroly, umožnit vstup na pozemky dotčené projektem a jeho realizací.

5. Uchovávat odpovídajícím způsobem v souladu se zákonem č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, a v souladu se zákonem č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, po dobu deseti let od finančního ukončení projektu, zároveň však alespoň po dobu tří let od ukončení operačního programu dle čl. 88 a násl. Nařízení Rady (ES) č. 1083/2006, o obecných ustanoveních o Evropském fondu pro regionální rozvoj, Evropském sociálním fondu a Fondu soudržnosti a o zrušení nařízení (ES) č. 1260/1999, minimálně však do konce roku 2035, veškeré originály, tuto smlouvu včetně jejích dodatků a další originály dokumentů, vztahujících se k projektu, přičemž běh lhůty se začne počítat od 1. ledna kalendářního roku následujícího poté, kdy byla provedena poslední platba na projekt. Finančním ukončením projektu se rozumí den, ke *kterému je uskutečněna poslední platba spojená s realizací projektu ze strany řídícího orgánu* a veškeré finanční prostředky/dotace jsou proplaceny na účet příjemce (tj. objednatele).

6. Objednatel je zejména povinen poskytnout zhotoviteli součinnost nutnou k provedení díla.

7. Zhotovitel je povinen písemně informovat objednatele o všech dalších (nových) poddodavatelích (včetně jejich identifikačních a kontaktních údajů a o tom, které služby pro něj v rámci předmětu plnění každý z poddodavatelů poskytuje) a o jejich změně, a to nejpozději do 7 kalendářních dnů ode dne, kdy zhotovitel vstoupil s poddodavatelem ve smluvní vztah či ode dne, kdy nastala změna. Zhotovitel je oprávněn změnit poddodavatele, pomocí něhož prokázal část splnění kvalifikace v rámci zadávacího řízení, na základě, něhož byla uzavřena tato smlouva, jen z vážných objektivních důvodů a s předchozím písemným souhlasem objednatele, přičemž nový poddodavatel musí disponovat kvalifikací ve stejném či větším rozsahu, který původní poddodavatel prokázal za zhotovitele.

8. Zhotovitel zajistí, aby jeho pracovníci (včetně poddodavatelů), kteří budou přítomni v prostorách objednatele, dodržovali všechny bezpečnostní předpisy tak, jak s nimi byli seznámeni objednatelem.

9. Zhotovitel je povinen do 2 pracovních dnů objednatele písemně informovat o jakýchkoli změnách pracovníků podílejících se přímo na realizaci díla., např. odchod zaměstnance zhotovitele, který má vzdálený přístup k instalovaným zařízením.

10. Minimálně dva členové realizačního týmu zhotovitele se musí zúčastnit na základě pozvánky objednatele kontrolních dní v sídle objednatele (neurčí-li objednatel výslovně jinak, např. že kontrolní den proběhne prostřednictvím videokonference), které budou probíhat ode dne, kdy smlouva nabude účinnosti, až do úspěšného ukončení zkušebního provozu, a to v termínech, které stanoví objednatel.

11. Zhotovitel je povinen účastnit se na základě pozvánky objednatele všech jednání týkajících se předmětu smlouvy, řídit se při provádění plnění dle této smlouvy jeho pokyny a poskytnout mu požadovanou dokumentaci. Účast na těchto jednáních není považována za technickou podporu, údržbu, poradenství ani konzultaci a zhotoviteli za takové jednání nenáleží odměna. Smluvní strany se dohodly na tom, že tato jednání mohou probíhat též videokonferenčně.

12. Zhotovitel je povinen z každého jednání dle předchozího odstavce a z každého kontrolního dne týkajícího se plnění předmětu smlouvy vyhotovit zápis o průběhu a závěrech jednání dle předchozího odstavce či kontrolního dne, který bude v případě odsouhlasení podepsán zástupci objednatele i zhotovitele, a to bezprostředně po takovémto jednání a současně odeslán na e-mail objednatele nebo bude objednateli a předán jinou obdobnou formou. Každý ze zápisů bude obsahovat minimálně tyto náležitosti: pořadové číslo zápisu, datum konání, místo konání, seznam přítomných či omluvených účastníků, program jednání, popis sjednaných úkolů a závěrů jednání dle předchozího odstavce či kontrolního dne; popis splnění úkolů

ujednaných na předchozím jednání dle předchozího odstavce či předchozím kontrolním dni; číslo smlouvy a datum jejího uzavření, číslo veřejné zakázky. Objednatel si vyhrazuje právo zápis nepřevzít, nepodepsat a prohlásit jej vadným, nebude-li obsahovat některý z výše uvedených údajů.

13. Zhotovitel je povinen smluvně zavázat své případné poddodavatele tak, aby plnili veškeré povinnosti zhotovitele uvedené v této smlouvě ve stejném rozsahu jako on sám. Zhotovitel je povinen na vyžádání objednatele předložit smlouvu mezi ním a poddodavatelem, která upravuje tyto oblasti.

14. Zhotovitel bere na vědomí, že jeho aktivity, které provádí na zařízeních objednatele prostřednictvím vzdáleného přístupu, budou monitorovány a zaznamenávány.

15. Zhotovitel má povinnost uchovat v tajnosti veškerá obchodní tajemství objednatele (dále jen „obchodní tajemství"), osobní údaje a citlivé osobní údaje dle „Nařízení Evropského parlamentu a Rady 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů - GDPR" a další informace týkající se objednatele, které v souvislosti s poskytováním předmětu plnění dle této smlouvy objednatel sdělí zhotoviteli (dále jen „důvěrné informace") a nepoužít je k jinému účelu než k plnění závazků podle této smlouvy, nepoužít je ve svůj prospěch, ve prospěch třetí osoby nebo v neprospěch objednatele ani je nesdělit žádné jiné osobě a učinit vše potřebné pro jejich ochranu a zamezení jejich zneužití. Smluvní strany dále ujednaly, že zhotovitel má v souvislosti s ujednáním dle tohoto odstavce této smlouvy zejména povinnost zajistit:
    a. mlčenlivosti vůči třetím osobám o veškerých skutečnostech, o nichž se dozvěděl v souvislosti s výkonem činnosti na základě této smlouvy;
    b. že obchodní a technické informace, které mu byly svěřeny objednatelem či osobou pověřenou objednatelem, nezpřístupní třetím osobám bez písemného souhlasu objednatele a nepoužije pro jiné účely než plnění předmětu a podmínek této smlouvy;
    c. že zabezpečí před nepovolanými osobami takové informace, které tvoří nebo mohou tvořit obchodní tajemství a takové, které případně spadají pod ochranu zák. č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, ve znění pozdějších předpisů;
    d. povinnost mlčenlivosti osob, které pověří plněním této smlouvy, tj. zaměstnanců zhotovitele a dalších osoby, které zhotovitel použije či pověří v souvislosti s poskytováním plnění dle této smlouvy (poddodavatelé);
    e. uložení veškerých dat, která budou užita v průběhu provádění díla, v souladu s účelem a za podmínek dle této smlouvy, a to zejména tak aby nedošlo k jejich zneužití třetí osobou;
    f. přijetí takových technických a organizačních opatření s tím spojených, kterým bude zabezpečeno zneužití informací a dat, která budou užita v průběhu provádění díla, třetí osobou.
16. Pokud je sdělení důvěrných informací třetí osobě nezbytné pro plnění závazků zhotovitele vyplývajících mu z této smlouvy, může zhotovitel tyto důvěrné informace poskytnout pouze s předchozím písemným souhlasem objednatele, a to za předpokladu, že tato třetí osoba písemně potvrdí svůj závazek zachování mlčenlivosti a důvěrnosti informací, které jí byly sděleny. V případě porušení závazku zachování mlčenlivosti a ochrany důvěrných informací ze strany této třetí osoby, je za toto porušení odpovědný v plném rozsahu zhotovitel.

IX.

Oznámení a komunikace

1. Veškerá komunikace na základě této smlouvy bude probíhat v souladu s tímto článkem. Kromě jiných způsobů komunikace dohodnutých mezi stranami se za účinné považují osobní doručování, doručování doporučenou poštou, datovou schránkou, či elektronickou poštou, a to na adresy

smluvních stran, nebo na takové adresy, které si strany vzájemně písemně oznámí. Kontaktní údaje je možné nahlásit na kontrolních dnech, kde se tato skutečnost napíše do zápisu.

2. Oznámení správně adresovaná se považují za uskutečněná v případě osobního doručování anebo doručování doporučenou poštou okamžikem doručení, v případě posílání elektronickou poštou okamžikem obdržení potvrzení od protistrany při použití stejného komunikačního kanálu.

X.

Licenční ujednání

1. Zhotovitel prohlašuje, že je na základě svého autorství či na základě právního vztahu s autorem návrhu technického řešení oprávněn vykonávat svým jménem a na svůj účet veškerá autorova majetková práva k výsledkům tvůrčí činnosti zhotovitele dle smlouvy včetně jejich hmotného zachycení, zejména autorské dílo užít ke všem způsobům užití a udělit objednateli jako nabyvateli oprávnění k výkonu tohoto práva v souladu s podmínkami smlouvy
2. Zhotovitel poskytuje touto smlouvou objednateli a objednatel touto smlouvou přijímá nevýhradní oprávnění k užití výsledku tvůrčí činností zhotovitele dle této smlouvy
3. Zhotovitel poskytne objednateli veškeré potřebné licence pro řádné fungování a provoz díla jako celku.
4. Zhotovitel výslovně prohlašuje, že je oprávněn disponovat právy k duševnímu vlastnictví, včetně práv autorských zahrnutých v předmětu díla v rozsahu nezbytném k řádnému plnění předmětu této smlouvy, a zavazuje se za tímto účelem zajistit řádné a nerušené užívání díla objednatelem.
5. Územní rozsah a časový rozsah licencí je neomezený.
6. Veškeré náklady související s licencemi jsou zahrnuty v ceně za dílo či poskytnutí záruky a technické podpory a zhotovitel není oprávněn po objednateli považovat úhradu těchto nákladů zvlášť.
7. Zhotovitel se zavazuje, že prováděním plnění dle této smlouvy nezasáhne neoprávněně do autorských práv třetí osoby. Zhotovitel je povinen objednateli uhradit jakékoli majetkové a nemajetkové újmy, vzniklé v důsledku toho, že objednatel nemohl předmět díla, v důsledku porušení povinností zhotovitele, užívat řádně a nerušeně. Jestliže se jakékoli prohlášení zhotovitele v tomto článku ukáže nepravdivým nebo zhotovitel poruší jiné povinnosti podle tohoto článku smlouvy, jde o podstatné porušení této smlouvy a zhotovitel uhradí ve prospěch objednatele smluvní pokutu ve výši 50.000 Kč za každé jednotlivé porušení takové povinnosti. Zaplacením smluvní pokuty není nijak dotčeno ani omezeno právo objednatele na náhradu škody, kterou lze vymáhat vedle smluvní pokuty v plné výši. S nositeli chráněných práv duševního vlastnictví vzniklých v souvislosti s realizací díla dle této smlouvy je zhotovitel povinen vždy smluvně zajistit možnost volného nakládání s těmito právy objednatelem.

XI.

Odpovědnost za škodu a pojištění

1. Zhotovitel je povinen uhradit objednateli škodu, která mu vznikla vadným plněním, a to v plné výši. Zhotovitel rovněž objednateli uhradí náklady vzniklé při uplatňování práv z vadného plnění.
2. Zhotovitel prohlašuje a zavazuje se, že po celou dobu platnosti této smlouvy bude mít sjednánu pojistnou smlouvu pro případ způsobení škody třetí osobě s limitním plněním na jednu škodní událost minimálně **50 mil. Kč**. Pojištění musí obsahovat krytí škod způsobené na majetku, zdraví třetích osob včetně krytí odpovědnosti za finanční škody. Kopie pojistné smlouvy předloží zhotovitel objednateli před podpisem smlouvy.
3. V případě, že při činnosti prováděné zhotovitelem dojde ke způsobení prokazatelné škody objednateli nebo třetím osobám, která nebude kryta pojištěním sjednaným ve smyslu odstavce 2 tohoto článku, bude zhotovitel povinen tyto škody uhradit z vlastních prostředků.

XII.

Sankce

1. V případě, že zhotovitel neprovede dílo včas, je povinen zaplatit objednateli smluvní pokutu ve výši 0,05 % z ceny za dílo bez DPH dle čl.V odst. 1 této smlouvy, a to za každý započatý den prodlení.
2. Pro případ prodlení objednatele se zaplacením ceny za dílo dle této smlouvy sjednávají smluvní strany úrok z prodlení ve výši stanovené občanskoprávními předpisy.
3. V případě nesplnění povinnosti dle čl. VIII odst. 9 této smlouvy je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 1.000 Kč, a to za každý i započatý den prodlení s oznámením personální změny. V případě nezúčastní-li se zhotovitel kontrolních dní v sídle objednatele (či kontrolních dní, které proběhnou videokonferenčně) dle čl. VIII odst. 11 této smlouvy bez dřívějšího souhlasu objednatele s absencí zhotovitele či nezúčastní-li se zhotovitel jednání týkajícího se předmětu smlouvy na základě pozvánky objednatele dle čl. VIII odst.12 této smlouvy bez dřívějšího písemného souhlasu objednatele s absencí zhotovitele, je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 1.000 Kč za každý jednotlivý takto zmařený průběh kontrolního dne či jednoho každého jednání týkajícího se předmětu smlouvy na základě pozvánky.
4. V případě nepředá-li či nedoručí-li zhotovitel zápis o průběhu kontrolního dne či zápis o průběhu a závěrech jednání týkajícího se předmětu smlouvy dle čl. VIII odst. 12 této smlouvy objednateli ani do pěti pracovních dní ode dne konání jednání či kontrolního dne, je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 1.000 Kč, a to za každý i započatý den prodlení s předáním či doručením každého takovéhoto zápisu.
5. V případě porušení povinnosti dle čl. XI odst. 2 této smlouvy, tj. povinnosti mít po celou dobu platnosti této smlouvy sjednanou pojistnou smlouvu pro případ způsobení škody třetí osobě s limitním plněním na jednu škodní událost minimálně 50 mil. Kč, je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 5.000 Kč za každý i započatý měsíc, v němž nebude mít sjednanou shora uvedenou pojistnou smlouvu.
6. Smluvní pokuta a úrok z prodlení jsou splatné do 30 dní ode dne doručení písemného vyúčtování příslušné výše povinné straně.
7. Zaplacením jakékoli smluvní pokuty není dotčen nárok objednatele na náhradu škody, objednatel má nárok na náhradu škody vedle smluvní pokuty v plné výši. Zaplacením smluvní pokuty není dotčena povinnost splnění povinnosti, která je prostřednictvím smluvní pokuty zajištěna.

XIII.
Zdrojové kódy

1. Zhotovitel se zavazuje předat objednateli kompletní dílo dle této smlouvy včetně všech jeho částí a součástí, dále se zavazuje předat veškeré zdrojové kódy, které jsou potřebné pro provoz, údržbu, úpravu, aktualizaci a modernizaci díla, a v neposlední řadě se zavazuje předat také dokumentaci (včetně kompletní programové dokumentace – tj. především architektura, dokumentace kódu, dokumentace algoritmů) související s dodávaným dílem dle této smlouvy.
2. Nedohodnou-li se smluvní strany jinak, je zhotovitel povinen v den předání díla předat objednateli také zdrojové kódy díla, které je počítačovým programem. Toto ustanovení se nevztahuje na produkty třetích stran, které nejsou autorským dílem zhotovitele a jeho poddodavatelů. Zdrojový kód musí být spustitelný v prostředí objednatele a zaručující možnost ověření, že je kompletní a ve správné verzi. Zdrojový kód bude předán na nepřepisovatelném technickém nosiči dat a označením „zdrojový kód". O předání tohoto technického nosiče dat bude sepsán předávací protokol.
3. Povinnost zhotovitele dle odst. 2 tohoto článku se přiměřeně použije i pro jakékoliv opravy, změny a doplnění zdrojového kódu díla, k nimž dojde při plnění této smlouvy, v rámci záručních oprav či v rámci pozáručního servisu.

XIV.

Odstoupení od smlouvy

1. Smlouvu lze ukončit buď dohodou smluvních stran, nebo odstoupením od smlouvy kterékoliv ze smluvních stran.

2. Rozhodne-li se některá ze smluvních stran od smlouvy odstoupit, je povinna svoje odstoupení písemně oznámit druhé smluvní straně s uvedením termínu, ke kterému od smlouvy odstupuje. V odstoupení musí být dále uveden důvod, pro který strana od smlouvy odstupuje, včetně popisu skutečností, ve kterých je tento důvod spatřován. Dohoda o ukončení smluvního vztahu musí být písemná, jinak je neplatná.

3. Objednatel i zhotovitel mají právo od smlouvy odstoupit v případě podstatného porušení smlouvy druhou smluvní stranou, pokud je konkrétní porušení povinnosti příslušnou smluvní stranou jako podstatné sjednáno ve smlouvě nebo stanoveno zákonem.

Smluvní strany se dohodly, že za podstatné porušení smlouvy ze strany zhotovitele, pokud není ve smlouvě uvedeno jinak, považují zejména:

a) prodlení zhotovitele s provedením díla delší než 15 kalendářních dnů,

b) prodlení zhotovitele s plněním jeho závazku dle smlouvy řádně a včas odstranit řádně objednatelem uplatněné vady delší než 15 kalendářních dnů,

c) postup při provádění díla způsobem, který zjevně neodpovídá dohodnutému rozsahu plnění a termínu předání plnění objednateli,

d) neplnění povinnosti dané mu smlouvou i přes písemnou výzvu a poskytnutí přiměřené lhůty k nápravě.

4. Odstoupí-li některá ze stran od této smlouvy, ať již na základě smluvního ujednání či ustanovení zákona, stanovují strany svá práva a povinnosti, trvající i po odstoupení od smlouvy, takto:

a) strany vstoupí neprodleně v jednání za účelem smírného vyřešení jejich vztahů.

b) zhotovitel provede soupis všech jím vykonaných činností a úkonů ke splnění jeho závazků dle smlouvy do doby ukončení Smlouvy, oceněných stejným způsobem dle smlouvy (dále jen „soupis");

c) zhotovitel vyzve objednatele k protokolárnímu předání a převzetí všech plnění dle soupisu;

d) objednatel není povinen soupis převzít, pokud obsahuje nesprávné údaje

e) zhotovitel provede vyúčtování plnění dle soupisu a vystaví závěrečnou fakturu

f) je povinen do 14 dnů ode dne, kdy nastanou účinky odstoupení, převést již uhrazenou celou cenu zboží zpět na účet objednatele a objednatel se zavazuje ve stejné lhůtě převést zpět zboží zhotoviteli,

g) strana, která porušila smluvní povinnost, jejíž porušení bylo důvodem odstoupení od této smlouvy, je povinna druhé straně nahradit náklady s odstoupením spojené. Tím není dotčen nárok na náhradu škody ani povinnost zaplatit smluvní pokutu.

5. Na zhotovitelem předané a objednatelem převzaté plnění dle soupisu se přiměřeně i po ukončení smlouvy vztahují licenční ujednání, ujednání o záruce ze smlouvy včetně odpovědnosti za vady, slevy, smluvní pokuty a náhrady škody za vadné plnění.

6. Odstoupením od smlouvy nezaniká nárok oprávněné strany na zaplacení smluvních pokut a náhradu škody.

XV.

Závěrečná ustanovení

1. Vztahy touto smlouvou neupravené se řídí příslušnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, a zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších předpisů.

2. Tato smlouva nabývá platnosti dnem podpisu oběma smluvními stranami, účinnosti smlouva nabývá dnem jejího uveřejnění v registru smluv v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů (dále také „zákon o registru smluv"). Zveřejnění dle předchozí věty zajistí objednatel.

3. Zhotovitel bere na vědomí a výslovně souhlasí s tím, že smlouva včetně příloh a případných dodatků bude zveřejněna v souladu se zákonnými požadavky, zejména zákonem o registru smluv.

4. V případě plurality osob na straně zhotovitele se tyto osoby zavazují, že budou vůči objednateli a třetím osobám z jakýchkoliv právních vztahů vzniklých v souvislosti s plněním předmětu smlouvy zavázáni společně a nerozdílně, a to po celou dobu plnění smlouvy, i po dobu trvání jiných závazků vyplývajících ze smlouvy.

5. Zhotovitel nesmí bez souhlasu objednatele postoupit svá práva a povinnosti plynoucí ze smlouvy třetí osobě.

6. Zhotovitel dále prohlašuje, že on sám či poddodavatel, který se podílí na plnění této smlouvy z více než 10 % hodnoty této smlouvy není osobou, na kterou se vztahují mezinárodní sankce dle zákona č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů ve spojení s čl. 5k nařízení Rady (EU) č. 833/2014 ze dne 31. června 2014, o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění nařízení Rady (EU) č. 2022/578 ze dne 4. dubna 2022 a zároveň že žádné finanční prostředky, které obdrží za plnění dle této smlouvy, nepoužije v rozporu s mezinárodními sankcemi uvedenými v § 2 zákona č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů, zejména, že tyto finanční prostředky přímo ani nepřímo nezpřístupní osobám, subjektům či orgánům s nimi spojeným uvedeným v sankčních seznamech v souvislosti s konfliktem na Ukrajině nebo v jejich prospěch. **Zhotovitel se zavazuje, že jakoukoli změnu skutečností, která bude mít vliv na skutečnosti dle tohoto odstavce, oznámí písemně objednateli do 5 pracovních dnů od okamžiku, kdy se o této skutečnosti dozví.**

7. Smlouva je vyhotovena v elektronické podobě, podepsaná elektronickými podpisy oprávněných osob smluvních stran. Tuto smlouvu lze měnit nebo doplňovat po dohodě smluvních stran pouze písemnými, očíslovanými dodatky, podepsanými oprávněnými zástupci obou smluvních stran. Změnit nebo doplnit smlouvu mohou smluvní strany pouze formou písemných dodatků, při respektování právní úpravy obsažené v zákoně o ZZVZ, případně jiném obecně závazném právním předpise upravujícím oblast veřejných zakázek

8. Smluvní strany shodně prohlašují, že smlouva byla podepsána vážně a svobodně, nikoli v tísni nebo za nápadně nevýhodných podmínek, a na důkaz toho k ní připojují své právoplatné podpisy.

Přílohy:

Příloha č. 1 Technická specifikace

Příloha č. 2 Technická specifikace nabízených technologií

Příloha č. 3 Cenová nabídka

Příloha č. 4 Seznam realizačního tymu

Za objednatele v Hradci Králové dne

[redacted]

.....

MUDr. Libor Seneta, ředitel

Za zhotovitele v(e) [bude doplněno před uzavřením smlouvy] dne

[redacted]

.....

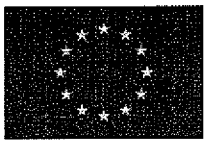
Jaroslav Dvořák,

člen představenstva

[redacted]

Tomáš Ječmínek,

člen představenstva



Spolufinancováno Evropskou unií

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

Příloha č. 1: Technická specifikace

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
EKP	Elektronická karta pacienta
EU	Evropská unie
FW	Firewall

Zkratka/pojem	Význam
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
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
KHK	Královéhradecký kraj
PČR	Policie České republiky
PD	Projektová dokumentace
PNP	Přednemocniční neodkladná péče
RCT	Radiový komunikační terminál radiové sítě Pegas/Matra
SaP	Síly a prostředky

Zkratka/pojem	Význam
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
ZZS	Zdravotnická záchranná služba (ve všeobecném významu)
ZZS KHK	Zdravotnická záchranná služba Královéhradeckého kraje

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 Královéhradeckého kraje. Součástí plnění VZ jsou dále servisní služby po dobu udržitelnosti projektu.

Zdravotnická záchranná služba Královéhradeckého kraje 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) a komunikační systémy (KS) ZZS KHK a došlo by tedy k omezení, případně znemožnění plnění úkolů ZZS KHK.

Konkrétně se jedná o zvýšení kybernetické bezpečnosti pro následující IS (dle výzvy ostatní IS):

1. Informační systém zdravotnického operačního střediska ZZS KHK – jedná se o primární IS sloužící pro hlavní činnost ZZS KHK, tj. poskytování PNP na území Královéhradeckého kraje.
2. Elektronická pošta – jedná se o hlavní informační systém (IS) zajišťující komunikaci mezi zaměstnanci a podporu výkonu jejich činností.
3. Pagingová síť – jedná se o radiovou komunikační síť (KS) pro komunikaci dispečinku ZOS s výjezdovými skupinami v rámci řízení poskytování PNP posádkami v terénu, tedy podporu výkonu jejich činností, konkrétně předávání výzev jednotlivým posádkám.

Zabezpečením uvedených informačních a komunikačních 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 KHK s využitím těchto IS a KS.

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 a KS ZZS KHK vyplývajících z projevů kybernetických rizik (kybernetických bezpečnostních událostí).

Zvýšením bezpečnosti bude dosaženo nejen garantované provozování uvedených IS a KS, 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. 4 – Rozsah dodávky a souvisejících služeb.

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 – Předmět a rozsah dodávky** – 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 5 - Harmonogram** – kapitola obsahuje harmonogram realizace předmětu plnění VZ.
- **Kapitola 6 – Místa plnění** – kapitola obsahuje místa plnění v rámci realizace předmětu plnění VZ.
- **Kapitola 7 – 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 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 a KS provozovaných Zadavatelem, kterým je Zdravotnická záchranná služba Královéhradeckého kraje.

Cílem projektu je zvýšení kybernetické bezpečnosti pro následující IS:

1. Informační systém zdravotnického operačního střediska ZZS KHK – jedná se o primární IS sloužící pro hlavní činnost ZZS KHK, tj. poskytování PNP na území Královéhradeckého kraje.
2. Elektronická pošta – jedná se o hlavní informační systém (IS) ZZS KHK zajišťující komunikaci mezi zaměstnanci ZZS KHK a podporu výkonu jejich činností.
3. Pagingová síť – jedná se o komunikační síť (KS) pro komunikaci výjezdových skupin ZZS s dispečinkem ZOS v rámci řízení poskytování PNP posádkami v terénu, tedy podporu výkonu jejich činností.

Detailní popis IS je uveden v kap. 7.2 – Informační systémy k zabezpečení.

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

b) / § 18 nástroj pro ochranu integrity komunikačních sítí

c) / § 19 nástroj pro ověřování identity uživatelů

e) / § 21 nástroj pro ochranu před škodlivým kódem

h) / § 24 nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

i) / § 25 aplikační bezpečnost

j) / § 26 kryptografické prostředky

k) / § 27 nástroj pro zajišťování úrovně dostupnosti informací

Předmětem jsou nástroje pro zajištění řešení kybernetické bezpečnosti v daných oblastech. Nástroje mohou pokrývat jen část oblasti, případně více oblastí. Předmětem dodávky není komplexní zajištění kybernetické bezpečnosti v daných oblastech, ale dodávka technologií a služeb dle požadavků u vedených níže tak, aby jimi byly doplněny stávající technologie a bezpečnostní opatření ZZS KHK a tím společně ZZS KHK zajistí kybernetickou bezpečnost svého kyberprostoru.

Rozsah dodávky je uveden v následující kapitole.

4 ROZSAH DODÁVKY A SOUVISEJÍCÍCH SLUŽEB

4.1 VYMEZENÍ PŘEDMĚTU A ROZSAHU DODÁVKY

Rozsah dodávky je následující:

#	Položka rozpočtu	Počet	Stručný popis položky	ID[1]
1	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 analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí a související služby. Popis požadavků na předmět plnění je uveden v kap. 4.4.2.	H.4
2	Systémy pro monitoring systémů a komunikační infrastruktury	1 soubor	Dodávka systémů pro monitoringu systémů a komunikační infrastruktury v obou datových centrech, systémy pro sběr dat o síťovém provozu, a to jak na vstupu do interních sítí, tak také v rámci serverů VMWare. Součástí je dodávka, instalace, nastavení, implementace nastavení a pravidel a napojení na systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí a související služby. Popis požadavků na předmět plnění je uveden v kap. 4.4.3	H.5
3	Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí	1 soubor	Dodávka systému analýzy bezpečnostních logů (IS ZOS, el. pošta, pagingová síť, infrastruktura). Součástí bude i monitoring a reportingu změn v AD. Součástí je dodávka, instalace, nastavení, implementace nastavení a pravidel a související služby. Popis požadavků na předmět plnění je uveden v kap. 4.4.4	H.5, H.7
4	Analytické nástroje ZOS pro vytváření bezpečnostních analýz	1 soubor	Dodávka analytického nástroje pro ZOS pro vytváření bezpečnostních analýz. Součástí je dodávka, instalace, nastavení, implementace nastavení a pravidel a související služby. Popis požadavků na předmět plnění je uveden v kap. 4.4.5.	H.5
5	Úpravy IS ZOS	1 soubor	Úpravy IS ZOS v následujícím rozsahu:	H.5, H.3

[1] Jedná se o pomocné interní označení příslušnosti do položky v rozpočtu projektu bez specifického významu pro VZ.

#	Položka rozpočtu	Počet	Stručný popis položky	ID[1]
			1. Zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů. 2. Monitoring a reporting a přístupů. 3. Napojení na komunikační prvky – izolace dispečinku. Součástí je dodávka úprav, implementace, nastavení a napojení na systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí a související služby. Popis požadavků na předmět plnění je uveden v kap. 4.4.6.	
6	Dodávka a implementace technologií 802.1x pro zabezpečení přístupů do LAN sítě	1 soubor	Implementace technologie 802.1x na přístupových switchích centrálních lokalit (2x DC) a výjezdových stanovišť (14). Ověření zařízení a uživatelů autentizací v rámci RADIUS serverů Microsoft NPS s integrací do jednotného Active Directory. Součástí je dodávka aktivních prvků, implementace, nastavení a napojení na systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí a související služby. Popis požadavků na předmět plnění je uveden v kap. 4.4.7.	H.8 H.9
7	Zajištění šifrování v rámci komunikační sítě	1 soubor	Síťové prvky, které podporují šifrovanou komunikaci v rámci WAN sítě. Součástí je implementace a související služby. Popis požadavků na předmět plnění je uveden v kap. 4.4.8.	H.11
8	Infrastruktura (HW) pro běh dodávaného SW a technologií	1 soubor	Infrastruktura (HW) pro: 1. Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí 2. Systémy pro monitoring systémů a komunikační infrastruktury a implementaci 802.1x 3. Analytické nástroje ZOS pro vytváření bezpečnostních analýz 4. Aplikační firewall pro IS ZOS 5. Další dodávané technologie, případně pro specifické potřeby dodávky Jedná se o datové úložiště, servery, implementaci a související služby. Popis požadavků na předmět plnění je uveden v kap. 4.4.9.	H.6 H.5 H.10 H.13
9	Systémový SW pro běh	1 soubor	Systémový SW pro:	H.7 H.5

#	Položka rozpočtu	Počet	Stručný popis položky	ID[1]
	dodávaného SW a technologií		1. Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí 2. Systémy pro monitoring systémů a komunikační infrastruktury a implementaci 802.1x 3. Analytické nástroje ZOS pro vytváření bezpečnostních analýz 4. Aplikační firewall pro IS ZOS 5. Další dodávané technologie, případně pro specifické potřeby dodávky Jedná se o operační systémy, případně databázový SW, případně jiný SW nezbytný pro běh systému, implementaci a související služby. Popis požadavků na předmět plnění je uveden v kap. 4.4.9.	H.10 H.12
10	Nástroje pro testování zranitelností a testování zranitelností	1 soubor	Dodávka nástrojů pro testování zranitelnosti a penetračních testů v souladu se standardy ZKB a závěrečných testů zranitelnosti z externí sítě na systémy IS ZOS, Elektronickou poštu a Paging a následné periodické testování bezpečnostních zranitelností systémů, které komunikují s externími subjekty. Součástí je dodávka, instalace, nastavení, implementace a související služby. Součástí je také provedení testů zranitelností a penetračních testů. Popis požadavků na předmět plnění je uveden v kap. 4.4.10.	H.4
11	Řízení aktualizací a vzdálená správa zabezpečovaných IS, provozní infrastruktury a bezpečnostních technologií	1 soubor	Řízení aktualizací (instalace bezpečnostních záplat a záplat zajišťujících dostupnost důležitých a citlivých dat) a vzdálená správa zabezpečovaných IS, provozní infrastruktury a bezpečnostních technologií včetně instalace a konfigurace. Popis požadavků na předmět plnění je uveden v kap. 4.4.11.	H.16

Tabulka 2: Předmět a rozsah dodávky

4.1.1 Související služby a náležitosti dodávky

Součástí dodávky jsou dále následující služby a náležitosti:

1. Projektové řízení dodávky řešení
2. Provedení bezpečnostního auditu.
3. Zpracování návrhu dodávky a konfigurace technických opatření v souladu s výstupy a doporučeními vyplývající z bezpečnostního auditu, související konzultace.

4. Dodávka, implementace, instalace, zapojení a konfigurace technických opatření v souladu s výstupy a doporučeními vyplývající z bezpečnostního auditu.
5. Migrace vybraných systémů a technologií na novou infrastrukturu.
6. Konfigurační změny zabezpečovaných IS a implementace změn informačních systémů a jejich součástí.
7. Ověření funkčnosti dodaných technologií, zabezpečovaných IS a jejich (sou)částí.
8. Provedení testování zranitelnosti / 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. Poskytnutí informací pro zpracování nebo aktualizaci bezpečnostní dokumentace včetně hodnocení aktiv a rizik s tím, že bezpečnostní dokumentace by měla plně reflektovat veškeré technologické a funkční změny.
11. Seznámení s obsluhou dodávaného systému a jeho budoucím provozem (správci).
12. Zařazení do provozního prostředí objednatele (dohled, zálohování apod.).
13. Provedení zkušebního provozu.
14. Poskytnutí záruky min. 5 roky na vybavení v rámci technických opatření.

Doplňující požadavky na implementaci:

1. Zajištění kontinuity provozu ZZS KHK. Po stránce nepřetržitého provozu ZZS KHK 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.

4.1.2 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.

4.1.3 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 KHK) 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.

4.2 VÝCHODISKA A PŘIPRAVENOST

Pro řešení jsou stanovena následující východiska:

#	Popis východiska
1.	Zdravotnická záchranná služba Královéhradeckého kraje 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 KHK. Z uvedeného plyne, že informační a komunikační systémy podporující procesy poskytování PNP ze strany ZZS KHK 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 „Technologie pro Operační středisko ZZS Královéhradeckého kraje II", který byl Královéhradeckým krajem realizován pro Zdravotnickou záchrannou službu Královéhradeckého kraje (ZZS KHK) v rámci Integrovaného operačního programu (IOP), výzvy č. 11. Současné řešení není možné nahradit, jen modernizovat při zachování veškeré stávající funkcionality a vybavení. Technologie a vybavení ZOS jsou předmětem zabezpečení technologiemi dodávanými v rámci dodávek uvedených dále v tomto dokumentu.
3.	Připravenost datových center bude zajištěna min. v následujícím rozsahu: 1. Dostatečně kapacitní napájení datového centra pro umístění technologií. 2. Klimatizace v datovém centru. 3. Strukturovaná kabeláž v rámci DC, mezi 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. 7 – Výchozí stav.

4.3 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 KHK – jedná se o primární IS sloužící pro hlavní činnost ZZS KHK, tj. poskytování PNP na území Královéhradeckého kraje.
    b. Elektronická pošta – jedná se o hlavní informační systém (IS) ZZS KHK zajišťující komunikaci mezi zaměstnanci ZZS KHK a podporu výkonu jejich činností.
    c. Pagingová síť – jedná se o komunikační síť (KS) pro komunikaci výjezdových skupin ZZS s dispečinkem ZOS v rámci řízení poskytování PNP posádkami v terénu, tedy podporu výkonu jejich činností.

2. Budou zachovány a zabezpečeny všechny současné integrace uvedených IS a vazby na jiné IS a technologie nezbytné pro provoz ZZS KHK.
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.

4.4 POŽADAVKY NA DODÁVKY

V této kapitole jsou uvedeny požadavky na dodávky.

4.4.1 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 KHK.
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. Je připravována nová vyhláška o kybernetické bezpečnosti. Pokud nabude platnosti v době realizace dodávky, je požadován i soulad s touto vyhláškou.
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.

#	Požadavek
P.9	Soulad se Zákonem č. 240/2000 Sb. O krizovém řízení a o změně některých zákonů v aktuálním znění.
P.10	Pokud výrobce nabízených technologií dodává specifické technologie pro specifické trhy (český, resp. trh EU), musí být nabízená technologie určená pro trh relevantní pro ZZS KHK (český, resp. trh EU). HW a SW licence a jejich PN (produktové číselné označení) musí být dostupné přímo v oficiálním ceníku výrobce pro relevantní trh a licencován a určen (registrován) přímo pro ZZS KHK. Podpora na licence ve všech úrovních musí být zajištěna přímo jejich výrobcem, kterého může Zadavatel přímo kontaktovat.
P.11	Při definici požadavků jsou všechny uvedené požadavky/parametry závazné jako minimální. Je-li součástí definice požadavku „umožňuje", „lze", „je možné", „možnost" apod., je uvedený požadavek/parametr závazný a požadovaná funkcionalita musí být v rámci dodávky dodána/naimplementována, předvedena a pokud je licencována, tak součástí dodané licence. Tyto technické požadavky jsou minimálně možné, účastník zadávacího řízení (dále jen „Účastník") může nabídnout charakteristiky (funkce) lepší.

Tabulka 4: Obecné a společné požadavky

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

4.4.2 Aplikační firewall pro IS ZOS

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

Systémy IS ZOS komunikují s externími systémy pomocí web services. Proto je požadováno rozšíření zabezpečení systémů IS ZZS o webový aplikační firewall, který bude chránit webové služby před potenciálními útočníky, kteří by mohli využít zranitelná místa aplikací nebo protokolů pro sledování, modifikaci dat nebo ohrožení chodu takové aplikace. Aplikační firewall musí kontrolovat, zda tento provoz neobsahuje útoky a izoluje webové služby od útočníků. V rámci implementace WAF bude zaveden i standard bezpečnostních mechanismů jako TLS v rámci HTTPS komunikace pro publikované aplikace/služby do externích sítí.

#	Požadavek
P.12	Dodávka webového aplikačního firewallu pro zabezpečení webových služeb (web services) v rámci externí komunikace IS ZOS. Minimálně je třeba zabezpečit následující aplikace: 1. Endpoint NIS IZS (SOS5) – publikováno do sítě NIS IZS 2. SOSView – publikováno do sítě Internet 3. Mobilní zadávání dat – MZD/EKP přístup z tabletů ve vozidlech. Jedná se o služby IS ZOS dostupné z externích sítí.
P.13	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

#	Požadavek
	prolomením logovacích URL hrubou silou (Brute Force útoky) s možností eskalace a potlačení technologií CAPTCHA v případě podezření, že je aplikace pod útokem.
P.14	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.15	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) – konfigurace doporučených bezpečnostních mechanismů (TLS apod.). 21. Automatická aktualizace bez zásahu uživatele, která obohatí metody WAF o data ze světových labů a honeypottů, pro lepší vyhodnocení kampaní a zero-day útoků 22. Podpora nastavení bezpečnostních politik podle IP adresy, doménového jména a URI 23. Povoleni jednotlivých HTTP metod pro jednotlivá URL. 24. Detekce anomálií a podezřelých operacích na aplikační vrstvě 25. Implementace (instalace, konfigurace, seznámení s funkcionalitami a obsluhou, dokumentace)

#	Požadavek
	26. Záruka a aktualizace SW apod. na 5 let.
P.16	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.17	Aplikační FW může být realizován, jak samostatným redundantní HW (HW ve verzi rack mount), tak virtuální appliance v rámci HW a systémového SW, který bude součástí dodávky řešení (viz kap. 4.4.9) a redundance bude tak zajištěna Failover konfigurací virtualizační platformy. Pokud bude dodáno jako virtuální appliance, musí dodavatel v rámci dodávky dle kap. 4.4.9 zajistit dostatečnou kapacitu a výkon pro provoz dodávaného řešení.
P.18	Umístění aplikačního firewallu do DC v rámci primárního zdravotnického operačního střediska. S možností migrace mezi datovými centry ZZS.
P.19	Napojení a předávání alertů a logů do systému analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí (viz kap. 4.4.4). WAF musí podporovat logování ve formátu minimálně Syslog, a případně s navrženým logovacím systémem (viz kap. 4.4.4). Součástí předávání logů do systému analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí 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 5: Aplikační firewall pro IS ZOS

4.4.3 Systémy pro monitoring systémů a komunikační infrastruktury

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

Je požadována realizace monitoringu systémů a komunikační infrastruktury v obou datových centrech, a to jak rozšířením stávajících nebo dodávkou nového nástroje. Musí se jednat o ucelené škálovatelné řešení umožňující dlouhodobé i real-time monitorování sítě na bázi technologie NetFlow s následujícími minimálními požadavky.

#	Požadavek
P.20	Je požadována dodávka SW pro monitoring systémů a komunikační infrastruktury a ucelené a škálovatelné řešení umožňující dlouhodobé i real-time monitorování sítě na bázi technologie NetFlow složené z: 1. Systém pro monitoring systémů a komunikační infrastruktury 2. Sondy síťového provozu (virtuální i fyzické) 3. Kolektoru síťového provozu 4. Modul automatického vyhodnocování IP toků

#	Požadavek
	Je požadována vzájemná integrace monitoringu síťového provozu na bázi NetFlow se systémem monitoringu systémů a komunikační infrastruktury. Tak aby bylo možné získat základní informace o datových tocích v rámci konzole monitoringu systémů a komunikační infrastruktury.
P.21	Minimální požadovaná funkční specifikace SW pro monitoring systémů a komunikační infrastruktury: 1. SW monitorující systémy a komunikační infrastrukturu ZZS na bázi ověření dostupnosti zařízení (ICMP) a stavu služeb (HTTP/HTTPS včetně content monitoringu apod), stavu portů a performance metrik (min.: CPU, RAM, HDD, Response time) pro 500 zařízení. 2. Monitoring může být prováděn: ICMP, SNMP, WMI, HTTP/HTTPS, Bat script, PS script atd. Prezentace monitorovaných zařízení musí být možná jak v rámci uživatelsky modifikované mapy (včetně integrace obrázků/fotek do mapy), tak i seznam/list zařízení, možnost filtrování pohledu/náhledu podle kritérií, jako je název/IP, Mac adresa, umístění, značka, role zařízení (server, směrovač, úložiště atd.), typy pověření, operační systémy, stav monitorování (spuštění/vypnutí, údržba). 3. Notifikace o změnách stavů a překročení prahových hodnot s možností eskalace (podle délky stavu zvolený způsob notifikace - např.: v první fázi e-mail, v druhé fázi SMS) 4. Integrace na SMTP mail systém ZZS, SMS systém ZZS (MobilChange), Mobilní aplikace SOSNow a MedText. 5. Funkce discovering/scan na L2/L3, a to jak na základě IP rozsahů, tak získání informací z routrů. Discovering musí identifikovat standardními technologiemi propojení portů a vykreslení topologie sítě. Monitorovací systém by měl být schopen skenovat podle IP adresy, podsítě nebo různých rozsahů IP adres, podle souboru hostitele serveru a zdroje SNMP a dále všechny virtuální počítače na virtuálním hostitelském serveru. 6. Během discovery nebo po něm by měly být získány podrobné hodnoty výkonu prostřednictvím SNMP v1, v2, v3, WMI, ADO, Telnet, SSH, VMWare, JMX, SMIS, AWS. 7. Reporty/sestavy o fungování infrastruktury a jejich částí dle konfigurace/zadání obsluhy včetně možnosti pohledu časové souslednosti událostí. Možnost exportu takových reportů a sestav včetně jejich plánovaného spouštění. Inventory HW a SW na základě SNMP informací o monitorovaných zařízeních. 8. REST API rozhraní umožňující integraci monitorovacího nástroje s jinými systémy pro získávání informací o stavu monitorovaných zařízení a možnosti ovládání monitorovacího systému (převedení zařízení do režimu údržby, přidat nebo odebrat zařízení atd.). 9. Integrace systémů monitoringu provozu sítě na bázi NetFlow ze systémů níže. 10. Provoz monitorovacího SW musí být realizován na samostatném odděleném HW, který bude součástí dodávky řešení (viz kap. 4.4.9) a bude připojen dvěma nezávislými porty do centrálního L3 switche. Monitorovací SW nesmí být tak (kromě centrálního L3 SW) závislý na infrastruktuře, kterou monitoruje.
P.22	Minimální požadovaná funkční specifikace sondy síťového provozu pro virtualizační platformu: 1. specializované dedikované zařízení (sonda) ve formě virtuálního zařízení virtualizační platformy pro vytváření detailních statistik IP toků o dění na síti, standardizovaný protokol pro výměnu dat o IP tocích (NetFlow v5, v9, IPFIX) včetně pokročilých funkcí filtrování

#	Požadavek
	exportů, rozpoznávání aplikací, extrakce informací o http a SIP provozu a sledování performance metrik (server response time, jiter, round trip time, delay), 2. dostupné jako virtuální zařízení pro navrženou virtualizační platformu, 3. sonda s 1 monitorovacím portem 10GbE, 4. detekce aplikací dle standardu NBAR2, monitorování a analýza HTTP provozu a VoIP statistik, podpora monitorování MAC adres, standardů NEL, NSEL, 5. podpora vzorkování na úrovni paketů i toků, 6. podpora filtrování a export datových toků na základě AS, 7. zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS, 8. časová synchronizace zařízení proti centrálnímu zdroji času na síti, 9. podpora autentizace vůči LDAP (Active Directory), 10. řízení uživatelského přístupu
P.23	Minimální požadovaná funkční specifikace fyzické sondy síťového provozu: 1. specializované dedikované zařízení (sonda) ve formě fyzického zařízení pro vytváření detailních statistik IP toků o dění na síti směrované na monitorovací porty sondy. 2. stejné požadavky jako u sondy pro virtualizační platformu (předcházející požadavek) 3. sonda s 1 monitorovacím portem 1GbE 4. Podporované monitorovací protokoly SNMP 2c,3
P.24	Minimální požadovaná funkční specifikace kolektoru síťového provozu: 1. Specializované zařízení (kolektor) určené pro uložení, vizualizaci a vyhodnocení síťových statistik exportovaných NetFlow/IPFIX dat. 2. Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite. 3. Možnost dohledání libovolné komunikace až na úroveň jednotlivých flow záznamů, průběžné grafy provozu, top statistiky, reporty, alerty, databáze aktivních zařízení na síti vč. identifikace zařízení. 4. Rack mount zařízení, snadná instalace do stávající síťové infrastruktury. 5. Datové úložiště minimálně o velikosti 1TB, použití RAID1. 6. Dva plnohodnotné management (administrativní) porty 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat. 7. Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS. 8. Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. Separace dat s omezením přístupu pro jednotlivé role/uživatele. 9. Podpora autentizace vůči LDAP (Active Directory). 10. Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména. 11. Podpora pro Cisco NEL, Cisco NSEL, Cisco NBAR2, IPFIX položek proměnlivé délky. 12. Schopnost sbírat a ukládat dlouhodobě data z tisíců zdrojů flow dat. 13. Kolektor automaticky identifikuje každý zdroj flow statistik, který mu tyto statistiky zasílá ke zpracování. O daném zdroji získá základní informace, jako jsou název, počet a rychlost rozhraní. Pro každý zdroj flow statistik automaticky zobrazuje graf průběhu provozu. 14. Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard s podporou více záložek (konfigurace per uživatel).

#	Požadavek
	15. Vytváření dlouhodobých grafů a přehledů s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH), včetně plné konfigurace grafů a pohledů uživatelem. 16. Generování statistik a podrobných výpisů nad volitelnými časovými intervaly s volitelnými filtry. Různé formáty výstupů, minimálně PDF, CSV. 17. Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Koláčové i průběhové grafy. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF nebo CSV. Automatická distribuce reportů e-mailem. Možnost automatického ukládání reportů na externí síťové úložiště. 18. Časová synchronizace zařízení proti centrálnímu zdroji času na síti. 19. Možnost přístupu a konfigurace zařízení prostřednictvím sériové linky (RS-232). 20. Podpora autentizace vůči LDAP (Active Directory). 21. Řízení uživatelského přístupu.
P.25	Minimální požadovaná funkční specifikace automatického vyhodnocování IP toků síťového provozu: 1. Rozšiřující systém na kolektor pro automatické vyhodnocování IP toků provádějící automatickou detekci bezpečnostních nebo provozních anomálií datové sítě a jejich hlášení formou událostí. Systém založen na pokročilých metodách tzv. behaviorální analýzy, které umožňují odhalovat hrozby a incidenty, které překonaly zabezpečení na perimetru nebo bezpečnostní ochranu koncových stanic, a pro které dosud není dostupná signatura. 2. Výkon zpracování min. 1000 toků/s. 3. Systém umožňuje deduplikovat flow statistiky před jejich vlastní analýzou. 4. Systém zobrazuje informace o identitě uživatelů obsaženou ve flow datech jako součást události. 5. Systém podporuje persistenci doménových jmen, tedy uložení doménového jména původce události v okamžiku zaznamenání výskytu této události. 6. Systém obsahuje předdefinovanou sadu detekčních metod a algoritmů pro analýzu flow statistik, detekci bezpečnostních incidentů, provozních problémů a síťových anomálií. 7. Detekce skenování portů, slovníkové útoky, útoky odepření služeb (DoS), útoky na síťové protokoly SSH, RDP, Telnet a další obdobné služby. 8. Detekce anomálií v DNS, DHCP, SMTP, multicast provozu a nestandardní komunikace. 9. Systém umožňuje identifikovat bezpečnostní události (např. komunikaci s botnet command & control centry, přístup na phishing servery apod.) využíváním zdrojů IP a host reputačních databází poskytovaných výrobcem a aktualizovaných nejméně každých 24 hodin. Systém umožňuje zapojit další zdroje IP a host reputačních dat pro automatickou detekci. 10. Detekce nadměrné zátěže sítě, výpadků služeb, chybějících reverzních DNS záznamů, nových a cizích zařízení připojených k síti. 11. Detekované události je možné automaticky agregovat tak, aby související události byly prezentovány v rámci pojmenované hrozby (např. infikované zařízení v síti, chybně nakonfigurované zařízení, používání nevhodných aplikací nebo služeb apod.).

#	Požadavek
	12. Správa uživatelů a přístupových práv k událostem prostřednictvím uživatelských rolí. Separace událostí s omezením přístupu pro jednotlivé role/uživatele. 13. Veškerá funkcionalita detekce anomálií je založena na vyhodnocování flow dat bez nutnosti paketové analýzy, např. nasazení speciálních senzorů výrobce, systém nevyžaduje viditelnost na úrovni zrcadlení provozu. 14. Součástí události je identifikace uživatele získaná z externího zdroje uživatelské identit v okamžiku detekce události, tato informace je perzistentní.
P.26	Instalace a konfigurace dodávaných komponent a celkového řešení na infrastrukturu dodávanou dle kap. 4.4.9. Součástí konfigurace je nastavení monitoringu systémů a komunikační infrastruktury tak aby monitoring pokrýval všechny LAN/WAN prvky a komponenty WAN sítě ZZS a navazujících technologií jako je NIS IZS, AML a INFO35. Z pohledu serverů bude úvodní implementace obsahovat všechny servery operačního řízení včetně monitoringu dostupnosti jejich služeb. U Systému monitoringu provozu sítě se bude součástí konfigurace prvotní nastavení a následné vyhodnocení monitorovaných dat a případná úprava konfigurace tak aby systéme poskytoval relevantní data o datových tocích ZZS LAN/WAN. Součástí zdrojů dat budou i data z aktivních prvků, které jsou schopny odesílat data typu NetFlow do dodávaného řešení.
P.27	Záruka 5 let, režim 5x8, garantovaná doba opravy do následujícího pracovního dne na místě včetně aktualizace SW.

Tabulka 6: Systémy pro monitoring systémů a komunikační infrastruktury

4.4.4 Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí

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

Pro systém analýzy bezpečnostních logů celého IS ZOS se požaduje řešení, které bude sdružovat záznamy o událostech z jednotlivých aplikačních modulů IS ZOS a el. pošty a z okolí systému (tzn. 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 nebo jeho infrastruktury.

#	Požadavek
P.28	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, Active directory, 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, pagingu nebo jejich infrastruktury.
P.29	Zadavatel požaduje, rozšíření/povýšení stávajícího systému analýzy bezpečnostních logů - SIEM, kterým je IBM QRadar (viz kap. 7.4.1) za účelem získání co nejvyšší kvality dodávaného řešení,

#	Požadavek
	minimalizaci možnosti vzniku následných rizik a zaručení stability a udržitelnosti daného řešení. Řešení SIEM IBM QRADAR je primárním systémem analýzy a dlouhodobého uchovávání bezpečnostních logů a vyhodnocení kybernetických událostí.
P.30	Sběr logů z aplikačních, bezpečnostních a síťových systémů využívaných v rámci ZZS nebo dodávaných v rámci tohoto projektu.
P.31	Požadujeme sběr dat z OS a DB serverů IS ZOS a elektronické pošty požadujeme minimálně pro následující události: 1. Přihlášení 2. Odhlášení 3. Neúspěšné pokusy o přihlášení Ukládání sesbíraných dat do úložiště nástroje pro následnou analýzu.
P.32	Požadujeme sběr dat/logů z Pagingového systému pro následující události: 1. Přihlášení 2. Odhlášení 3. Neúspěšné pokusy o přihlášení Ukládání sesbíraných dat do úložiště nástroje pro následnou analýzu. *Údaje budou sbírány z logů Pagingového systému, které budou zpřístupněny v rámci součinnosti.*
P.33	Minimální licenční požadavky na systém analýzy bezpečnostních logů – SIEM: 1. Požadujeme podporu a support výrobce na 5 let včetně práva SW upgrade. Neomezený počet zadaných ticketů a dostupnost podpory 7 x 24. 2. Zadavatel nepřipouští dodání partnerských ESA licencí. 3. Softwarové licence a jejich PN (produktové číselné označení) musí být dostupné v ceníku výrobce. 4. Podpora na licence ve všech úrovních, musí být zajištěna možností kontaktování výrobce, kterého může Zadavatel přímo kontaktovat 5. Požadujeme, aby samostatný formulář pro hlášení kybernetického bezpečnostního incidentu na Národní úřad pro kybernetickou a informační bezpečnost, byl přímo součástí grafického rozhraní produktu. 6. Licence pro zpracování trvalého toku událostí a síťových flow z 80-ti serverů Zadavatele v SIEM (virtuální servery). 7. Licence pro trvalé zpracování neomezeného počtu nebo objemu logů v rámci log managementu (Samotný HW musí zvládnout minimálně trvalý tok 15.000 EPS) 8. Licence musí umožnit budoucí změnu architektury z All-in-One na distribuovaný systém nebo systém s vysokou dostupností bez nutnosti reinstalace nebo dalších licenčních poplatků. 9. Licence umožňuje dočasné překročení limitu příjmu událostí a síťových flow bez ztráty jejich korelace.
P.34	Minimální funkční požadavky na systém analýzy bezpečnostních logů: 1. Řešení musí být hodnocené v segmentu „leaders" v GartnerMagicQuadrantu alespoň jednou za minulé tři roky,

#	Požadavek
	2. Podporované protokoly: Syslog, Windows Events Collection (WinRM/ RPC), FTP, S/TP/SCP, SNMP, ODBC/JDBC, CP-LEA, SDEE, log file protokol, 3. bezagentový sběr logů (sběr bez nutnosti instalovat agenta na cílový systém), 4. možnost sběru logů samostatným lokálním kolektorem s přeposíláním do centrálního systému, 5. možnost nasazení jak prostřednictvím VirtualAppliance nebo samostatným HW, 6. SIEM musí být schopen monitorovat a zpracovávat síťové pakety směrované na jeho dedikovaný síťový port ze SPAN/TAP portů aktivních síťových prvků. 7. společné webové uživatelské rozhraní SIEM pro management, analýzu a reporting, 8. možnost definovat uživatelům systému přístup k jednotlivým zařízením, jejich skupinám či síťovým segmentům, 9. automatická identifikace systémů – zdrojů logů, 10. podpora šifrované komunikace mezi zdroji logů a systémem analýzy bezpečnostních logů, pravidel pro sběr dat a archiv událostí, 11. 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.), 12. podpora sběru síťových toků (NetFlow, JFLow, Sflow) z navržených infrastrukturních prvků (switche, routery, NetFlow sondy), 13. řešení musí umožňovat automatické aktualizace, 14. poskytovat interní kontroly stavu zařízení (healthcheck) a upozornění uživatele v případě problému, 15. poskytování analytických a korelačních funkcí bez dalších zásahů a činností (out-of-the-box), 16. možnost rozšíření výběrů o uživatelské položky z obsahu logů, 17. zajištění integrity nasbíraných dat, 18. Near-real-time analýza událostí, 19. způsob zadávání vyhledávání: vyhledávací rozhraní systému správy logů musí poskytovat podporu jak pro zadání dotazu s použitím Booleovy logiky, tak pro regulární výrazy, 20. kombinované hledání v indexovaných i neindexovaných datech v systému správy logů s použitím regulárních výrazů a fulltextového vyhledávání v nestrukturovaném textu současně, 21. schopnost korelovat události DHCP, VPN a Active Directory a sledovat průběh uživatelské relace (session) v rámci celé instituce (přesná identifikace uživatele), 22. schopnost korelovat data o událostech se statickými a dynamickými seznamy označujícími položky, které mají či nemají být v síti povoleny (tj. seznam nezabezpečených protokolů), 23. přístup k datům skrze otevřené REST API pro integraci s dalšími systémy, 24. podpora korelace dat proti výsledkům scanům zranitelností třetích stran, 25. uchovávání logů i flows jak v normalizovaném formátu, tak i „raw" formátu,
P.35	Je požadováno, aby systém QRADAR SIEM byl provozován na odděleném HW včetně úložiště a neovlivňoval tak výkonnost infrastruktury produkčních systémů. Potřebný HW je součástí plnění dle kap. 4.4.9 – Infrastruktura (HW) a systémový SW pro běh dodávaného SW a technologií.

#	Požadavek
	Je požadováno, aby systém disponoval funkcí poskytování automatického backup/recovery procesu, který bude zapracován do celkového systému backup/recovery Zadavatele.
P.36	V rámci realizace je požadována detailní analýza a prováděcí projekt, které budou podrobně řešit: 1. *Doporučení pro logování* a. Doporučený obsah logovacích událostí a síťových toků b. Způsob záznamu a doručení logovacích událostí a flow c. Síťové toky d. Požadavky na součinnost Objednatele a třetích stran 2. Architektura SIEM v prostředí Zadavatele a. SIEM software (Nasazení a adresace, HW, SW, Komunikace) b. Behaviorální analýza uživatelů c. Konfigurace systému SIEM i. Klasifikace zdrojů ii. Síťové rozsahy iii. Korelační pravidla iv. Politika hesel v. Profily a role vi. Autentizace a autorizace uživatelů vii. Notifikace viii. Retenční politiky ix. Integrita uložených logovacích událostí a flow x. Nastavení modulu a formuláře pro hlášení kybernetického bezpečnostního incidentu NÚKIB xi. Reporting, minimálně dle ISO27000:2013 d. Popis Integrace jednotlivých připojených systémů do SIEM e. Návrh akceptačních kritérií a testů, včetně akceptačního protokolu pro všechny dodávané části díla. f. Návrh monitoringu, zálohování a obnovy všech částí díla. g. Časový harmonogram realizace. h. Návrh osnovy školení. Dokument analýzy a prováděcího projektu bude vypracován v písemné i elektronické editovatelné podobě, ve formátu MS Word/Excel.
P.37	Implementace na základě prováděcího projektu bude obsahovat kompletní dodávku implementačních služeb SIEM, jeho instalaci a konfiguraci v systémovém prostředí zadavatele pro informační systémy definované v prováděcím projektu a související infrastrukturu. Zejména se jedná o: 1. Instalace SIEM a jeho komponent do prostředí 2. Nastavení LogManagementu, včetně vývoje parserů. 3. Nastavení Flow 4. Nastavení retence dat 5. Nastavení korelačních pravidel s využitím framework MITRE ATT&CK 6. Nastavení modulu pro hlášení kybernetického bezpečnostního incidentu NÚKIB 7. Nastavení use-cases

#	Požadavek
	8. Nastavení všech principů a zásad uvedených v analýza a prováděcím projektu 9. Ladění False-positives Alarms 10. Nastavení autorizace a oprávnění 11. Vytvoření Dasboard profilů 12. Nastavení reportingu Nastavení notifikací
P.38	Školení v rozsahu: 1. 2 dny x 8 hodin, pro max. 5 osob 2. školí se v místě Zadavatele, který zajistí i prostory a prezentační techniku. Po dohodě obou stran je možné školení i distanční formou. 3. struktura a rozsah školení bude součástí prováděcího projektu 4. účastník musí po absolvování školení připojit standardní zdroj a vytvořit či upravit pravidlo
P.39	Je požadováno za 1 měsíc a za 3 měsíce vyhodnocení provozu a doladění korelačních pravidel na základě získaných dat během provozu implementovaného systému a dle požadavků Zadavatele.
P.40	Implementace notifikací s využitím stávajících notifikačních nástrojů ZZS. Notifikace budou prováděny následujícími nástroji: 1. E-mail 2. SMS 3. Push aplikace na mobilní zařízení (systém SOSNow) 4. Případně další *Pro notifikaci e-mailem bude využíván protokol SMTP.*
P.41	Pro zajištění vyšší bezpečnosti a auditu MS Active Directory požadujeme sběr dat/logů z MS Active Directory pro reporting všech změn provedených jednotlivými uživateli/administrátory v rámci Microsoft Active Directory (AD) ZZS (počet zaměstnanců – potenciálních uživatelů 800), tak aby bylo možné vyhodnocovat a kontrolovat změny oprávnění, které byly v rámci AD provedeny. Je požadováno sbírat, vyhodnocovat a reportovat minimálně: 1. Vytvoření nového objektu (uživatele nebo skupiny). 2. Vymazání objektu (uživatele nebo skupiny). 3. Zneplatnění (disable) uživatele. 4. Přidání člena skupiny. 5. Vymazání člena skupiny. Pro manipulaci s objekty důležitými pro IS ZOS budou vytvořena pravidla a notifikace pro správce AD. Systém musí umožnit hloubkové forenzní a bezpečnostní monitorování všech klíčových konfiguračních, uživatelských a administrátorských změn v AD prostředí. Systém musí umožnit i zabránění útočníkům provádět změny v kritických skupinách, nastavení GPO atd, v AD a zaznamenání původní IP adresy/názvu pracovní stanice pro události uzamčení účtu, aby bylo možné jednodušeji odstraňovat problémy s uzamčením účtu.

#	Požadavek
P.42	Pro oddělenou analytickou práci s logy aplikací, bezpečnostních a síťových systémů využívaných v rámci ZZS nebo dodávaných v rámci dodávky je požadována dodávka samostatného doplňujícího nástroje pro logování z IT infrastruktury: 1. Aktivní prvky (sítě) 2. Informační systémy – IS ZOS a systém elektronické pošty 3. Komunikační systémy – Pagingový systém 4. Databáze (ORACLE, MS SQL) 5. Operační systémy (MS Windows, Linux) – servery, pracoviště ZOS 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 (log server v kap. 4.4.9 – Infrastruktura (HW) a systémový SW pro běh dodávaného SW a technologií).
P.43	Dodávka a implementace nástroje na logování z IT infrastruktury, IS ZOS, Pagingového systému 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 tato část logování bude provozována na samostatném HW. Požadované 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 2 GB za den, licence s podporou na nebo licence opravňující produkt využívat po dobu min. 5 let a min. v uvedeném objemu za den. 4. Jeden společný datový sklad pro všechna indexovaná data – jeden dotaz nebo report může zahrnout všechna indexovaná data 5. Nebude 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. Bezpečné nakládání s daty, zjednodušený audit a zajištění integrity dat tak aby se dalo zjistit, zda nebylo s daty manipulováno. 13. Monitoring své vlastní konfigurace a využití s cílem udržet si kompletní auditní záznamy o tom, kdo přistupuje k systému, jaké dotazy spouští, na jaké reporty se dívá, jaké konfigurační změny provádí a další.

#	Požadavek
	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 sumy, procentuálních vyjádření, číslování řádků, atd.) 16. Na základě ad hoc analýz budou vytvářena pravidla a korelace v produkčním systému analýzy bezpečnostních logů.
P.44	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. E-mailová komunikace – přístupy (oprávněné a neoprávněné) včetně geolokace, chyby systému atd.
P.45	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, elektronické pošty a pagingového systému (úspěšné i neúspěšné) 6. Zobrazení přehledu e-mailové komunikace ZZS (chyby, vytížení apod.) 7. Možnost dalšího rozvoje dle požadavků ZZS – otevřený systém
P.46	Součástí dodávky a implementace je definování, výchozí optimalizace a nastavení reaktivních opatření pro IS ZOS, el. poštu a pagingového systému.
P.47	Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí bude provozován na infrastruktuře (HW a systémový SW) požadovaný a dodávaný dle kap. 4.4.9 – Infrastruktura (HW) a systémový SW pro běh dodávaného SW a technologií.

Tabulka 7: Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí

4.4.5 Analytické nástroje ZOS pro vytváření bezpečnostních analýz

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

#	Požadavek
P.48	V rámci stávajícího analytického systému ORACLE BI (produkt SOS-BI), požadujeme rozšířit datovou základnu o import a normalizaci dat bezpečnostních logů z aplikací IS ZOS.
P.49	Vytvoření vzorových analýz nad bezpečnostními daty z hlediska pokusu o zneužití přístupu k jednotlivým aplikacím a modulům IS ZOS.
P.50	Vytvořené analýzy bude možné spouštět automaticky v nastavené periodě a výstupy distribuovat el. poštou definovaným uživatelům/správcům.
P.51	Uživatelé tohoto analytického nástroje pak budou moci vytvářet vlastní analýzy nad bezpečnostními záznamy aplikací IS ZOS a budou tak schopni definovat požadavky na konfiguraci aktivních incidentů v rámci systému analýzy bezpečnostních logů. Systém analýzy bezpečnostních logů bude moci být aktualizován na základě konkrétních požadavků správců systému IS OŘ zjištěných v analytickém nástroji pro ZOS.
P.52	Je vyžadováno stanovení základní kategorie možných bezpečnostních incidentů a tomu bude přizpůsobena struktura uložení dat bezpečnostních logů v databázi datového skladu tak, aby byla optimální pro dané analýzy. Uživatel tak bude mít k dispozici snadno použitelné údaje v datových kostkách (oblasti dat).
P.53	Je požadováno, aby data bezpečnostních logů byla navázána na stávající datové objekty, jako jsou události (hlášení) a pacienti. Tím musí být umožněno v analýzách vyhledávat anomální chování i na základě příslušnosti dat, ke kterým byl v aplikacích a modulech IS ZOS zachycen přístup. Například aktivní událost, výjezd a ošetření pacienta zajišťuje určitý okruh zaměstnanců, kteří jsou v události, výjezdu a v kartě pacienta zaznamenaní (dispečer, posádka, doktor). Přístup k datům od uživatele mimo okruh těchto zaměstnanců může naznačovat bezpečnostní incident, který by, obzvlášť při četnějším výskytu u daného uživatele, měl být sledován a řešen.
P.54	Požadované řešení má umožnit analýzy bezpečnostních logů i na základě anomálií v časovém sledu. Například zaměstnancovo (uživatelovo) nezvyklé navýšení počtu prohlížených a/nebo modifikovaných záznamů v určitém měsíci / týdnu / dni oproti ostatním měsícům / týdnům / dnům může naznačovat bezpečnostní incident.
P.55	Musí být možné analýzy na základě objemu dat, ke kterým uživatel modulu IS ZOS přistupoval oproti ostatním jeho kolegům ve stejné funkci (porovnání vůči standardnímu chování)
P.56	Možnost dohledání detailů všech přístupů k datům na základě znalosti konkrétní události, resp. existujícího bezpečnostního incidentu / nahlášeného úniku dat.
P.57	Analytické nástroje ZOS pro vytváření bezpečnostních analýz budou provozovány nově dodávané infrastruktuře (HW a systémový SW) v kap. 4.4.9 – Infrastruktura (HW) a systémový SW pro běh dodávaného SW a technologií). Dodavatel musí provozní požadavky dodávané technologie zohlednit v rámci navrhovaného HW a SW.

#	Požadavek
P.58	Není požadováno navýšení ani změna stávajících licencí. Součástí dodávky je systémová podpora na 5 let.

Tabulka 8: Analytické nástroje ZOS pro vytváření bezpečnostních analýz

4.4.6 Úpravy IS ZOS

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

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.

IS ZOS zaznamenává informace o činnostech v rámci tohoto IS a pro předpokládané zpracování takovýchto údajů externími systémy je třeba zajistit export těchto činností i mimo prostředí IS ZOS. Data zaznamenaná mimo prostředí IS ZOS nesmí již obsahovat konkrétní osobní údaje. Externí systémy pak mohou vyhodnocovat činnosti IS ZOS z poskytnutých dat a vyhodnocovat potenciální problémové chování uživatelů IS ZOS.

V rámci systému IS ZOS je požadováno zaznamenávat do externích systémů všechny operace s daty typu osobní údaj, a to jak jejich modifikace, tak jejich zobrazení.

V rámci IS ZOS dojde k úpravám, kdy bude možné přijímat i aletry upozorňující na bezpečnostní události, a to nejenom z uvedených bezpečnostních prvků, ale všech komponent zabezpečení (např. prostřednictvím systému vyhodnocení logů). Bude se jednat o aletry bezpečnostních událostí relevantních k provozu centrálního dispečinku a celého IS ZOS s kritickou důležitostí. Bezpečnostní aletry v rámci IS ZOS budou definovány a konfigurovány na základě požadavků ZZS a dle toho zpracovány. IS ZOS tedy bude částečně plnit funkci SOC.

Oprávněné osoby centrálního dispečinku budou mít možnost pomocí rozhraní v IS ZOS 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 (např. provoz dispečinku v ostrovním systému). Vlastní izolace bude realizována na bezpečnostních/komunikačních prvcích integrací z IS ZOS. 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.

#	Požadavek
Napojení na Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí (viz kap. 4.4.4)	
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 a vyhodnocení kybernetických bezpečnostních událostí (viz kap. 4.4.4).
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)

#	Požadavek
	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	**Telefonní ústředna** je integrována s IS ZOS prostřednictvím JTAPI / CTI rozhraní stávající telefonní ústředny. Vlastní přístup na server stávající telefonní ústředny je logován v rámci systémových prostředků OS. Data jsou tedy sbírána na systémové úrovni. Součástí dodávky je parsování logů, jejich analýza a ukládání do Systému analýzy bezpečnostních logů.

#	Požadavek
P.66	<u>Záznamový systém (REDAT)</u> 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 je parsování logů záznamového systému přes IS OŘ, jejich analýza a ukládání do Systému analýzy bezpečnostních logů.
P.67	<u>Integrace telefonie a radiofonie</u> 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.68	Aplikační SW na pracovištích ZOS: Vlastní přístup do OS na pracovištích ZOS bude logován v rámci systémových prostředků operačního systému. *Sbíraná data z operačních systémů a dalších technologie na pracovištích ZOS budou sbírána na systémové úrovni.*
Napojení IS OŘ na komunikační prvky – izolace dispečinku	
P.69	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.70	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). 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.
Infrastruktura (HW) a systémový SW pro úpravy IS ZOS	
P.71	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.

#	Požadavek
	Pokud některý z požadavků na úpravy IS ZOS bude vyžadovat realizaci přídavných komponent/systémů budou tyto provozovány na nově dodávané infrastruktuře (HW a systémový SW) v kap. 4.4.9 – Infrastruktura (HW) a systémový SW pro běh dodávaného SW a technologií).

Tabulka 9: Úpravy IS ZOS

4.4.7 Dodávka a implementace technologií 802.1x pro zabezpečení přístupů do LAN sítě

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

#	Požadavek
P.72	Pro zabezpečení přístupu do LAN/WAN sítě ZZS požadujeme implementaci technologie 802.1x na přístupových switchích centrálních lokalit (2x DC) a výjezdových stanovišť. Vlastní implementace bude využívat pro ověření zařízení a uživatelů autentizaci v rámci RADIUS serverů Microsoft NPS s integrací do jednotného Active Directory. Pro neautorizovaná zařízení a uživatele bude vytvořena v rámci jednotlivých lokalit i GUEST VLAN s definovaně omezeným přístupem do sítě. Minimální požadavky: 1. Integrace s RADIUS servery Microsoft NPS v rámci AD ZZS 2. Konfigurace všech stávajících LAN prvků umožňujících konfiguraci 802.1x v rámci WAN sítě ZZS 3. Vytvoření GUEST VLAN ve všech lokalitách WAN ZZS a její zabezpečení v rámci dostupných technologií v dané lokalitě 4. Vzorová konfigurace PC a NB pro 802.1x 5. Konfigurace speciálních zařízení (Tiskárny apod.) bez podpory 802.1x 6. Testovací provoz implementace bez reálného odepření přístupu včetně vyhodnocení provozu 7. Přechod do provozního režimu včetně odepření přístupu neautorizovaným zařízením
P.73	Správce infrastruktury musí být informován o všech neoprávněných pokusech s maximálním rozsahem informací o takovém pokusu (Datum a čas, MAC adresa, prvek, port apod.). Informace musí být možné získávat online při výskytu nebo reportem za dané časové období.
P.74	Součástí implementace bude i systém logování výskytu jednotlivých zařízení (MAC adres) v rámci WAN ZZS. Systém bude umožňovat reporting nejenom MAC adres, ve kterých lokalitách, prvcích a portech se daná MAC adresa vyskytovala, ale též od kdy do kdy byla připojena a jakou IP adresu v rámci WAN ZZS obdržela. Reportovací systém bude udržovat databázi výskytu MAC adres a přidělených IP adres jednotlivým MAC adresám s časovou závislostí. Musí být tedy realizována integrace s používanými DHCP servery Microsoft. Reportovací sytém musí umožňovat získávat přehled i o připojených zařízeních do aktivních prvků, které nebudou podléhat autentizaci prostřednictvím 802.1x.
P.75	Pro centrální lokality bude třeba realizovat i dodávku těchto aktivních prvků typu přepínač: Pro lokalitu Hradecká centrální redundantní L3 prvek pro segmentaci sítě. Po centrální lokality 2ks přístupových přepínačů. Pro lokalitu Hradecké centrální redundantní prvek L3

#	Požadavek
	1. Ethernetový spravovatelný přepínač L3 pro instalaci do racku 2. Min. 24x 1/10/25 GbE SFP/SFP+/SFP28 a 4x 40/100 GbE Uplink QSFP+/QSPF28 neblokovaných portů. 3. Propustnost min. 2 Tbps, neblokovaná architektura a packetový výkon 1Bpps. Velikost sdíleného bufferu min. 36 MB. 4. Podpora IPv4 a IPv6. 5. L3 routing: Static, OSPFv2/OSPFv3, Minimální počet host IPv4 routes 200k a First Hop Redundancy Protocol (např. VRRP nebo HSRP), podpora multicast routingu (IGMP snooping, PIM SM, PIM SSM) a podpora virtualizace směrovacích tabulek – např. Virtual Routing and Forwarding (VRF) 6. Podpora Jumbo Frames, min. 9 kb, podpora agregace portů (LACP) s využitím dvou switchů ve stacku (jedna agregace přes dva switche). 7. Podpora min. 1000 VLAN, podpora instance spanning-tree protokolu per VLAN a IEEE 802.1w - Rapid Spanning Tree Protocol 8. 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. 9. QoS (prioritizace služeb), Minimální počet HW QoS 8 front. QoS - Strict Priority Queue, classification – ACL, DSCP, CoS based, marking - DSCP, CoS, Policing, Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) 10. Detekce protilehlého zařízení s podporou CDP a LLDP. 11. Šifrování na L2 dle IEEE 802.1AE (MACsec 256-bit) na všech portech (plně kompatibilní s centrálním L3 prvkem v lokalitě Bláhovka - C9500-24Y4C-A). 12. Možnost konfigurace mirroring portu – SPAN pro monitoring provozu konkrétního portu/portů nebo VLAN. Možnost realizace technologie remote SPAN mirroring. 13. Monitorování aplikačních toků prostřednictvím technologie NetFlow nebo ekvivalentní (všech packetů) s možností definice klíčových atributů a parametrů monitorovaných toků s exportem dat ve formátu NetFow v9 nebo IPFIX – kompatibilní s provozovaným FlowMon Collectorem. 14. Redundantní napájení. 15. Podpora CLI (Telnet/SSHv2) – autentizace local a RADIUS, SNMP v2 a v3 management, Web UI, včetně omezení přístupu na management z definovaných adres a subnetů, odesílání zpráv na syslog server. 16. Propojení switchů do jednoho stacku (přepínače se chovají jako jeden z pohledu managementu i připojených zařízení – včetně automatického loadbalancingu) vysokorychlostním redundantním datovým propojením 2x min. 100Gbps včetně kabelů. (1 m) S možností využití max. 2 per switch uplinkových/standardních portů nebo vyhrazených stack portů. Veškerý potřebný drobný materiál (kabely, SFP+, QSFP, stack cable apod.) k optimálnímu propojení a redundantnímu stacku. 17. Požaduje se dodávka těchto modulů pro každý ze switchů stacku (mimo materiál pro propojení do stacku): • 4ks SFP-10G-SR 10GBASE-SR SFP Module • 4ks SFP-25G-SR 25GBASE-SR SFP28 Module for MMF 18. Součástí dodávky musí být instalace a konfigurace na místě včetně aktualizací všech firmware na poslední aktuální a stabilní verze a součinnost při zařazení do stávajícího

#	Požadavek
	prostředí. Součástí implementace bude i návrh procesu zařazení centrálního L3 prvku do infrastruktury z pohledu minimalizace výpadků a negativního ovlivnění operačního řízení ZZS a vlastní realizace zařazení prvku do infrastruktury, tak aby dodaný prvek plně převzal funkce centrálního L3 prvku. Vlastní zařazení prvku do infrastruktury bude prováděno harmonogramu a v čase dle požadavků Zadavatele. Součástí požadované konfigurace mohou být i rozšířené funkce/vlastnosti prvku požadované v technické specifikaci. 19. implementace (montáž, instalace, konfigurace, seznámení s funkcionalitami a obsluhou, dokumentace) 20. veškerý potřebný drobný materiál (kabely apod.) 21. Záruka min. na 5 let - technická podpora a servis (24x7x365), jediné kontaktní místo pro hlášení poruch pro všechny HW i SW komponenty dodávaného systému. Zahájení servisních prací do 4 hodin a na základě identifikace závady doručení náhradního dílu do následujícího pracovního dne a následná instalace a konfigurace prvku (pokud to bude typ závady vyžadovat). Pro centrální lokality požadujeme dodávku přístupových aktivních prvků typu přepínač s podporou 802.1x. Jedná se celkem o 2 ks přepínačů (switchů) které musí plnit následující min. parametry (každý jeden switch): 1. provedení rack mount 2. ethernetový spravovatelný přepínač vrstvy 2 3. min. 24x 10/100/1000Mbs PoE+ TP portů a 4 x 1Gportů SFP 4. minimální propustnost přepínacího subsystému min. 56Gbps 5. možnost zapojení více switchů do jednoho stacku (přepínače se chovají jako jeden z pohledu managementu i připojených zařízení – včetně automatického load balancingu), kapacita propojení 80Gbps – součástí dodávky nejsou požadovány technické prostředky (porty/modul) pro realizaci vlastního stacku, 6. podpora VLAN (min. 1000), 7. software podporující CLI (Telnet/SSH), SNMP management, včetně omezení přístupu na management z definovaných adres a subnetů, 8. bezpečnost – port security a implementace 802.1X, automatické zařazování do VLAN 802.1x – RADIUS server Windows AD, 9. podpora „jumbo" rámců, 10. detekce protilehlého zařízení (např. CDP nebo LLDP), 11. podpora IPv4 a IPv6, 12. implementace (montáž, instalace, konfigurace, seznámení s funkcionalitami a obsluhou, dokumentace) 13. veškerý potřebný drobný materiál (kabely apod.) 14. Záruka min. na 5 let.
P.76	Dodávka 2 ks přepínačů L2 do centrálních lokalit s min. požadavky: 1. Obecné technické požadavky na poptávaný přepínač a. L2 přepínač b. Podpora IEEE 802.3ad

#	Požadavek
	c. Podpora IEEE 802.1q d. Podpora IEEE 802.1ab e. Možnost propojení s prvkem podporující IEEE 802.1s f. Podpora IEEE 802.1w g. Podpora ACL IPv4 h. Podpora 802.1x i. Podpora MAB j. Podpora Radius CoA k. Podpora Radius Accounting l. Podpora ARP inspekce m. Podpora IGMP a DHCP snooping n. Podpora Jumbo Frame o velikosti alespoň 9000B o. Podpora SPAN p. Podpora administrátorského přístupu pomocí Telnet, SSH a HTTPS q. Podpora REST API pro konfiguraci a monitoring prvku r. Podpora SNMP v1/v2c/v3, Syslog (včetně možnosti komunikace pomocí TCP), Radius a TACACS+ protokolu pro autentizaci administrátorů 2. Specifické technické požadavky na poptávaný přepínač a. Minimálně 48x 10/100/1000 RJ-45 a 4x 1000/10000 SFP+ síťové porty b. Podpora 802.3af/at na 24x 10/100/1000 RJ-45 portech c. PoE budget alespoň 370W d. Samostatný RJ-45 konzolový a USB port e. Velikost maximálně 1RU f. Minimální přepínací kapacita 170 Gbps g. Propustnost minimálně 2500 Mpps h. Minimální počet podporovaných VLAN alespoň 4000 i. Napájecí zdroj a přívodní elektrický kabel pro CZ jsou součástí dodávky j. Proudění vzduchu ze strany do zadní částí přepínače k. Podpora duálního firmwaru 3. Požadavky na podporu přepínačů výrobcem a. Nativní podpora HW výrobce s možností výměny vadného HW do třiceti dnů a to až pět let po ohlášení konce prodeje přepínače výrobcem b. Placená podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7
P.77	Dodávka 13 ks přepínačů L2 na výjezdové základny s min. požadavky: 1. Obecné technické požadavky na poptávaný přepínač a. L2 přepínač b. Podpora IEEE 802.3ad c. Podpora IEEE 802.1q d. Podpora IEEE 802.1ab e. Možnost propojení s prvkem podporující IEEE 802.1s f. Podpora IEEE 802.1w g. Podpora ACL IPv4

#	Požadavek
	h. Podpora 802.1x i. Podpora MAB j. Podpora Radius CoA k. Podpora Radius Accounting l. Podpora ARP inspekce m. Podpora IGMP a DHCP snooping n. Podpora Jumbo Frame o velikosti alespoň 9000B o. Podpora SPAN p. Podpora administrátorského přístupu pomocí Telnet, SSH a HTTPS q. Podpora REST API pro konfiguraci a monitoring prvku r. Podpora SNMP v1/v2c/v3, Syslog (včetně možnosti komunikace pomocí TCP), Radius a TACACS+ protokolu pro autentizaci administrátorů 2. Specifické technické požadavky na poptávaný přepínač a. Minimálně 24x 10/100/1000 RJ-45 a 4x 1000/10000 SFP+ síťové porty b. Podpora 802.3af/at na 12x 10/100/1000 RJ-45 portech c. PoE budget alespoň 180W d. Samostatný RJ-45 konzolový a USB port e. Velikost maximálně 1RU f. Minimální přepínací kapacita 120 Gbps g. Propustnost minimálně 180 Mpps h. Minimální počet podporovaných VLAN alespoň 4000 i. Napájecí zdroj a přívodní elektrický kabel pro CZ jsou součástí dodávky j. Proudění vzduchu ze strany do zadní částí přepínače k. Podpora duálního firmwaru 3. Požadavky na podporu přepínačů výrobcem a. Nativní podpora HW výrobce s možností výměny vadného HW do třiceti dnů a to až pět let po ohlášení konce prodeje přepínače výrobcem b. Placená podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7
P.78	Instalace a konfigurace dodávaných komponent a celkového řešení. Součástí konfigurace je zařazení dodávaných komponent do monitoringu infrastruktury a monitoringu síťového provozu. Instalace a konfigurace včetně aktualizací všech firmware na poslední aktuální a stabilní verze. Všechny centrální prvky a jedna vzorová vzdálená lokalita budou instalovány na místě. Zadavatel následně zajistí rozvoz a instalaci ostatních vzdálených lokalit, přičemž Uchazeč bude pro tyto účely v době instalace dostupný pro vzdálenou podporu a kontrolu funkčnosti. Vzorová vzdálená lokalita bude vybrána v rámci realizace prováděcího projektu na základě požadavku Zadavatele.

Tabulka 10: Dodávka a implementace technologií 802.1x pro zabezpečení přístupů do LAN sítě

4.4.8 Zajištění šifrování v rámci komunikační sítě

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

Je požadována realizace zabezpečené komunikační infrastruktury jak na bázi VPN s využitím šifrovacích algoritmů dle doporučení ZKB. Jedná se tedy o dodávku řešení VPN WAN sítě při využití veřejných

internetových připojení a zajištění zabezpečené komunikace pomocí technologie MacSec na úrovni optického propojení lokalit bez ztráty propustnosti propojení.

#	Požadavek
P.79	Pro zajištění šifrování v rámci komunikační sítě požadujeme následující dodávky: 1. Zajištění šifrování na L2 FO propojení 2. Zajištění šifrování v rámci WAN sítě ZZS.
P.80	Pro zajištění šifrování v rámci WAN sítě požadujeme realizaci WAN sítě na bázi protokolu IPSec s šifrovacími algoritmy AES256, IKEv2. Struktura WAN sítě bude obsahovat dvě centrální lokality osazené centrálními zařízeními celkem 2 kusy (viz následující požadavek) a celkem 16 lokalit osazených zařízeními pro lokality. V rámci realizace propojení lokalit bude využito dynamické směrování provozu v závislosti na dostupnosti technologií lokalit a směrování provozu do dané lokality. Např. systémy operačního řízení budou směrovány do centra sítě A a internet a ostatní technologie do centra B a v případě výpadku některé technologie směrování provozu na funkční lokalitu.
P.81	Konfigurace bude provedena minimálně v následujícím rozsahu: 1. definice IP rozsahů, komunikační matice 2. upgrade firmware firewalů zapojených do SD-WAN na aktuální verzi operačního systému podporovanou výrobcem firewallu 3. vytvoření a konfigurace virtuálních domén 4. konfigurace routování a prostupů mezi virtuálními doménami, v případě potřeby řešit NAT pro překryvné sítě 5. konfigurace dynamických IPSec VPN 6. konfigurace dynamického routování BGP 7. konfigurace firewall policy 8. konfigurace SD-WAN policy 9. konfigurace logování na centrální místo 10. zaškolení správců v rozsahu minimálně 8 hodin 11. dokumentace
P.82	Minimální požadavky na prvek v lokalitách WAN ZZS (15 ks): 1. Základní technické požadavky a. Požadujeme platformu postavenou na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, akcelerace IPsec VPN, porovnávání se signaturovou databází, ...) b. Celá dodávka musí obsahovat všechny HW komponenty a licence na dobu 5 let. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány. c. Požadujeme dodání zařízení ve formátu HW appliance o velikosti desktop

#	Požadavek
	d. Možnost rozšíření platformy i další prvek typu NGFW jehož cílem bude zajišťování sdílení telemetrických informací, vizualizace stavu sítě, zařízení a klientů, přičemž cele řešení musí být podporováno výrobcem. e. Možnost o rozšíření platformy pro sběr logů a grafického reportingu včetně oboustranné komunikace (tím se rozumí minimálně odeslání a zpětné načítání logů pro účel vizualizace), přičemž zde musí existovat garantovaná podpora funkcionality 2. HW parametry a. Počet síťových rozhraní RJ45 10/100/1000 - min 8x b. Dedikovaný konzolový port – min 1x c. USB port umožňující připojení USB flash paměti pro zálohování konfigurace, zároveň umožňující připojení USB modemu pro záložní připojení internetu – min 1x d. Minimálně 2 x SFP port. e. Podpora redundantního napájení 3. Výkonnostní parametry a. Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B- min 9000 Mbps, 9000 Mbps, 6000 Mbps b. Latence firewallu (64 B UDP paket) - max 5 mikro sec c. Počet naráz otevřených spojení – min 1 250 000 d. Počet nových spojení za sekundu - min. 40 000 e. Počet firewall pravidel až 5 000 f. Podpora virtualizace (min 10 virtuálních kontextů) g. Podpora funkce bezdrátový kontrolér – min 90 AP h. Podpora funkce integrovaný switch controller – podpora min. 12 switchů 4. Networking a Vysoká dostupnost (HA) a. Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky a IPsec SAs mezi nódy v clusteru b. HA musí podporovat až 4 nódy v HA režimu c. Režim fungování L2 – transparentní režim, L3 – NAT/Router d. Podpora VLAN e. Podopora multicast, vytváření politiky pro multicast routování f. Podpora 802.3ad link aggregation g. Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading h. Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace i. Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP j. Policy-based routing k. Podpora uplatňování základních pravidel pro kontrolu na přístupové vrstvě (NAC pravidla, politiky) l. Zařízení musí podporovat možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky (SD-WAN).

#	Požadavek
	m. Funkce SD-WAN nesmí být licenčně omezeno. V rámci nabízeného řešení musí být dodáno v podobě, jenž umožňuje neomezené využívání i v případě, že dojde k nárůstu počtů zařízeních komunikující skrze SW-WAN do internetu, tak i v případě, že dojde k navýšení počtu konektivit a jejich rychlosti. n. Integrované SD-WAN řešení musí podporovat podle dokumentace výrobce min. 200 členů virtuálního rozhraní, které sdružuje konektivitu a jsou na něj uplatněna pravidla provozu a routingu. 5. Funkce SSL VPN a. Nabízené řešení musí podporovat možnost připojení klientů do VPN pomocí proprietární SSL VPN. Aplikace pro do VPN musí být podporována nejběžnějšími operačními systémy, jako například: Windows, macOS, Linux, Android nebo iOS. b. Podpora bez klientského připojení do VPN na úrovni webového portálu, pomocí standardního internetového prohlížeče. c. Možnost zabezpečení připojení do VPN vynucením dvou faktorového ověření. Například pomocí emailu, SMS, hardwarovou klíčenkou, nebo proprietární aplikace dostupná pro Android i iOS. d. Zařízení musí umožňovat rozšíření pro využití dostupného dvou faktorového ověření e. Zařízení musí být dodáno s min. 2 licencemi pro případné vyzkoušení dvou faktorového ověření f. Vynucení ověření klientského certifikátu pro zvýšení zabezpečení. g. Minimální počet současně navázaných SSL VPN tunelů: 180 h. Minimální propustnost SSL VPN: 850 Mbps 6. Funkce IPsec VPN a. podpora site-to-site VPN b. podpora klientských VPN c. dostupnost VPN klienta pro koncové stanice (Windows, MacOS) z veřejně dostupných webových stránek d. funkce klientských IPSec VPN nesmí být licencovaná na počet uživatel. V opačném případě požadujeme dodání neomezené licence. e. Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 180 f. Minimální počet klientských IPSEC VPN tunelů: 2200 g. propustnost IPSec VPN min. 6 Gbps (měřeno při AES256-SHA256) h. podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování i. podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování j. podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace k. Podpora VXLAN l. Podpora L2TP, PPTP, GRE m. podpora dynamických routovacích protokolů OSPF, BGP ve VPN IPsec 7. UTM funkce a. Funkce detekce aplikací na L7 (Application Control)

#	Požadavek
	i. detekce známých aplikací na základě signatur ii. signaturový database automaticky aktualizované výrobcem iii. alespoň 4 000 podporovaných aplikací iv. pro populární cloudové aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) požadujeme pokročilé akce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login atd. (relevantní k dané aplikaci) v. možnost tvorby vlastních signatur vi. detekované aplikace je možné: povolit, monitorovat, blokovat vii. na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci viii. funkce detekce aplikací se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně požadujeme možnost využití v rámci tzv. NGFW pravidel popsaných výše. b. Funkce detekce a potlačení narušení (IPS/IDS) i. minimální propustnost IPS inspekce 1,2 Gbps ii. signatury automaticky aktualizované výrobcem iii. alespoň 11 000 rozpoznávaných hrozeb (signatur) definovaných výrobcem iv. možnost tvorby vlastních signatur v. funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům vi. funkce tzv. fail-open - při přetížení IPS je možné definovat, zda dojde k blokaci nebo propuštění provozu c. Funkce antivirové kontroly i. ochrana před škodlivým kódem (malware, trojské koně apod.), včetně ochrany před polymorfním kódem ii. signatury automaticky aktualizované výrobcem iii. požadujeme AV kontrolu rozšířenou o inspekci tzv. sandbox technikou, poskytovanou formou služby dodávané výrobcem FW (licence musí být součástí dodávky) iv. možnost rozšíření o inspekci tzv. sandbox technikou formou lokálné HW appliance stejného výrobce v. deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 800 Mbps vi. funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. vii. Podpora služby výrobce, která umožní detekovat malware, který byl objevený v době od poslední aktualizace AV signaturové databáze pomocí globální a rychle se aktualizující databáze hashů viii. Funkce odstranění škodlivého aktivního obsahu z dokumentů kancelářských aplikací. d. Funkce kategorizace webových stránek

#	Požadavek
	i. založená na centrálně spravované databázi výrobce ii. minimálně 50 filtračních kategorií iii. možnost definice vlastních kategorií iv. možnost definice vlastních seznamů zakázaných URL v. kategorizace musí zahrnovat i české a slovenské internetové stránky e. Funkce blokování video obsahu portálu YouTube i. založená na centrálně spravované databázi výrobce ii. minimálně 9 filtračních kategorií iii. možnost definice vlastních kanálů na základně channel ID f. Funkce DNS filtru i. Možnost blokovat DNS dotazy na základě příslušnosti k URL kategorii (obdobné kategorie jako u předchozího bodu) ii. Možnost definovat vlastní tzv. deny-list domén iii. Možnost přesměrovat komunikace se zakázanými doménami na vlastní portal/URL iv. Možnost importu seznamu blokovaných domén do DNS filtru v. Detekce a blokování komunikace do botnet sít g. Funkce ochrany před únikem citlivých informací (DLP) i. možností analýzy běžných typů dokumentů a protokolů ii. možnost definice pravidel min. na základě regulárních výrazů, watermarkovacího nástroje a typu kontroly typu file checksum h. Funkce blokace stahování konkrétních typů souborů i. možnosti zablokovat stahování souborů s konkrétními typy, jako např. MSI, EXE... ii. funkce blokace stahování konkrétních typů souborů se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. i. Emailový antispamový modul i. jednoduchá antispamová a antivirová inspekce elektronické pošty j. Podpora SSL dekrypce i. podpora SSL dekrypce a inspekce pro ochranu jak koncových zařízeních, nebo serverů ii. funkce SSL dekrypce se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. iii. zařízení musí u SSL inspekce dosáhnout min. propustnost 700 Mbps k. Podpora pravidel pro obranu proti útokům typu DoS i. zařízení musí umožnit uplatnit pravidla proti DoS útokům na základě politik, které se aplikují na konkrétní interface zařízení. ii. podpora detekce anomálií na 3. a 4. vrstvě iii. podpora např. TCP SYN FLOOD, ICMP FLOOD, SCTP SRC SESSION iv. funkce musí umožňovat provoz nejen blokovat, ale i sledovat pro možnost orientace na síti l. Explicitní proxy i. podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP)

#	Požadavek
	ii. podpora transparentního ověřování uživatel proti MS AD protokolem Kerberos iii. funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta iv. Funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatel na terminálovém server
	8. Firewall
	a. Možnost nastavovat firewall politiku na základě geografických údajů b. Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem c. Možnost snadné integrace cloudové služby. Minimálně na: MS Azure, Amazon Web Services, Google Cloud d. Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru e. Viditelnost do provozu na aplikační úrovni f. Možnost dynamického stahování externích seznamů IP adres a jejich následné použití ve firewall policy g. Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo). h. Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu i. Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření. j. Traffic Shaping, QoS s podporou priroritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii k. Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu l. Podpora funkce reverzní proxy m. Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů n. Administrátorské účty mohou být volitelně zabezpečený pomocí dvou faktorového ověření
	9. Integrovaný kontroler bezdrátových sítí (Wi-Fi)
	a. Wifi kontroler integrovaný do NGFW platformy b. Bezdrátová síť (SSID) může být reprezentována virtuálním síťovým rozhraním – provoz tunelován z AP do kontroleru c. podpora bezpečnostních profilů (AV, AppControl, Webfilter, DLP) přímo na wifi kontroleru d. podpora SSL dekrypce uživatelského provozu přímo na wifi kontroleru e. Podpora wifi přístupových bodů stejného výrobce s výrobcem FW řešení

#	Požadavek
	f. Možnost volby z různých modelů (802.11abgn, 802.11ac, 802.11ac wave2, indoor, outdoor, WiFi 6) g. Podpora BSS Coloring h. On-wire rogue AP detekce a mitigace i. Podpora fast-roamingu (802.11 k,v,r) j. podpora více PSK u jednoho SSID k. podpora IPSEC tunelu pro šifrování data plane (uživatelských dat) l. Podpora WPA3 protokolu 10. Integrovaný switch kontroler a. Zařízení musí podporovat switch kontroler jenž umožní spravovat switche výrobce z jednoduchého GUI b. Možnost správy VLAN c. Spolu s NAC politikami musí nabídnout možnost automatické přiřazení VLAN pro konkrétní zařízení či skupinu zařízeních d. Z integrovaného switch kontroleru musí být obsluha schopna pomocí GUI jednoduše definovat VLAN na konkrétní port e. V případě správy switche s funkcí PoE musí být v GUI možnost resetování PoE pro vzdálený restart zařízení 11. Multi-tenance (virtualizace) a. Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů atp. b. Součástí dodávky musí být licence na min. 10 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech) c. Každý virtuální kontext je zároveň samostatným wifi kontrolerem d. Podporou izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálnícn kontextů) 12. Management a. FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici b. Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě c. Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury) 1. Požadavky na podporu přepínačů výrobcem a. Nativní podpora HW výrobce s možností výměny vadného HW do třiceti dnů a to až pět let po ohlášení konce prodeje přepínače výrobcem b. Placená podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 2. Požadavky na dodávku:

#	Požadavek
	a. Dodávka aktivních prvků dle specifikace na místa/lokality určené zadavatelem na území Královéhradeckého kraje (15 lokalit). b. Propojovací kabely a moduly potřebné k realizaci dodávky c. Všechny potřebné softwarové licence. d. Fyzická instalace přepínačů do rozvaděče a jejich konfigurace, podle požadavků zadavatele i přenos stávající konfigurace. e. Upgrade firmware na aktuální verzi.
P.83	Minimální požadavky na WiFi AP v lokalitách WAN ZZS (17 ks): 1. Formát AP: indoor s interními anténami 2. Příslušenství k montáži na zeď/strop/T-Rail 3. Počet rádií: minimálně 3 pro přenos v pásmech 2,4 a 5GHz a samostatné monitorovací rádio 4. Minimálně 2x2 MIMO 5. Dedikované rádio pro analýzu okolního provozu 6. Dedikované Bluetooth/ZigBee rádio pro lokalizační služby 7. Současná podpora 2,4 GHz a 5GHz pásma 8. Podpora standardu 802.11ax 9. 2x 10/100/1000 Base-T RJ45 uplink porty s možností sestavení LAG 10. 1x USB port typu A 11. 1x seriový port RJ45 12. Počet SSID: až 16 13. Cellular Co-existence 14. Podpora BSS Coloring 15. Podpora TWT (Target Wake Time) 16. Spektrální analýza přímo na AP 17. Možnost zachytávání paketů na AP pro jejich analýzu 18. Provoz všech rádií i při napájení pomocí 802.3af 19. Podpora všech následujících standardů - 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11w, 802.11ac, 802.11ax, 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az 20. Kensigton lock 21. Nativní podpora HW výrobce s možností výměny vadného HW do třiceti dnů a to až pět let po ohlášení možnosti objednat nabízené AP 22. Placená podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 Součástí dodávky je: 1. Fyzická montáž a WiFi AP na místa/lokality určené zadavatelem na území Královéhradeckého kraje (16 lokalit). 2. Konfigurace WiFi AP, napojení na kontrolér bezdrátové sítě – funkci řídícího prvku sítě tzv. WiFi kontroléru zajišťuje stávající FireWall FortiGate 100F.

#	Požadavek
P.84	Implementace management nástroje a napojení všech prvků do managementu: 1. Dodávka systému pro centrální správu dodávaných NGFW, přepínačů a AP a napojení všech dodávaných prvků do tohoto systému centrální správy. 2. Hlavní požadavky a. Musí se jednat o virtuální appliance s podporou VMware, KVM a Hyper-V b. Množství spravovaných aktivních NGFW zařízení (fyzických nebo virtuálních) musí být minimálně 10 c. Množství spravovaných přepínačů a AP není licenčně omezeno d. Možnost škálovatelného navýšení množství spravovaných NGFW zařízení na základě přidání další licence e. Podpora minimálně 4 vNIC portů f. Možnost zapojit řešení v režimu vysoké dostupnosti g. Možnost volitelně zapnout logovací funkce h. Plná integrovatelnost s poptávaným nástrojem pro analýzu dat z NGFW zařízení i. Možnost rozdělení zařízení na oddělené administrativní sekce (každý NGFW nebo virtuální kontext NGFW může být v jiném administrativním kontextu) j. Pokud firewall, který je centrálně spravován podporuje virtuální kontexty, tak musí být možné v spravovat je odděleně jako by se jednalo o fyzický oddělené firewally k. Možnost správy administrátorských účtů na základě profilů, kde dle přiřazeného profilu bude mít daný administrátor oprávnění vidět nebo spravovat zařízení v různých administrativních kontextech l. Podpora SNMPv2, SNMPv3 m. Podpora API n. Správa přes webové rozhraní HTTPS a SSH CLI o. Administrátorské účty musí být možné konfigurovat lokálně nebo na vzdáleném serveru (LDAP, RADIUS, Tacacs+) p. Podpora statického směrování q. Podpora logování na externí Syslog server r. Každý administrativní celek musí mít možnost mít vlastního administrátora, který nebude mít přístup do jiných administrativních celků 3. Požadavky na centrální správu a. Možnost nastavení centrálních policy pro všechny zařízení, sdílení společné jedné politiky na více zařízeních, aplikace bloků konfigurace na vybráná místa politiky b. Možnost vytváření skupin zařízení na základě jejich geografické polohy nebo logického členění c. Podpora vytváření vzorů konfigurací pro nově instalovaná zařízení d. Možnost vytváření a aplikace konfiguračních skriptů pro spravované firewally, možnost spouštět skripty i ručně nebo automaticky při přidání nového zařízení - autokonfigurace e. Revize konfigurací spravovaných firewallů jestli nejsou pravidla duplikována f. Ukládání konfiguračních revizí a porovnávání změn mezi nimi

#	Požadavek
	g. Podpora centrálního upgradu firmwaru spravovaných firewallů h. Podpora správy licencí spravovaných firewallů i. Podpora stahování signatur přes centrální management pro spravovaná zařízení j. Podpora centrální konfigurace a monitoring VPN sítě, použití běžných topologií sítě (hvězda, full-mesh, dual hub), podpora vytváření VPN zabezpečených certifikáty - interní certifikační autorita, automatická aplikace existující VPN konfigurace na nově přidaná zařízení k. U monitoringu IPsec VPN možnost manuálního vypnutí a povolení tunelu l. Podpora kompletní konfigurace a dohledu nad poptávanými přepínači m. Podpora ZTP instalace nových NGFW a přepínačů n. Schopnost analyzovat provoz NGFW a nabídnout tvorbu bezpečnostních politik na základě analýzy provozu o. Dynamické zobrazení topologie spravovaných zařízení p. Možnost nastavení módu, kdy bude hlavní administrátor schvalovat změny v konfiguraci firewallů ještě před tím, než se aplikují q. Požadavky na centrální management poptávaných bezdrátových AP r. automatická nebo manuální autorizace AP na základě auto discovery mechanismu s. možnost kompletní konfigurace SSID, systémového a rádiového nastavení a autentizace uživatelů t. zobrazení stavu AP včetně jim přiřazených SSID, asociovaných klientů interferujích SSID včetně síly signálu intereferujícího SSID vůči konkrétnímu AP u. možnost vyhledávání, v jednotném management rozhraní, konkrétních zařízení nebo uživatel na základě minimálně následujících parametrů: IP adresa, MAC adres, uživatelské jméno v. možnost automatické aktualizace operačního sytému AP po jeho registraci k firewall platformě w. možnost automaticky registrovat AP po jeho registraci k firewall platformě na servisní portál výrobce AP x. možnost manuální karantény konkrétního uživatele z jednotného management rozhraní, která zamezí další možnosti připojení se uživatele k bezdrátové síti y. možnost hromadného upgrade firmware AP z jednotného management rozhraní 4. Obecné požadavky na správu poptávaných přepínačů a. Efektivní správa poptávaných přepínačů z hlediska konfigurace, zabezpečení provozu na přístupové vrstvě sítě včetně logování provozu pro zefektivnění jejich nasazení a následné správy b. Management platforma musí umožnit grafické znázornění fyzické a logické topologie spravovaných přepínačů až do úrovně připojeného klienta včetně identifikace typu koncového zařízení c. Management platforma musí umožnit zobrazení a vyhledávání koncových zařízení připojených ke spravovaným přepínačům ve fyzické i logické topologii d. Management platforma musí umožnit provést segmentaci provozu v L2 doméně (oddělit provoz jednotlivých stanic v L2 síti) bez nutnosti dodatečné enkapsulace datového toku z jednotlivých stanic do přenosových tunelů na externí zařízení

#	Požadavek
	e. Management platforma musí umožnit automatickou zálohu konfigurace přepínačů a možnost její migrace na nový přepínač v případě výměny přepínače f. Management platforma musí umožnit poskytnout údaje o vytížení jednotlivých přepínačů jak z pohledu CPU a paměti, datových toků na jednotlivých portech, chybovosti provozu na portech a také umožnit software otestovat připojenou kabeláž g. Management platforma musí umožnit spravovat karanténu koncových zařízení vyvolanou administrátorem nebo automaticky na základě bezpčnostního incidentu zjištěného management platformou, externím analytickým nástrojem nebo samotným administrátorem sítě h. Management platforma musí umožnit hromadnou správu více přepínačů najednou pro akce jako je například upgrade jejich operačního systému a registrace jejich podpory i. Management platforma podporuje administrátorský přístup pomocí SSH/HTTPS a také je z ní je možné SSH přístup na samotné přepínače j. Management platforma musí umožnit použití REST API pro konfiguraci a monitoring systému k. Management platforma musí umožnit jednoduchou aktualizaci konfigurace nové přepínače v případě výměny prvků 5. Požadavky na podporu výrobce a. Podpora výrobce v režimu 24x7 na systém i konfiguraci je součástí nabídky
P.85	Dodávka systému pro sběr logů ze všech dodávaných síťových prvků: 1. Základní technické požadavky a. Nástroj pro bezpečnostní analýzu logů z NGFW zařízení (poptávané souběžně s produktem pro analýzu dat z NGFW) se schopnostií jejich korelace včetně možnosti ukládání logů b. Funkce analýzy logů s využitím Indicators of Compromise a Virus Outbreak Detection. Dodavatel dodá případné nutné licence pro tyto funkcionality c. Podpora automatizace reakcí na bezpečnostní události detekované nabízeným řešením směrem k NGFW zařízení přímo v grafickém rozhraní nabízeného řešení včetně potřebné licence pro takovou funkci d. Virtuální appliance pro platformu VMWare, Microsoft Hyper-V, KVM (fyzické zařízení není přípustná alternativa) e. Možnost nativní integrace s poptávaným zařízením typu NGFW, které bude sloužit jako zdroj dat pro analýzu f. Alokovatelná kapacita dlouhodobého úložiště logů je alespoň 3TB a minimální limit pro množství přijatých logů k analýze za jeden den je alespoň 5GB (licence pro takovou denní kapacitu je součástí dodávky řešení) g. Možnost zvýšení denní kapacity analyzovaných logů nad 5GB za den pomocí dodatečné licence h. Minimálně 4x vNIC i. Možnost provozovat poptávané řešení jako prosté uložiště logů bez jejich další analýzy z dalších zařízení zákazníka

#	Požadavek
	j. Možnost logické segmentace poptávaného nástroje s možností izolace jednotlivých segmentů z hlediska jejich administrace a zdroje dat 2. Požadavky na logování, vizualizaci a reporting a. Musí se jednat o centrální logovací prvek pro všechny NGFW firewally, poptávané přepínače a AP b. Musí umět ukládat jakékoliv Syslog zprávy c. Vizualizace provozu nad všemi firewally d. Možnost dostat se z vizuálního zobrazení proklikem na konkrétní logy e. Realtime a historický náhled do logů f. Samostatná sekce týkající se hrozeb v síti g. Podpora prohlížení statistických údajů nad logy h. Podpora reportů nad logy ve formátu HTML/CSV/XML/PDF i. Generování reportů v pravidelných intervalech j. Předefinované vzory pro reporty na nejčastější použití k. Možnost vytváření vlastních reportů na základě konkrétních SELECT dotazů do databáze l. Možnost úpravy reportů do vlastního designu – vlastní loga, texty, úprava hlavičky m. Možnost tvorby komplexních reportů (Top X uživatelů/zařízení dle množství zjištěných hrozeb, přeneseného provozu atd.) nad analyzovanými daty z grafického rozhraní poptávaného nástroje n. Event Management - upozorňování na důležité informace z logů – emailem, snmp trapy nebo syslog zprávou o. Předvytvořený dashboard pro využití dohledovým centrem p. Možnost customizace rozhraní pro NOC/SOC dle konkrétních požadavků na dohlížené informace 3. Požadavky na management a. Plnohodnotná správa pomocí grafického rozhraní a CLI b. Podpora SNMPv2 a SNMPv3 a REST API c. Samostatná sekce v grafickém rozhraní pro zobrazní zjištěných hrozeb d. Možnost šifrování přenášené komunikace mezi poptávaným řešením pro analýzu dat a poptávaným NGFW zařízením 4. Požadavky na podporu výrobce a. Podpora výrobce v režimu 24x7 na systém i konfiguraci je součástí nabídky Konfigurace dodávaného systému a předávání logů a alertů do Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí (viz kap. 4.4.4).
P.86	Součástí dodávky musí být instalace a konfigurace řešení včetně přechodu ze stávající WAN sítě ZZS na dodávanou infrastrukturu, tak aby byl minimálně omezen provoz lokalit. Změna se nesmí projevit v rámci centrálních lokalit. Součástí konfigurace je zařazení dodávaných komponent do monitoringu infrastruktury a monitoringu síťového provozu. Instalace a konfigurace musí být včetně aktualizací všech firmware na poslední aktuální a stabilní verze.

#	Požadavek
	Všechny centrální prvky a jedna vzorová vzdálená lokalita budou instalovány na místě. Zadavatel následně zajistí rozvoz a instalaci ostatních vzdálených lokalit, přičemž Uchazeč bude pro tyto účely v době instalace dostupný pro vzdálenou podporu a kontrolu funkčnosti. Vzorová vzdálená lokalita bude vybrána v rámci realizace prováděcího projektu na základě požadavku Zadavatele.
P.87	Napojení a předávání alertů a logů do systému analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí (viz kap. 4.4.4).
P.88	Je požadována dodávka HW a nezbytných licencí, záruka na funkčnost dodaného řešení po dobu 5 let.

Tabulka 11: Zajištění šifrování v rámci komunikační sítě

4.4.9 Infrastruktura (HW) a systémový SW pro běh dodávaného SW a technologií

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

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 (min. 5 let a min. v rozsahu stávajícího IS ZOS) a v návaznosti na splnění těchto podmínek a potřeb technologie, uchazeč navrhne a dodá vhodnou HW a SW infrastrukturu.

#	Požadavek
P.89	Dodávka infrastruktury a běhového prostředí pro následující části dodávky: 1. Virtualizační prostředí pro aplikační bezpečnost a další bezpečnostní komponenty, které nebudou mít dedikovaný HW. 2. Systémy pro monitoring systémů a komunikační infrastruktury (4.4.3) 3. Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí (kap. 4.4.4) Následující požadavky na infrastrukturu (HW) a systémový SW pro běh dodávaného SW jsou minimální, tj. pokud mají dodávky dodavatele nároky vyšší, navrhne dodavatel odpovídající řešení a v nabídce jej popíše.
P.90	Dodávka min. 2 ks virtualizačního serveru s min. konfigurací: 1. Dvouprocesorový server určený do stávajícího chassi DELL EMC MX7000. 2. 1x CPU min. 32C / 64T, frekvence min. 2GHz, 48 MB Cache a podporou DDR3200 (CPU musí být typu Intel z důvodu live migrace virtuálních serverů). 3. RAM min. 256 GB (8x32) RDIMM, 3200MT/s. 4. HDD min. 2x 240 GB SSD RAID1 nebo ekvivalentní řešení vhodné pro virtualizaci. 5. LAN min. dvouportová karta 25 GbE s Offload podporou iSCSI a FcoE. 6. TPM 2.0. 7. Redundantní zdroje.

#	Požadavek
	8. Plnohodnotná management karta (OOB) propojená dedikovaným LAN portem s managementem šasi. Správa serveru pouze v HTML5 s možností KVM over IP přístupu k serveru. 9. Management plně integrovaný se správou šasi dohledového cloud GUI, shodného jako šasi 10. Licence VMware v aktuální verzi pro osazené CPU a počet Core. Nabízený produkt (varianta) musí podporovat minimálně vysokou dostupnost (HA), živou migraci virtuálního stroje, živou migraci úložiště (virtuálního disku) a akcelerovanou grafiku pro virtuální stroj a kompatibilní se stávajícím řešením. 11. SW plugin či licence, pro zpřístupnění HW dohledu z prostředí VMware vCenter. 12. Licence Windows Server Datacenter v aktuální verzi pro příslušný počet CPU a Core, s možností downgrade a včetně instalačních médií. Možno použít i OEM provedení, pokud bude licenčně vyhovovat. 13. Licence zálohovacího systému pro zálohování minimálně dodávaných komponent a systémů tak aby byly zálohovány v rámci jednotného systému zálhování ZZS KHK. 14. Součástí dodávky budou všechny potřebné komponenty pro instalaci do šasi. 15. Záruční servis a podpora HW 7 let, SLA max. 4 + 4 hodiny po nahlášení závady. Oprava v místě instalace, servis je poskytován výrobcem, jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému, možnost stažení ovladačů a management software na webových stránkách po celou dobu platné podpory. 16. Podpora SW 5 let.
P.91	Zadavatel umožní využití stávající kapacity diskových polí v objemu 3TB. Stávající kapacita bude využita pro běžný chod systémů a jejich data (např. SOS-BI, AD monitoring, 802.1x apod.). Nejedná se tedy o kapacitu určenou pro ukládání logů a dat z celé infrastruktury (na to jsou určeny prostředky specifikované níže). Pokud dodavatel potřebuje pro svou dodávku větší diskovou kapacitu, je součástí dodávky i diskové pole pro ukládání dat z bezpečnostních technologií splňující minimálně: 1. Kapacita pro ukládání dat dodávaných bezpečnostních technologií na 5 let provozu. 2. Významné parametry: RAID6, iSCSI min. 10Gbps, redundantní zdroj a dostatečný výkon pro chod dodávaných systémů. 3. Připojitelné do virtualizace na dodávané a servery. 4. Podpora na 5 let typu NBD, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení.
P.92	Monitoring systémů a komunikační infrastruktury bude provozován na samostatné, oddělené infrastruktuře, aby byla zajištěna nezávislost monitorovacího prostředí na monitorované infrastruktuře. Dodávka min. 1 ks samostatného monitoring serveru s min. konfigurací: 1. provedení Rack mount (včetně potřebných montážních komponent a ramene pro kabeláž) 2U, pro přístup ke všem komponentám serveru není nutné nářadí, barevně značené hot-plug vnitřní komponenty

#	Požadavek
	2. minimálně 1x CPU min. 24 fyzickými jádry při frekvenci min. 2.8Ghz na jádro. Požadovaná cache CPU min. 128M a maximální výkon 180 W. Výkon celého systému odpovídá minimálně hodnotě Base = 168 získané z měření www.spec.org) 3. minimálně 128 GB na frekvenci 3200MHz, požadujeme ideální rozložení paměťových modulů v návaznosti na technické požadavky paměťových kanálů daného typu server, paměť rozšiřitelná min. na 1TB typu DDR4 4. server musí podporovat osazení min. 4 x 3,5palcových disků SAS, SSD nebo SATA, server osazený hot-plug disky min.: 2x 1.6TB SSD SAS při splnění hodnoty DWPD 3 a min. 2x 4TB 7.2K RPM NLSAS 5. Síťové rozhraní Min. 2 x 1GbE ethernet port a Min. 2x 10/25Gb SFP28 port včetně 2ks SFP+ SR modulů do serveru, 2ks SFP+ SR modulů do Switche (Cisco 9500) a FO kabelů LC/LC 5 m 6. Redundantní síťové napájecí zdroje s možností nastavení limitů výkonu a spotřeby v BIOSu 7. Interface min 3 x USB (1 vpředu, 2 vzadu) a sériový port RS232 8. hw řadič s minimálně 2 GB cache a podporou RAID 0, 1, 5, 6, 50, 60, podpora SED disků a SSD disků, podpora globálního i dedikovaného hot-spare, podpora Auto resume po ztrátě napájení, podpora 12Gbps technologie rozhraní disků 9. certifikace pro aktuální verze VMware ESX, vSphere, Windows Server, Red Hat Enterprise Linux 10. Management serveru nezávislý na operačním systému poskytující management funkce a vlastnosti: webové rozhraní HTML5 a dedikovaná IP adresa, sledování hardwarových senzorů (teplota, napětí, stav, chybové senzory) error alerty (server reset, kritické senzorové hodnoty atd.) za použití e-mail traps, paging, IPv6, 11. Vyžadována je schopnost monitorovat a spravovat server (hardwarová konfigurace, RAID konfigurace, server reset, reboot, power-on/off/cycle atd.) 12. Management musí podporovat dvou faktorovou autentifikaci a AD/LDAP 13. Záložní BIOS v dedikované ROM s možností manuální/automatické obnovy 14. Vestavěné GUI s podporou HTML5 a dedikovaná IP adresa IPv4, IPv6 a nezávislý management je s dedikovaným ethernet portem, který není součástí požadovaných ethernet portů 15. podpora na 5 let typu NBD, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení 16. Automatické zakládání servisních požadavků v případě poruchy, oprava v místě instalace, servis je poskytován výrobcem, jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému, možnost stažení ovladačů a management software na webových stránkách po celou dobu platné podpory. 17. operační systém dle požadavků navrženého nástroje na monitoring komunikační infrastruktury a licencován na dodávaný HW 18. Licence zálohovacího systému pro zálohování minimálně dodávaných komponent a systémů tak aby byly zálohovány v rámci jednotného systému zálohování Objednatele. je vyžadována kompatibilita se stávajícím prostředím – server bude zařazen do stávající infrastruktury.

#	Požadavek
	Dodávka min. 1 ks samostatného serveru pro SIEM s min. Konfigurací: 1. Server RACK o velikosti max. 2U 2. min. 1x 16jádrový procesor, min. 2 GHz, třídy Silver 3. min. 96 GB RAM 4. dostatečná lokální disková kapacita zapojená v RAID6 pro logy a flow pro uchování na min 18 měsíců. 5. 1 x dual-port síťová karta min 10Gb ETH RJ-45 6. 1 x dual-port síťová karta min 10Gb ETH SPF+ 7. Servisní karta pro vzdálenou správu. 8. Redundantní napájecí zdroj 9. Veškerý instalační materiál (kabely, SFP moduly apod.) pro připojení HW do stávající infrastruktury 10. podpora na 5 let typu NBD, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení se službou ponechání vadného disku v případě jeho výměny. 11. Operační systém dle požadavků SIEM je vyžadována kompatibilita se stávajícím prostředím – server bude zařazen do stávající infrastruktury
P.93	Dodávka min. 1 ks samostatného log serveru (doplňujícího nástroje pro logování z IT infrastruktury) s min. konfigurací: 19. provedení Rack mount (včetně potřebných montážních komponent a ramene pro kabeláž) 2U, pro přístup ke všem komponentám serveru není nutné nářadí, barevně značené hot-plug vnitřní komponenty 20. minimálně jeden 16jádrový 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) 21. min. 32 GB RAM (min. 8 GB moduly 2666MHz typu DDR4) 22. min. 5x 4 TB disk min 7200 otáček a min 3x 1,92 TB SSD s min DPWD 3 23. min. 4x 1Gbase-T ethernet síťové porty s podporou IPv4, IPv6 24. 2 redundantní síťové napájecí zdroje 25. Interface: 3 x USB a sériový port 26. hw řadič s minimálně 2 GB cache a podporou RAID 0, 1, 5, 6, 50, podpora SED disků a SSD disků, podpora globálního i dedikovaného hot-spare 27. certifikace pro aktuální verze VMware ESX, vSphere, Windows Server, Red Hat Enterprise Linux 28. 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) 29. vyžadována je schopnost monitorovat a spravovat server out-of-band bez nutnosti instalace agenta do operačního systému

#	Požadavek
	30. management musí podporovat dvou faktorovou autentifikaci, filtrování přístupu na základě IP adres (IP blocking) a AD/LDAP 31. požadujeme vestavěné GUI s podporou HTML5 a možnost komunikace pomocí: HTTPS, CLI, IPMI, WSMAN, REDFISH 32. Veškerý instalační materiál (kabely, SFP moduly apod.) pro připojení HW do stávající infrastruktury 33. podpora na 5 let typu NBD, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení 34. operační systém dle požadavků navrženého nástroje na logování z IT infrastruktury 35. Licence zálohovacího systému pro zálohování minimálně dodávaných komponent a systémů tak aby byly zálohovány v rámci jednotného systému zálohování Objednatele. je vyžadována kompatibilita se stávajícím prostředím – server bude zařazen do stávající infrastruktury
P.94	Dodávka a instalace systémového SW – požadujeme dodávku systémového SW pro všechny nabízené systémy. Jedná se o minimálně následující systémový SW: 1. Operační systémy serverů, kde požadujeme dodávku všech licencí potřebných operačních systémů a mimo to požadujeme 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. 2. Databáze pro dodávané systémy. 3. Pro virtualizaci dodávaných serverů požadujeme kompatibilní řešení se stávající virtualizací tak, aby bylo možné zařadit do jedné konfigurační konzole – minimálně licence virtualizačního SW pro dodávaný počet CPU kompatibilní se stávajícím virtualizačním SW (viz kap. 7.4), s podporou výrobce na 5 let. 4. Pro zařazení virtualizačních serverů do systému zálohování je požadována dodávka licence kompatibilního systému zálohování pro dodávané konfigurace virtualizačních serverů. ZZS poskytne součinnost při konfiguraci do stávajícího zálohovacího řešení. Stávající technologie, na které je odkazováno, jsou uvedeny v kap. 7.4 – Stav ostatních informačních a komunikačních technologií. V případě, že nabízené řešení vyžaduje další nespecifikovaný systémový SW tak musí být součástí nabídky.
P.95	Součástí dodávky je zařazení dodávané infrastruktury do stávající infrastruktury (napojení na stávající infrastruktury a připojení k virtualizačnímu prostředí) včetně dodávky potřebných kabelů. Součástí dodávky bude i začlenění do systému zálohování provozovaného Objednatelem. Návrh propojení do stávající infrastruktury a způsob zálohování bude součástí implementační analýzy a návrhu řešení a bude podléhat schválení zadavatelem.
P.96	Dodávka, zapojení, instalace technologií, instalace a zprovoznění dodávaných technologií a prvků na dodaných technologiích na místě včetně aktualizací všech firmware na poslední aktuální a stabilní verze a zařazení do monitoringu infrastruktury. Součástí dodávky není strukturovaná kabeláž.

Tabulka 12: Infrastruktura (HW) a systémový SW pro běh dodávaného SW a technologií

4.4.10 Nástroje pro testování zranitelností a testování zranitelností

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

#	Požadavek
P.97	Je požadována dodávka nástroje/nástrojů pro periodické testování bezpečnostních zranitelností interních systémů i systémů, které komunikují s externími subjekty i jako součást penetračních testů.
P.98	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.99	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 1x týdně)
P.100	Předmětem dodávky není periodické provádění testů zranitelností (nad rámec testů v rámci vedlejších aktivit), ale zajištění nástrojů pro provádění a vyhodnocování uvedených testů.
P.101	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.102	Instalaci skeneru musí být možné realizovat na prvky s operačními systémy Microsoft Windows 10 a vyšší, Microsoft Windows Server 2012 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.103	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.104	Řešení musí být schopné identifikovat chybějící záplaty/zranitelné služby a aplikace běžící na skenovaných systémech.
P.105	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.
P.106	Provedení testů zranitelnosti: 1. Provedení testů zranitelnosti pro zabezpečované IS (informační systémy a technologie jsou popsány v kap. 7.2 – Informační systémy k zabezpečení).

#	Požadavek
	2. Pro zabezpečované systémy budou provedeny závěrečné testy zranitelnosti z externí sítě. V zájmu ověření korektního fungování zabezpečení komunikační sítě a zajištění vysoké úrovně bezpečnosti provozovaných aplikací je požadováno provedení jednorázových penetračních testů.
P.107	Závěrečné testy zranitelnosti budou provedeny z externí sítě na zabezpečované. Jedná se tedy o testy zranitelnosti realizované přes bezpečnostní prvky – perimetry (FireWall). 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.108	V zájmu ověření a zajištění vysoké úrovně bezpečnosti provozovaných aplikací je požadováno provedení jednorázových penetračních testů. Penetrační testy 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. Testy budou provedeny jak při využití WAF, tak přímo vůči serveru, který aplikaci poskytuje. Testy budou provedeny jak autentizovanou (s právy běžného uživatele), tak neautentizovanou formou (anonymní přístup). 3. 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 zranitelností. Testy budou realizovány dle aktuální verze OWASP Web Security Testing Guide (WSTG) 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. Penetrační testy budou provedeny na následující aplikace: 1. Endpoint NIS IZS (SOS5) – publikováno do sítě NIS IZS 2. SOSView – publikováno do sítě Internet 3. Mobilní zadávání dat – MZD/EKP přístup z tabletů ve vozidlech. *Zadavatel zajistí součinnost dodavatelů uvedených systémů v rámci součinnosti.*

#	Požadavek
P.109	Výstupem testů zranitelnosti a penetračních testů musí být: 1. Závěrečná zpráva, která bude obsahovat soupis provedených testů a jejich výsledků, detailní popis odhalených zranitelností, určení úrovně jejich rizika a konkrétní postup umožňující jejich odstranění nebo mitigaci. 2. Doporučení pro 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: Nástroje pro testování zranitelností a testování zranitelností

4.4.11 Řízení aktualizací a vzdálená správa zabezpečovaných IS, provozní infrastruktury a bezpečnostních technologií

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

#	Požadavek
P.110	Pro řešení řízení aktualizací požadujeme vytvoření plánů postupů aktualizací a jejich testování pro minimalizaci dopadů případných nekompatibilit na kritickou infrastrukturu. Minimální požadavky: 1. Definice postupů aktualizací na základě druhu systému a návazné infrastruktury. 2. Návrh rozdělení jednotlivých systémů a jejich návazností dle důležitosti. (např. telefonie 155, dispečink, podpůrné systémy, administrativa apod.) z pohledu nasazení a testování aktualizací. 3. Volba nástrojů výrobců pro aktualizace s návrhem zjednodušení a přiměřené automatizace procesů s pohledu zajištění maximální dostupnosti kritických systémů. 4. Implementace vybraných systémů aktualizací výrobců jednotlivých systémů. 5. Součástí dodávky bude i odzkoušení správnosti plánů postupů aktualizací a jejich průběžná aktualizace v rámci servisní podpory.
P.111	V rámci návrhu plánů postupů aktualizací požadujeme realizovat systém, který bude schopen identifikovat minimálně bezpečnostní aktualizace SW, a to napříč systémy (servery, DB, komunikační infrastruktura) a to minimálně pro základní systémy IS OŘ. Včetně evidence (inventarizaci) těchto zjištění.
P.112	Návrh procesů správy koncových a centrálních zařízení včetně implementace autentizace s využitím AD účtů.
P.113	Systém pro audit pracovních stanic (250ks), který bude poskytovat minimálně následující vlastnosti: 1. Audit a evidence SW 2. Evidence licencí 3. Audit a evidence HW 4. Evidence majetku včetně převodek a protokolů 5. Vzdálené distribuce SW 6. Vzdálená plocha a správa

#	Požadavek
P.114	V případě možnosti exportu logů komponent určených pro aktualizace požadujeme jejich zasílání do centrálního systému logů včetně návrhu jejich zpracování, notifikací a reportů.
P.115	Notifikace správců o dostupnosti kritických aktualizací.
P.116	Sledování využití / vytížení jednotlivých výpočetních prvků infrastruktury: 1. Všech serverů zabezpečovaných IS a dodávaných bezpečnostních technologií. 2. Koncových stanic IS ZOS.
P.117	Součástí je dodávka, instalace, a implementace dodávaných technologií a související služby.

Tabulka 14: Řízení aktualizací a vzdálená správa zabezpečovaných IS, provozní infrastruktury a bezpečnostních technologií

4.4.12 Bezpečnostní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.118	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.119	Vybavení musí plnit podmínky zákona č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
P.120	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.121	Zabránění vstupu neautorizovaného subjektu do systému – zamezení možnosti přístupu neoprávněného subjektu.
P.122	Zajištění šifrované komunikace mezi všemi součástmi systému a pracovišti uživatelů, případně zajištění komunikace v odděleném síťovém prostředí.
P.123	Evidence přístupů všech uživatelů do systémů a technologií (logování) včetně časových údajů.
P.124	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.125	Veškeré logy budou dostupné pro externí Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí.

Tabulka 15: Bezpečnostní požadavky

4.4.13 Implementační a provozní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.126	Všechny komponenty musí být připraven na provoz 24x7x365 (non-stop).
P.127	Počet uživatelů informačních systémů se nezmění.
P.128	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.129	Instalace do prostředí objednatele uvedeného v kap. 7.4 – Stav ostatních informačních a komunikačních technologií a kap. 7.2 – Informační systémy k zabezpečení.
P.130	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.
P.131	Dodávka OS na servery, včetně instalace do prostředí objednatele, vč. potřebných licencí, pokud se jedná o licencovaný OS.
P.132	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.133	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 7.4.1 – Datové centrum, HW infrastruktura, systémový SW.
P.134	Zajištění administrátorských aplikací, konzolí pro všechny součástí systému (OS, DB, IS, ...) pro zajištění konfiguračního managementu systému anebo jeho součástí.
P.135	Dohled – dodávané systémy a technologie musí předávat informace o svém stavu (stavu služeb apod.) na žádosti SNMP GET. Zhotovitel poskytne parametry, podmínky a součinnost při nastavení dohledu dodaného řešení.
P.136	Architektura řešení celého systému musí korespondovat s požadavky na jeho dostupnost, uvedenými v servisní smlouvě.
P.137	Synchronizace času všech zařízení s time serverem nebo zprostředkovaně přes centrální systém.

Tabulka 16: Implementační a provozní požadavky

4.5 POŽADAVKY NA SLUŽBY

4.5.1 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 5 - 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

Název	Popis
	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 17: 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 2016 (MS Word 2016, MS Excel 2016, MS PowerPoint 2016)
- MS Project 2016
- 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.) nebo online úložištích (Sharepoint apod.). 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. Listinná forma není požadována

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.

4.5.2 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.

4.6 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.

5 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.	220	Dodávka a implementace HW, SW a síťové infrastruktury.
4	Vývoj a implementace úprav SW, dodávka dokumentace k SW.	220	Vlastní vývoj a implementace úprav IS dle analýzy a návrhu řešení.
5	Ověření funkčnosti dodaných technologií a systémů.	250	Otestování funkčnosti technologií a systémů a ověření jejich plné funkčnosti.
6	Seznámení s funkcionalitami, obsluhou dodávaných technologií	250	Seznámení s funkcionalitami, obsluhou dodávaných technologií
7	Dodávka dokumentace dodaného systému a jeho částí.	250	Min. uživatelská dokumentace, dokumentace skutečného provedení, systémová dokumentace, projektová dokumentace.
8	Převedení do zkušebního provozu.	251	Převedení do zkušebního provozu, odstranění všech vad a nedodělků, dokončení realizace a převedení do ostrého provozu.
9	Testování zranitelností / penetrační testy	280	Zpracování a předání testů zranitelností a penetračních testů a úpravy konfigurace bezpečnostních technologií tak, aby byly zjištěné zranitelnosti eliminovány. *Pozn.: jedná se o ověření správnosti nastavení bezpečnostních technologií v rámci dodávky,*
10	Ukončení realizace dodávky.	280	Součástí je zahájení doby provozu dodaného systému a poskytování servisních služeb.

Tabulka 18: Harmonogram

Doplňující informace:

- Pod pojmem „den" je míněn kalendářní den.

- Zhotovitel má možnost definovat kratší termíny plnění (v rámci dodávky), v nabídce nelze zkrátit dobu zkušebního provozu, která musí být min. 10 dnů.
- Zkrácení zkušební doby je možné pouze na základě písemné dohody se Zadavatelem

6 MÍSTA PLNĚNÍ

Realizace předmětu plnění bude probíhat v následujících místech plnění:

Místo	Adresa	Předmět realizace
Sídlo a primární datové centrum	Hradecká 1690/2A, Hradec Králové PSČ: 500 12	Primární datové centrum ZZS KHK – dodávky v návaznosti na technologie umístěné v tomto DC a dodávka částí technologie. Primární lokalita IS elektronická pošta a Pagingový systém a záložní lokalita pro DC ZOS (zabezpečované IS a KS), DC je propojeno s DC ZOS. Sídlo ZZS KHK – místo předání výstupů projektu.
Datové centrum IS ZOS ZZS KHK	Pražská 230/153z, Hradec Králové PSČ: 500 04	Datové centrum IS ZOS ZZS KHK – 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, DC je propojeno s primárním datovým centrem ZZS KHK. *Pozn.: lokalita označovaná také jako „Bláhovka"*
Záložní datové centrum ZZS KHK	Areál LZS Fakultní nemocnice Sokolská 581 Hradec Králové PSČ: 500 12	Záložní/zálohovací datové centrum ZZS KHK – umístění zálohovacích a souvisejících technologií, zálohování systémů a technologií do této lokality.

Tabulka 19: Místa plnění

7 VÝCHOZÍ STAV

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

7.1 ZDRAVOTNICKÁ ZÁCHRANNÁ SLUŽBA KRÁLOVÉHRADECKÉHO KRAJE (ZADAVATEL)

Kontext ZZS KHK v rámci řešení projektu je následující:

1. ZZS KHK 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 KHK musí zajistit výkon veřejné správy v oblasti zdravotnické záchranné služby a podmínky pro zajištění připravenosti poskytovatele zdravotnické záchranné služby (ZZS KHK) 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 KHK je využíván elektronická pošta.
    c. Pro komunikaci ZOS s výjezdovými skupinami (VS) je využíván Pagingový systém.

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

7.2 INFORMAČNÍ SYSTÉMY K ZABEZPEČENÍ

V rámci projektu budou realizována opatření k zabezpečení ostatních informačních systémů (IS) a komunikačních systémů (KS) ZZS KHK. 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 Královéhradeckého kraje bude zabezpečovat své informační (IS). Stručný výčet IS je uveden v dalším textu této kapitoly.

Všechny uvedené IS a KS jsou umístěny, provozovány a využívány uživateli v sídle ZZS KHK nebo na adresách na území Královéhradeckého kraje uvedených v kap. 6.

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 KHK nebyla Národním úřadem pro kybernetickou a informační bezpečnost určena jako provozovatel základní služby podle §22a ZKB.

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

Název IS	Správce	Stručný popis	Typ
IS ZOS	Zdravotnická záchranná služba Královéhradeckého kraje	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 KHK, tj. poskytování PNP na území Královéhradeckého kraje.	Informační systém (IS)
Elektronická pošta	Zdravotnická záchranná služba Královéhradeckého kraje	Systém pro příjem a odesílání elektronické pošty v rámci komunikace ZZS KHK. Jedná se o hlavní informační systém (IS) ZZS KHK zajišťující komunikaci mezi zaměstnanci ZZS KHK a podporu výkonu jejich činností.	Infomační systém (IS)
Pagingová síť	Zdravotnická záchranná služba Královéhradeckého kraje	Jedná se o radiovou komunikační síť (KS) pro komunikaci dispečinku ZOS s výjezdovými skupinami v rámci řízení poskytování PNP posádkami v terénu, tedy podporu výkonu jejich činností, konkrétně předávání výzev jednotlivým posádkám. Jedná se o komunikační systém (KS) ZZS KHK zajišťující komunikaci mezi zaměstnanci ZZS KHK a podporu výkonu jejich činností.	Komunikační systém (KS)

Tabulka 20: 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.

7.2.1 IS ZOS

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

7.2.1.1 Informační systémy a aplikační software ZOS

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

IS, SW, subsystém	Stávající 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 KHK: 1. Dispečink 2. Základna 3. Správa směn 4. Evidence směn 5. Svolávání 6. Statistiky 7. Kontrolní pracoviště 8. Administrace 9. Správa stanic Současně s tímto jsou realizovány následující integrace: 1. Interní (v rámci IS ZOS) a. Integrace telefonie – příjem tísňové výzvy. b. Integrace na GIS – zobrazení polohy tísňové výzvy, polohy výjezdu, lokalizace v mapě apod. c. Integrace na systém sledování vozidel – předávání výzvy k výjezdu, příjem a sledování stavů, sběr informací o výjezdu vozidel. d. EKP – předávání dat o pacientovi/pacientech k výjezdu pro posádku/posádky. e. Integrace na záznamový systém – připojování záznamů hovorů, přehrávání záznamů apod. f. Národní dopravně informační centrum – odesílání informací do NDIC o dopravních nehodách ze zaznamenaných událostí. g. Integrace telekomunikací a radiokomunikací – pro ovládání spojení a příjem statusů z RS. h. Integrace aplikace FirstResponder

IS, SW, subsystém	Stávající stav
	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. Rozhraní pro příjem dat mobilní aplikace Záchranka d. Lokalizace volání info 35/ AML e. Rozhraní pro výzvy LZS + HS 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 dispečinku. 2. Zobrazování poloh a stavů vozidel ZZS ze systému sledování vozidel (AVL). 3. Zobrazování poloh událostí a SaP dalších složek IZS v rámci integrace na NIS IZS. 4. Lokalizace pro IS OŘ, vyhledávání 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.
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.

IS, SW, subsystém	Stávající stav
	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. Elektronické podepisování certifikátem uživatele a biometrickým podpisem přebírajícího zdravotníka cílového zdravotnického zařízení. 5. Předávání Zprávy o výjezdu elektronickou cestou do Archivů zdravotnické dokumentace projektu eHealth. 6. Předání z MZD zpět do EKP. 7. Přebírání dat ze systému sledování vozidel. 8. Následné úpravy, dopracování, kontrola dat na výjezdových základnách. 9. 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. eHealth systém KHK – výměna a elektronická archivace zdravotnické dokumentace na území KHK. 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 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 a. Informační systémy zdravotních pojišťoven. Součástí je řada dalších důležitých funckionalit, které jsou popsané v dokumentaci k IS.

IS, SW, subsystém	Stávající stav
	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. 5. Předávání dat do elektronické knihy jízd (EKJ). 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. d. EKJ – elektronická kniha jízd. 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.
Elektronická kniha jízd (EKJ)	Elektronická kniha jízd přebírá data ze systému AVL a umožňuje vedení a sledování provozu vozidel. Stávající Elektronická kniha jízd (EKJ) je produkt Fleetware jehož výrobcem je společnost RADIUM s.r.o. 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.
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.

IS, SW, subsystém	Stávající stav
Telefonní ústředna	Telefonní ústředna je produkt Cisco Call Manager. 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. Nadstavbovou částí je subsystém eXperience pro přehrávání a analýzu zvukových záznamů. 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 TTC MARCONI 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. Zajištění integrace a obsluhy radiofonní komunikace prostřednictvím analogové radiové sítě ZZS.

IS, SW, subsystém	Stávající stav
	4. Integrace s IS ZOS – volání, návaznost hovorů na výzvy a události. 5. Záznamové zařízení (REDAT) – nahrávání radiofonní komunikace. 6. 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.
Integrace se systémem Pegas (CC-API)	CC-API slouží jako integrační rozhraní pro napojení informačních systémů a aplikačního SW k radiové síti PEGAS/TETRA a TETRAPOL. CC-API je produktem společnosti AIRBUS a výhradním dodavatelem technologie PEGAS/TETRA a TETRAPOL je společnost Pramacom Prague spol. s r.o. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu. 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.

Tabulka 21: IS ZOS

7.2.1.2 Pracoviště ZOS

Celkový počet pracovišť: 6 ks + 1 ks pro vedoucího směny + 1 ks testovací pracoviště, následující vybavení platí pro každé pracoviště jednotlivě.

Pracoviště ZOS jsou vybavena následovně:

1. Pracovní stanice PC Dell Optiplex 3050 (3x výstup na LCD).
2. 3x LCD monitory 24", full HD (1920x1080), audiolišta.
3. 1x dotykový LCD / touchscreen 19" pro ovládání integrace telefonie a radiofonie.
4. Klávesnice (USB).
5. Drátová myš (USB).
6. Bezdrátová Bluetooth náhlavní souprava připojená k integraci telefonie a radiofonie.
7. OS Windows 10, 64 bit.

7.2.2 Elektronická pošta

Systém pro příjem a odesílání elektronické pošty v rámci komunikace ZZS KHK. Část primární činnosti ZZS KHK, 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 KHK zajišťující podporu hlavní činnosti ZZS KHK, 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 KHK, 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 KHK zajišťující komunikaci mezi zaměstnanci ZZS KHK 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 KHK a je provozována v datovém centru ZZS KHK, tj. nejedná se o hosting ani službu.

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

Přístup je na základě identifikace a autorizace uživatele (v současné době bez 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 KHK – detaily viz kap. 7.3 – Umístění.
2. Systém elektronické pošty využívá systém Kerio Connect ve verzi 9.x na OS Debian
3. Aktiva jsou sdílenými aktivy v rámci primárního DC v rámci samostatného virtuálního serveru. V rámci projektu budou zabezpečena jen centrální aktiva v DC.
4. Provoz je zajištěn v režimu 7x24x365 – Elektronická pošta sice není kritickým systémem, ale je provozována nonstop z důvodu specifického provozu ZZS.
5. Součástí projektu je zajištění Nástroje pro ochranu před škodlivým kódem, tj. technické opatření „e) nástroj pro ochranu před škodlivým kódem".
6. 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.

7.2.3 Pagingová síť

Pagingová síť je provozována následujícím způsobem:

1. Navazuje na provozovaný IS ZOS (předávaní zpráv z IS ZOS do pagerové sítě), ale fyzicky je distribuována napříč všemi DC a lokalitami výjezdových základen (SW pro distribuci, vysílače, převaděče, pagery).
2. Aktiva jsou z části sdílenými aktivy v rámci DC IS ZOS v rámci virtualizované infrastruktury (viz výše detailní popis k IS ZOS), na které navazuje lokální řešení (vyhražené PC) pro prvotní vysílání zpráv v Primárním DC. Rozesílání dále pokračuje prostřednictvím několika převaděčů a koncových vysílačů v jednotlivých výjezdových základnách až do koncových pagerů uživatelů (členů posádek ZZS). V rámci projektu bude zabezpečena celá datová cesta z pohledu jak integrity, tak důvěrnosti přenášených informací.
3. Provoz je zajištěn v režimu 7x24x365 – Pagingová síť je jedním z klíčových systémů a je provozována nonstop z důvodu specifického provozu ZZS.
4. Součástí projektu je zajištění následujících opatření:

7.3 UMÍSTĚNÍ IS ZOS, SYSTÉMU ELEKTRONICKÉ POŠTY A DC

V následující tabulce jsou uvedena umístění IS ZOS:

Místo	Adresa	IS	Předmět realizace
Sídlo a primární datové centrum	Hradecká 1690/2A, Hradec Králové PSČ: 500 12	Elektronická pošta (primární DC) IS ZOS (záložní servery) Pagingový systém	Sídlo ZZS KHK a primární část administrativního provozu a využívání elektronické pošty (zabezpečovaný IS).
Zdravotnické operační středisko ZZS KHK (DC, dispečink)	Pražská 230/153z, Hradec Králové PSČ: 500 04	IS ZOS (DC IS ZOS) Elektronická pošta (uživatelé)	Datové centrum IS ZOS ZZS KHK, všechna aktiva IS ZOS umístěná v tomto DC. Dispečerská pracoviště ZOS, kde jsou aktiva (pracoviště) operátorů ZOS. *Také označováno jako „Bláhovka".*
Záložní datové centrum ZZS KHK	Areál LZS Fakultní nemocnice Sokolská 581 Hradec Králové PSČ: 500 12	Záložní DC ZZS KHK	Záložní/zálohovací datové centrum ZZS KHK – umístění zálohovacích a souvisejících technologií, zálohování systémů a technologií do této lokality.

Tabulka 22: Umístění

7.4 STAV OSTATNÍCH INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ

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

7.4.1 Datové centrum, HW infrastruktura, systémový SW a technologie

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

Parametr	Údaj(e), parametry a informace
Datové centrum IS ZOS (Lokalita Bláhovka)	
Záložní zdroj el. energie	Záložní napájení je využíváno v rámci napájení serverovny HZS, zajištěné jak UPS, tak motorgenerátorem.
HW infrastruktura	
Rackové skříně	Veškerá technologie v rámci serverovny je umístěna v několika RACK skříních.
Servery	Jako virtualizační servery je využíváno celkem pět serverů DELL PowerEdge. Pro další potřeby jsou provozováno ještě další tři samostatné servery DELL PowerEdge a jeden HP ProLiant. Servery jsou osazeny síťovým rozhraním jak na technologii Gigabit ethernet, tak také TenGigabitethernet.

Parametr	Údaj(e), parametry a informace
Disková úložiště	Úložiště je realizováno diskovým polem DELL SCv3020 10Gbps iSCSI a doplněno polem pro odkládání záloh QNAP NAS, který je také osazený 10Gbit rozhraním. Pro komunikaci diskových polí jsou vyhrazeny 10Gbps switche DELL, které tak tvoří infrastrukturu pro iSCSI.
Zálohování	Zálohování virtualizovaného prostředí je realizováno v rámci nastavených zálohovacích scénářů pomocí SW Veeam Backup pro VMware, případně prostou kopií dat na záložní NAS.
Systémový SW	
Operační systémy	V rámci dodávky virtualizačních serverů byly dodány licence Windows Server 2012 Datacenter. Pro některé servery je využit OS Linux v různých distribucích.
Virtualizační SW	Pro virtualizační servery je využito licence VMware Essentials Plus kit, který je určen pro 3 dvouprocesorové servery. Pro další dva servery je využito Oracle virtualizace.
DB	Pro provoz jsou využity databázové licence, a to jak ORACLE, tak Microsoft SQL server.
Dohled	Je realizován jako služba v rámci maintenace smlouvy s dodavatelem a za pomoci jeho prostředků.
Primární (centrální) datové centrum (Lokalita Hradecká)	
Záložní zdroj el. energie	Záložní napájení je zajištěno jak UPS, tak motorgenerátorem.
HW infrastruktura	
Rackové skříně	Veškerá technologie v rámci serverovny je umístěna v RACK skříni.
Servery	Jako virtualizační servery jsou využívány 2 servery DELL PowerEdge. Pro další potřeby je provozován ještě jeden samostatný servery DELL PowerEdge pro zálohu klíčového SW IS ZOS. Servery jsou osazeny síťovým rozhraním jak na technologii Gigabit ethernet, tak také TenGigabitethernet.
Disková úložiště	Úložiště je realizováno diskovým polem DELL SCv3020 10Gbps iSCSI a doplněno polem pro odkládání záloh QNAP NAS, který je také osazený 10Gbit rozhraním. Pro komunikaci diskových polí jsou využity přímo core switche HP datového centra (10Gbit) a fyzická rozhraní SAS serverů a diskového pole.
Zálohování	Zálohování virtualizovaného prostředí je realizováno v rámci nastavených zálohovacích scénářů pomocí SW Veeam Backup pro VMware.
Systémový SW	
Operační systémy	V rámci dodávky virtualizačních serverů byly dodány licence Windows Server 2016 Datacenter. Pro některé servery je využit OS Linux v různých distribucích.
Virtualizační SW	Pro virtualizační servery je využito licence VMware Essentials Plus kit, který je určen pro 3 dvouprocesorové servery.

Parametr	Údaj(e), parametry a informace
DB	Pro záložní server je využita databázová licence ORACLE.
Dohled	V rámci infrastruktury je využíván produkt HP IMC pro dohled a monitoring.
Záložní/zálohovací datové centrum (Lokalita LZS)	
Záložní zdroj el. energie	Záložní napájení je zajištěno jen UPS.
HW infrastruktura	
Rackové skříně	Veškerá technologie v rámci serverovny je umístěna v RACK skříni.
Dohled	V rámci infrastruktury je využíván produkt HP IMC pro dohled a monitoring (společný s primárním DC).
Ostatní relevantní technologie	
QRADAR	Stávající řešení pro detekci kybernetických bezpečnostních incidentů - IBM QRADAR SOFTWARE PER INSTALL License. Řešení bude zachováno/rozšířeno, dodávané řešení musí být kompatibilní a propojené s tímto řešením.

Tabulka 23: Datové centrum, HW infrastruktura, systémový SW

7.4.2 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.
NIS IZS / PČR	Napojení na služby NIS IZS a LCT terminály Pegas/Matra. Síťový provoz tohoto napojení bude v rámci dodaných výstupů projektu monitorován.
Internet	V centrální lokalitě je zajištěno připojení k internetu, které bude možné využít i pro požadavky technologií v rámci realizace a provozu projektu.

Tabulka 24: Datové sítě

7.4.3 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 prostřednictvím VPN WAN. Pro tyto účely jsou všechny lokality vybaveny routery Cisco, na kterých jsou nakonfigurovány IPSec tunely do obou centrálních lokalit. Správa těchto routerů jsou zajištěna servisní maintenance smlouvou s dodavatelem.

Parametr	Údaj(e), parametry a informace
Firewally	V rámci centrálních lokalit jsou umístěny centrální FireWally FortiGate, které zajišťují 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. FireWall odděluje interní síť ZZS nejenom od sítě Internet, ale i od ostatních externích sítí jako je NIS IZS a AKČR apod.
LAN	Lokalita Bláhovka: V rámci DC IS ZOS jsou využity LAN prvky na bázi switchů. Přičemž centrální stack switchů Cisco 3850 realizuje i routrování VLAN segmentů LAN sítě. Lokalita Hradecká: V rámci Primárního DC jsou využity LAN prvky na bázi switchů. Přičemž centrální stack switchů HP 5800 realizuje i routrování VLAN segmentů LAN sítě.
Připojení pracovišť ZOS	Vlastní připojení pracovišť ZOS je realizováno tak, aby výpadek jednoho prvku neznamenal výpadek celého ZOS, ale maximálně poloviny pracovišť.
Připojení k lince 155	Telefonní ústředna operačního řízení Cisco Call Manager je napojena prostřednictvím hlasové brány a rozhraním ISDN30 do veřejné telefonní sítě. ISDN30 je vyhrazena pro používání linky 155 a pro potřeby dispečinku (operačního řízení). Telefonní ústředna operačního řízení je propojena k SIP trunk a k objektové ústředně.
Připojení k síti NIS IZS – MV ČR (PČR)	V rámci serverovny dispečinku (DC IS ZOS) 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 ke krajské síti	ZZS má v lokalitě dispečinku realizováno i napojení na krajské nemocnice v rámci IS eHealth a síť AKČR.
Připojení k internetu	V obou centrálních lokalitách je i centrální napojení do sítě Internet. Toto připojení je zabezpečeno FireWallem (viz výše). Poskytovatelem připojení do sítě Internet je CESNET. Záložní připojení je zajištěno nezávislým lokálním operátorem HK Free.
Datové centrum PČR	
Aktivní prvky	Připojení do datového centra PČR je realizováno samostatným L2 datovým okruhem určeným pouze pro připojení k LCT terminálů. Na straně PČR je umístěn switch, do kterého je připojena veškerá technologie na straně PČR. Na straně ZZS je vyvedeno do centrálního switche Cisco 3850.
Radiové terminály Pegas/Matra (LCT)	V lokalitě PČR je umístěno celkem 7 LCT terminálů propojených do sítě Pegas/Matra.

Tabulka 25: Síťová infrastruktura

7.4.4 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 KHK.
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 KHK.
    c. Pozáruční servis HW a SW infrastruktury.

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

KONEC DOKUMENTU

TECHNICKÁ SPECIFIKACE NABÍZENÝCH TECHNOLOGIÍ

Členěno podle kapitol dokumentu Příloha č. 1: Technická specifikace zadávací dokumentace

4.4.2 Aplikační firewall pro IS ZOS

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. Nabízené řešení plně splňuje požadavky uvedené v zadávací dokumentaci.

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

1. Endpoint NIS IZS (SOS5) – publikováno do sítě NIS IZS
2. SOSView – publikováno do sítě Internet
3. Mobilní zadávání dat – MZD/EKP přístup z tabletů ve vozidlech.

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.

Jedná se o konkrétní řešení F5-BIG-AWF-VE200MV18 BIG-IP Virtual Edition Advanced Web Application Firewall 200 Mbps s licencí BIG-IP Virtual Edition Threat Campaigns Add-on License for Advanced Web Application Firewall 200 Mbps and 25 Mbps.

Odkaz na parametry nabízeného řešení:

https://www.f5.com/pdf/products/big-ip-virtual-editions-datasheet.pdf

V rámci implementace bude realizovaná konfigurace na požadovaná aplikace (SOS5, SOSView, MZD/EKP) 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.

4.4.3 Systémy pro monitoring systémů a komunikační infrastruktury

Nabízené řešení plně splňuje požadavky uvedené v zadávací dokumentaci.

Skládá se z následujících komponent:

1. Systém pro monitoring systémů a komunikační infrastruktury
2. Sondy síťového provozu (virtuální i fyzické)
3. Kolektoru síťového provozu
4. Modul automatického vyhodnocování IP toků

Nabízíme virtuální a HW sondy Progress Flowmon Probe pro monitorování síťové infrastruktury. Tyto sondy zajistí sběr informací o síťové komunikaci v podobě IP toků (NetFlow v5/v9, IPFIX). Sondy jsou pasivní zařízení, která nemají vliv na provoz sítě, ale poskytují detailní viditelnost do komunikační infrastruktury. Všechna získaná data budou zpracovávaná na dedikovaném HW kolektoru, který zajistí prezentaci získaných dat.Součástí kolektoru bude SW modul - Flowmon Anomaly Detection Systém ve verzi Standard, pro pokročilou detekci anomálií chování v komunikační infrastruktuře, který pomáhá odhalit neznámé hrozby.

Systém pro monitoring systémů a komunikační infrastruktury

Nabízené řešení pro „Systém pro monitoring systémů a komunikační infrastruktury" bude realizováno monitorovacím nástrojem firmy Progress Software - WhatsUp Gold Premium 500 New Devices (5Y Service).

Odkaz na parametry nabízeného řešení:

https://www.whatsupgold.com/docs/librariesprovider2/default-document-library/ds-wug-premium.pdf?sfvrsn=70c21e2d_71

Nabízený monitoring systém splňuje požadavky uvedené v zadávací dokumentaci a bude sloužit k monitoringu dostupnosti systémů a komunikační infrastruktury.

Notifikace o změnách stavů a překročení prahových hodnot mohu být realizovány prostřednictvím SMTP mail systém ZZS, SMS systém ZZS (MobilChange), Mobilní aplikace SOSNow a MedText.

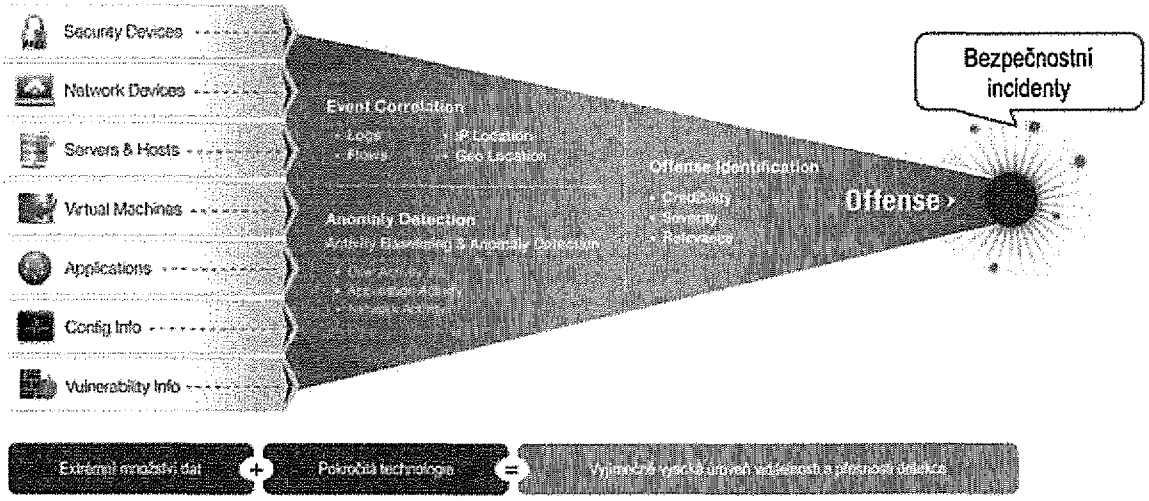
Provoz monitorovacího SW bude realizován na samostatném odděleném HW, který bude součástí dodávky řešení a bude připojen dvěma nezávislými porty do centrálního L3 switche. Monitorovací SW nebude tak (kromě centrálního L3 SW) závislý na infrastruktuře, kterou monitoruje.

4.4.4 Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí

Nabízené řešení plně splňuje požadavky uvedené v zadávací dokumentaci.

Uchazeč nabízí SIEM systém postavený na produktu IBM Security QRadar SIEM Suite.

IBM Security QRadar SIEM (dále též QRadar SIEM nebo QR SIEM) obsahuje všechny funkcionality moderních SIEM systémů. QRadar SIEM bude automaticky sbírat, archivovat a analyzovat data, zahrnující logy bezpečnostní povahy, síťová flow a zranitelnosti napříč celou infrastrukturou Objednatele. A to od síťových prvků přes různé operační systémy až po specifické aplikace Zadavatele. Nad těmito daty bude probíhat pokročilá analýza, korelace událostí a notifikace vyhodnocených bezpečnostních událostí a dalších fenoménů. Díky SIEM budou mít správci aktuální přehled o potenciálních i skutečných anomáliích, hrozbách a bezpečnostních incidentech monitorovaného prostředí.



Zařízení QRadar SIEM tvoří škálovatelná řešení, která jsou již po instalaci předkonfigurována a určena k co nejrychlejšímu nasazení v prostředí zákazníka. Dodávají se v podobě licence, kterou je možné nasadit na appliance (HW společně s OS a QRadar SW – výrobce Lenovo a DELL), jakýkoliv serverový fyzický nebo virtualizovaný HW splňující minimální parametry. Zařízení jsou instalována buď jako All-in-One nebo jako instalace jednotlivých komponenty pro stavbu distribuovaných QRadar infrastruktur (Console, Processor, Collector). Systém disponuje všemi charakteristickými komponentami dnešních SIEM (Security Information and Event Management) systémů. Jedná se o sběr, normalizaci, uložení, indexaci, korelaci, integraci externích bezpečnostních informací, identifikaci hrozeb, alerting, reporting a onLine prezentaci bezpečnostních událostí. Vše v prostředí jednotné management konzole. V nabízeném řešení SIEM počítáme s centrálním fyzickým serverem All-in-One. Licence operačního systému a databáze jsou součástí licencí pořízených produktů.

Centrální server má licenci na trvalé zpracování kontinuálního toku událostí a síťových flow z 80-ti serverů. Tuto hodnotu lze v době špiček několikanásobně překročit. Součástí je i licence pro neomezený příjem a parsování logů. Veškerý HW je navržen na trvalý tok 15.000 EPS. Centrální server pak navíc nemá žádná omezení na velikost SIEM úložiště a aktuálně je dimenzován na 18 měsíců RAW dat. Jedná se ale jen o limit nabízeného HW, licenčně není úložná kapacita nijak omezena. Počet sběrných konektorů (tzv. logsources) je neomezený. Stav (healthcheck) připojení každého konektoru je sledován a alertem indikován. Řešení není nijak omezeno počtem současně připojených administrátorů či operátorů. Zálohovaní konfigurace a denního přírůstku úložiště logů a flow je řešeno automatickou úlohou. Případná obnova je pak možná po jednotlivých dnech.

K dispozici je široká sada komunikačních protokolů jako je Syslog, Windows Events Collection (WinRM/ RPC), FTP, S/TP/SCP, SNMP, ODBC/JDBC, CP-LEA, SDEE, log file protokol. Mezi zdroji logů a

SIEM je možné použít šifrovanou komunikace, pokud to charakter komunikačního protokolu umožňuje.

Systém QRadar disponuje všemi charakteristickými komponentami dnešních Log Management a SIEM (Security Information and Event Management) systémů. Jedná se o sběr, normalizaci, uložení, full-text vyhledávání, archivaci, indexaci, předkonfigurovanou korelaci, identifikaci hrozeb, alerting, reporting (dle ISO27000:2013) a onLine prezentaci bezpečnostních událostí. Vše jako součást uceleného softwarového kódu v prostředí jednotné centrální grafické management konzole pro všechny komponenty. K dispozici je zároveň rozhraní příkazové řádky a některá nastavení je možné provést v klíčových konfiguračních souborech.

Všechna zařízení lze zapojit ve schématu vysoké dostupnosti čili jako dvou-uzlový cluster, bez nutnosti externích komponent třetích stran. Přechod na HA infrastrukturu je možné provádět za produkčního běhu celého systému. Úroveň oprávnění a viditelnosti vychází z principu RBAC a pro jednotlivé uživatele se odlišuje v závislosti na přidělených rolích. Základní role jsou v systému QRadar již předdefinovány a další je možné vytvořit. Role pokrývají nejen oblast připojených zdrojů ale i možnosti konfigurace, správy a práce v prostředí. Pro vlastní autentizaci (ověření) je možné integrovat QRadar s MSAD nebo obecným LDAP či RADIUS serverem a to v kombinaci s tím, že základní Admin účet a popřípadě další účty jsou lokální. Externí autentizace je možná prostřednictvím API, kdy QRadar vygeneruje pro každou externí aplikaci autentizační token. Jednotné centrální grafické rozhraní QRadar je standardní WEB aplikace nad aplikačním WEB serverem (tomcat).

Každý uživatel si může vytvořit vlastní pojmenované dashboardy a pohledy. V rámci těchto prvků je možné využít plně dril-down prohledávání až přímo k RAW události z logu či flow. Základní pohled je real-time pohled na nejnovější události tak, jak přicházejí. Při tvorbě pohledů a grafů je možné použít ad-hoc interaktivní vyhledávání s filtry nebo využít již předdefinované pohledy s grafy nebo vytvořit vlastní s využitím grafických filtračních polí a podmínek nebo též manuálně v dotazovacím poli s pomocí regulárních výrazů, či booleovy logiky. Předdefinované pohledy se především týkají plovoucích časových oken, omezení typu událostí podle kategorie nebo podle uživatele, či hostname nebo je možné změnit vzorkování dat. Takto připravené dotazy je možné uložit pro pozdější znovupoužití nebo je využít při tvorbě dalších pokročilých dotazů. Při tvorbě reportů je možné využít sady předdefinovaných reportů odpovídající regulačním nařízením (ISO 27000, PCI, SOX, HIPAA, apod.) nebo vytvářet v grafickém designeru vlastní reporty bez znalosti jazyka SQL a plánovat jejich pravidelné generování ve formátech RAW, PDF či CSV, XML a JSON. Počet reportů není nijak licenčně omezený.

Zařízení QRadar podporují především bezagentový sběr logů a flow z různých provozních prostředí. Informace proudící z těchto zdrojů je možné přijímat i v zabezpečené formě. Pro silné generátory logů je k dispozici lokálně instalovaný agent (WinCollect nebo tail2syslog). Podporovány jsou všechny hlavní formáty a protokoly sběru logů a flow jako je: Syslog, Windows Events Collection (WinRM/ RPC), FTP, S/TP/SCP, SNMP, ODBC/JDBC, CP-LEA, SDEE, log file protokol a další. Přímo do QRadaru je možné nasměrovat a obousměrně agregovat tok flow z analyzátorů datových toků (např. Flowmon). QRadar dokáže na základě prvních obdržených dat ze zdroje událostí tento zdroj oklasifikovat (switch Cisco, Linux Server, apod.) nebo pracovat s překrývajícími se adresními prostory zdrojů logů. Pro nerozpoznané zdroje logů je možné manuálně vybrat existující parser nebo je možné, ve vizuálním nástroji, nadefinovat vlastní nový. Položky v logu je možné rozčlenit do libovolného počtu atributů (tzv. custom properties). Informace o zdrojích logů lze importovat ve formě CSV seznamu. Nejčastěji vyhledávané položky se automaticky stávají předmětem agregace a vzniká pro ně samostatný index. Díky normalizaci logů nedochází ke změně jejich interpretace v souvislosti s technologickou změnou na zdroji. Seznam podporovaných zdrojů:

https://www.ibm.com/docs/en/dsm?topic=management-introduction-log-source

Události z logů a flow jsou v nedotčené podobě (RAW) ukládány a následně (near-real-time) vyhodnocovány předinstalovaným souborem pravidel, který je aktivovaný společně s oživením zařízení. Důležité je, že pravidla v systému posuzují logy a flow ve společných souvislostech, kdy dávají do souvislosti: hrozbu, zařízení, uživatele. Integrita uložených logů a flow je podepisována časovými razítky a je tak možné kdykoliv ověřit neměnnost uchovávaných dat. To, jak události z jednotlivých systémů budou uchovávány dlouho, řeší tzv. retenční politiky. Těch je možné definovat až 10 typů. Na starší data je aplikována komprimace. Stáří dat, která budou komprimována se nastavuje ve dnech.

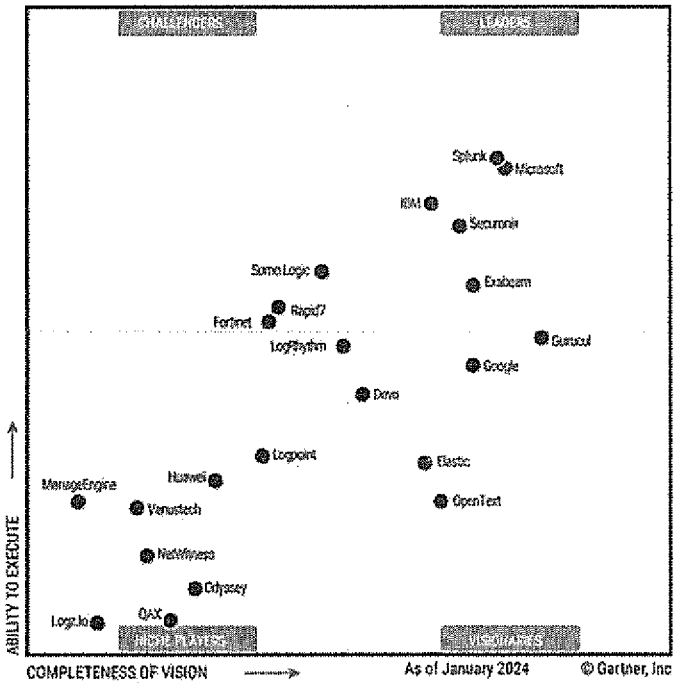
Systém QRadar disponuje integrovanou auditní komponentou, kdy ukládá a protokoluje veškeré úkony v něm provedené. Zároveň zařízení QRadar disponují interním monitoringem zdraví a běhu všech komponent. Na všechny zde zmíněné události jsou již automaticky nebo je možné dodatečně navázat alerty. Dále pro potřeby přístupům k datům a pro tvorbu programových a integračních rozšíření je možné využívat REST API rozhraní. https://www.ibm.com/docs/en/qradar-on-cloud?topic=administration-restful-api

Licenční nároky se řídí počtem požadovaného pokrytí 80-ti serverů převedených na počet RVU licencí produktu IBM Security QRadar Suite Software 100 Resource Unit License. Licence jsou nabízeny v programu Passport Advantage (nikoliv ESA) Jedná se o tyto licence:

D0AE4ZX	IBM Security QRadar Suite Software 100 Resource Unit License + Subscription & Support 12 Months Nové licence obsahující roční podporu. Měsíc 1-12.	16
2 x E0AE3ZX	IBM Security QRadar Suite Software 100 Resource Unit Annual Subscription & Support Renewal Obsahuje navazující 2-letou podporu. Měsíc 13-36.	16
2 x E0AE3ZX	IBM Security QRadar Suite Software 100 Resource Unit Annual Subscription & Support Renewal Obsahuje navazující podporu pro měsíc 37-60.	16

Umístění v Gartnerově kvadrantu (položka „IBM“):

Figure 1: Magic Quadrant for Security Information and Event Management



Gartner

Další požadavky této kapitoly, které neřeší SIEM, nabízíme následovně

Požadavek P.41

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 – Change Auditor for AD který zcela splňuje požadované vlastnosti. Nástroj bude instalován v prostředí AD ZZS.

Požadavky P.42 - 45

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 2 GB za den.

Nástrojem budou logovány minimálně:

1. Aktivní prvky (sítě)
2. Informační systémy – IS ZOS a systém elektronické pošty
3. Komunikační systémy – Pagingový systém
4. Databáze (ORACLE, MS SQL)
5. Operační systémy (MS Windows, Linux) – servery, pracoviště ZOS

Nástroj umožňuje samostatný přístup k různým službám pro různé osoby na základě oprávnění definovaného správcem a bude instalován na oddělený samostatný server (log server - popsán v kapitole 4.4.9).

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 Splunk 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:

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. E-mailová komunikace – přístupy (oprávněné a neoprávněné) včetně geolokace, chyby systému atd.

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:

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, elektronické pošty a pagingového systému (úspěšné i neúspěšné)
6. Zobrazení přehledu e-mailové komunikace ZZS (chyby, vytížení apod.)
7. 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 bude na 5 let včetně update SW a všech modulů.

4.4.5 Analytické nástroje ZOS pro vytváření bezpečnostních analýz

V rámci stávajícího analytického systému ORACLE BI (produkt SOS-BI), bude rozšířena datová základna o import a normalizaci dat bezpečnostních logů z aplikací IS ZOS.

Bude rozšířena datová pumpa pro získávání dat (bezpečnostních logů) z IS ZOS a budou vytvořeny vzorové analýzy nad bezpečnostními daty z hlediska pokusu o zneužití přístupu k jednotlivým aplikacím a modulům IS ZOS.

Uživatelé tohoto analytického nástroje pak budou schopni vytvářet vlastní analýzy nad bezpečnostními záznamy aplikací IS ZOS a budou tak schopni definovat požadavky na konfiguraci aktivních incidentů v rámci systému analýzy bezpečnostních logů. Systém analýzy bezpečnostních logů bude moci být aktualizován na základě konkrétních požadavků správců systému IS OŘ zjištěných v analytickém nástroji pro ZOS.

Budou stanoveny základní kategorie možných bezpečnostních incidentů a tomu bude přizpůsobena struktura uložení dat bezpečnostních logů v databázi datového skladu tak, aby byla optimální pro dané analýzy. Uživatel tak bude mít k dispozici snadno použitelné údaje v datových kostkách (oblasti dat).

Data bezpečnostních logů budou navázána na stávající datové objekty, jako jsou události (hlášení), výjezdy a pacienti.

Bude tak umožněno v analýzách vyhledávat anomální chování i na základě příslušnosti dat, ke kterým byl v aplikacích a modulech IS ZOS zachycen přístup. Například aktivní událost, výjezd a ošetření pacienta řeší určitý okruh zaměstnanců, kteří jsou v události, výjezdu a v kartě pacienta zaznamenaní (dispečer, posádka, doktor). Přístup k datům od uživatele mimo okruh těchto zaměstnanců může naznačovat bezpečnostní incident, který by, obzvlášť při četnějším výskytu u daného uživatele, měl být sledován a řešen.

Dodané řešení umožní analýzy bezpečnostních logů i na základě anomálií v časovém sledu. Například zaměstnancovo (uživatelovo) nezvyklé navýšení počtu prohlížených a/nebo modifikovaných záznamů v určitém měsíci / týdnu / dni oproti ostatním měsícům / týdnům / dnům může naznačovat bezpečnostní incident.

Budou možné analýzy na základě objemu dat, ke kterým uživatel modulu IS ZOS přistupoval oproti ostatním jeho kolegům ve stejné funkci (porovnání vůči standardnímu chování)

Bude možné dohledání detailů všech přístupů k datům na základě znalosti konkrétní události, resp. existujícího bezpečnostního incidentu / nahlášeného úniku dat.

Analytické nástroje pro vytváření bezpečnostních analýz budou provozovány na nově dodávané infrastruktuře (HW a systémový SW), přičemž stávající licence se nijak nezmění a součástí dodávky je systémová podpora na 5 let.

4.4.6 Úpravy IS ZOS

V této kapitole jsou popsány nabízené úpravy v IS ZOS tak, aby plně vyhovovaly požadavkům Zadavatele.

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)
- Telefonní ústředna
- Záznamový systém (REDAT)
- Integrace telefonie a radiofonie
- Aplikační SW na pracovištích 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:

- 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.

Napojení IS OŘ na komunikační prvky – izolace dispečinku

V rámci IS ZOS dojde k úpravám, kdy bude možné přijímat i aletry upozorňující na bezpečnostní události, a to nejenom z uvedených bezpečnostních prvků, ale všech komponent zabezpečení (např. prostřednictvím systému vyhodnocení logů). Bude se jednat o aletry bezpečnostních událostí relevantních k provozu centrálního dispečinku a celého IS ZOS s kritickou důležitostí. Bezpečnostní aletry v rámci IS ZOS budou definovány a konfigurovány na základě požadavků ZZS a dle toho zpracovány. IS ZOS tedy bude částečně plnit funkci SOC.

Oprávněné osoby centrálního dispečinku budou mít možnost pomocí rozhraní v IS ZOS 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 (např. provoz dispečinku v ostrovním systému). Vlastní izolace bude realizována na bezpečnostních/komunikačních prvcích integrací z IS ZOS. 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.

4.4.7 Dodávka a implementace technologií 802.1x pro zabezpečení přístupů do LAN sítě

Pro zabezpečení přístupů do síťové komunikační infrastruktury bude implementována technologie FortiNAC. Jedná se o řešení Network Access Control (NAC) ve formě virtuální appliance pro stávající virtualizační platformu, které zajistí kontrolu nad přístupem k síťovým zdrojům na bázi protokolu 802.1x.

FortiNAC bude integrován se stávající MS Active Directory, včetně DHCP serveru.

Řešení zajistí viditelnost koncových bodů v reálném čase, komplexní řízení přístupu, přesné třídění událostí a automatické řešení hrozeb v reálném čase. Součástí řešení je přehledný reporting o jednotlivých zařízeních (MAC adres). Reportovací sytém musí umožňovat získávat přehled i o připojených zařízeních do aktivních prvků, které nebudou podléhat autentizaci prostřednictvím 802.1x. Pro získávání těchto informací z některých prvků může jít o kombinaci navrženého řešení s dalším nástrojem.

Součástí dodávky a implementace je také nezbytný počet přepínačů s podporou protokolu 802.1x.

Konkrétně se jedná o řešení FNC-CAX-VM FortiNAC, FortiNAC Control and Application Extended-VM s licencí FortiNAC Pro License for 1K concurrent endpoint devices a podporou na 5 let a switche FS-148F-POE FortiSwitch-148F-POE a FS-124F-POE a FortiSwitch-124F-POE s podporou na 5 let.

Odkaz na parametry nabízeného řešení:
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinac.pdf
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortiswitch-secure-access-series.pdf

Část požadavku této kapitoly (požadavek P.75) řešíme na technologii Cisco.

Pro lokalitu Hradecká centrální redundantní prvek L3 prvek pro segmentaci sítě bude řešen dvěma prvky Cisco Systems Catalyst 9500 24x1/10/25G and 4-port 40/100G, Advantage (C9500-24Y4C-A) zapojenými do stacku.

Propojení switchů do jednoho stacku (přepínače se chovají jako jeden z pohledu managementu i připojených zařízení – včetně automatického loadbalancingu) bude realizováno vysokorychlostním redundantním datovým propojením 2x 100Gbps včetně kabelů (1 m). Při využití dvou uplinkových. Součástí dodávky bude i potřebné kabely (2x QSFP-100G-CU1Mkabely).

Součástí dodávky bude také dodávka těchto modulů pro každý ze switchů stacku (mimo materiál pro propojení do stacku):

4ks SFP-10G-SR 10GBASE-SR SFP Module

4ks SFP-25G-SR 25GBASE-SR SFP28 Module for MMF

Navržený model a konfigurace plně splňuje zadávací dokumentaci.

Pro centrální lokalitu bude realizována dodávka přístupových aktivních prvků typu přepínač s podporou 802.1x. Jedná se celkem o 2 ks přepínačů (switchů) které splňují požadované vlastnosti dle ZD. Bude řešeno dvěma prvky Cisco Systems C9200L-24P-4G-E Catalyst 9200L 24-port PoE+, 4 x 1G, Network Essentials.

Součástí dodávky je jak implementace (montáž, instalace, konfigurace, seznámení s funkcionalitami a obsluhou, dokumentace) tak potřebný drobný materiál (kabely apod.) pro připojení switchů do infrastruktury.

4.4.8 Zajištění šifrování v rámci komunikační sítě

Komunikační infrastruktura SD-WAN bude vybudována na platformě NGFW FortiGate. Fortinet Secure SD-WAN využívá pro zabezpečení komunikace mezi lokalitami pokročilé šifrovací technologie, které jsou integrovány přímo do zařízení FortiGate a jejich SD-WAN funkcionality.

Veškerá komunikace mezi pobočkami bude šifrována pomocí VPN tunelů na bázi protokolu IPsec. Tento protokol zajišťuje důvěrnost, integritu a autentizaci dat při přenosu přes veřejné i privátní sítě. IPsec je považován za průmyslový standard pro bezpečné šifrování WAN komunikace

FortiGate také umožní inspekci šifrovaného provozu (SSL/TLS), což může zvýšit úroveň bezpečnosti tím, že bude inspektován i šifrovaný provoz na aplikační vrstvě.

Správa všech zařízení FortiGate bude zajištěna nasazením virtuální appliance FortiManager, což je centralizovaná platforma pro správu bezpečnostních zařízení Fortinet. FortiManager zajistí správu konfiguraci, bezpečnostní politiky a aktualizace infrastruktury z jednoho rozhraní. Kromě firewallů Fortigate umožní FortiManager centrální správu dalších prvků jako jsou FortiAP, FortiSwitch a další.

Součástí dodávky a implementace bude také specializovaný logovací nástroj (FortiAnalyzer) pro sběr, uchování a analýzu log událostí z jednotlivých FW. Dodaná licence bude obsahovat tzv. retrospektivní analýzu, která umožní kontrolu zachycených událostí zpětně a jejich porovnání s nově objevenými zranitelnostmi.

Na jednotlivých lokalitách bude řešení FortiGate doplněno o zabezpečenou WiFi síť realizovanou na platformě FortiAP. Zabezpečení WiFi sítě bude realizováno jako WPA2-Enterprise s autentizací na bázi protokolu IEEE 802.1X a s šifrováním AES (Advanced Encryption Standard).

Konkrétně bude řešení postaveno na produktech FG-80F FortiGate 80F se softwarovým vybavením FC-10-0080F-809-02-60 Enterprise Protection (obsahujícím IPS, AI-based Inline Malware Prevention, Inline CASB Database, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium) a licencích FortiManager VM, FortiAnalyzer VM, Licence, 5 GB Logs/Day vše s podporou na 5 let.

Zabezpečená WiFi síť bude zrealizována na prvcích Fortinet FAP-231G-E FortiAP 231G s podporou na 5 let.

Správa zařízení bude řešena dvěma licencemi FMG-VM-10-UG FortiManager VM, Licence, 10 Device Add-on. Pro s podporou na 5 let.

Odkaz na parametry nabízeného řešení:

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-80f-series.pdf
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortiap-series.pdf
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf

Nabízené řešení v této kapitole plně splňuje požadavky uvedené v zadávací dokumentaci.

4.4.9 Infrastruktura (HW) a systémový SW pro běh dodávaného SW a technologií

Pro provoz navržených technologií a v souladu s požadavky zadavatele uvedených v této kapitole nabízíme 2 kusy virtualizačního serveru do stávajícího chassis DELL MX700 a to model DELL PowerEdge MX760C osazený procesorem Intel Xeon Gold 6430 2.1G, 32C/64T, 16GT/s, 60M Cache, podporou DDR5-4400, pamětí 8x 32GB RDIMM, 5600MT/s, Dual Rank, disky BOSS-N1 controller card + with 2 M.2 480GB - (RAID 1), kartou QLogic FastLinQ 41262 Dual Port 10/25GbE. Server obsahuje všechno požadované příslušenství a splňuje všechny požadavky definované v bodě P.90. Každý server bude dodán s operačním systémem Windows Server 2025 Datacenter pro potřebný počet core a licencí VMware vSphere Enterprise Plus pro potřebný počet core a podporou na 5 let. Záruční servis a podpora HW 7 let, SLA max. 4 + 4 hodiny po nahlášení závady s opravou v místě instalace, servis je poskytován výrobcem.

Pro všechny dodávané servery bude dodána licence Veeam Data Platform Foundation Universal Subscription License pro potřebný počet instancí s podporou na 5 let.

Pro zvýšení kapacity určené pro ukládání logů a dat z celé infrastruktury dodáme NAS Synology RS3621RPxs s hrubou diskovou kapacitou 240 TB a servisní podporu v místě instalace na 5 let.

Pro monitoring systémů a komunikační infrastruktury nabízíme server DELL PowerEdge R7615 osazený procesorem AMD EPYC 9254, 2.90GHz, 24C, 128M Cache, podporou DDR5-4800, pamětí 8x 16GB RDIMM, 5600MT/s, disky 2x 1.6TB SSD SAS ISE, Mixed Use, up to 24Gbps 512e 2.5in with 3.5in HYB CARR, AG Drive a 2x 4TB Hard Drive SAS ISE 12Gbps 7.2K 512n 3.5in Hot-Plug, AG Drive, kartami Broadcom 5720 Dual Port 1GbE LOM, Intel E810-XXV Dual Port 10/25GbE SFP28, OCP NIC 3.0 a zdroji Dual, Hot-Plug, Power Supply, 700W. Server obsahuje všechno požadované příslušenství a splňuje všechny požadavky definované v bodě P.92. Server bude dodán s operačním systémem Windows Server 2025 Standard pro potřebný počet core.

Pro provozování systému SIEM nabízíme server DELL model PowerEdge R760xs osazený procesorem Intel Xeon Silver 4514Y 2G, 16C R5-4800, pamětí 8x 16GB RDIMM, 5600MT/s, Single Rank, disky 10x 8TB Hard Drive SAS ISE 12Gbps 7.2K 512e 3.5in Hot-Plug, AG Drive, kartami Broadcom 57416 Dual Port 10GbE BASE-T Adapter, OCP NIC 3.0, Broadcom 57414 Dual Port 10/25GbE SFP28 Adapter, PCIe Low Profile, V2 a zdroji Dual, Hot-Plug, Power Supply Redundant (1+1), 1100W. Server obsahuje všechno požadované příslušenství a splňuje všechny požadavky definované v bodě P.92. Server bude dodán s operačním systémem podle požadavků systému SIEM.

Pro provozování logovacích nástrojů nabízíme server DELL model PowerEdge R760xs osazený procesorem Intel Xeon Gold 5416S 2G, 16C, pamětí 2x 16GB RDIMM, 5600MT/s, Single Rank, disky 5x 4TB Hard Drive SATA ISE 6Gbps 7.2K 512n 3.5in Hot-Plug, AG Drive, kartami PowerEdge R760xs Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM, MLK, Broadcom 5720 Quad Port 1GbE BASE-T Adapter, OCP NIC 3.0 a zdroji Dual, (1+1)RDNT, Hot-Plug PSU, 700W. Server obsahuje všechno požadované příslušenství a splňuje všechny požadavky definované v bodě P.93. Server bude dodán s operačním systémem Windows Server 2025 Standard pro potřebný počet core.

Servery pro monitoring, SIEM a logování budou dodány s podporou na 5 let typu NBD, s opravou v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení.

Nabízené řešení v této kapitole plně splňuje požadavky uvedené v zadávací dokumentaci.

4.4.10 Nástroje pro testování zranitelností a testování zranitelností

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.

Testy zranitelnosti

Budou 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, SOSView a MZD/EKP. 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.

Testy budou realizovány dle aktuální verze OWASP Web Security Testing Guide (WSTG) 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.

Výstupem testů zranitelnosti a penetračních testů bude závěrečná zpráva dle požadavků zadávací dokumentace.

4.4.11 Řízení aktualizací a vzdálená správa zabezpečovaných IS, provozní infrastruktury a bezpečnostních technologií

Následně je popsáno předpokládané naplněné jednotlivých požadavků z této kapitoly.

Požadavek P.110

Pro řešení řízení aktualizací bude vytvořen plán postupů aktualizací a jejich testování pro minimalizaci dopadů případných nekompatibilit na kritickou infrastrukturu.

Návrh bude splňovat minimální požadavky:

1. Definice postupů aktualizací na základě druhu systému a návazné infrastruktury.

2. Návrh rozdělení jednotlivých systémů a jejich návazností dle důležitosti. (např. telefonie 155, dispečink, podpůrné systémy, administrativa apod.) z pohledu nasazení a testování aktualizací.

3. Volba nástrojů výrobců pro aktualizace s návrhem zjednodušení a přiměřené automatizace procesů s pohledu zajištění maximální dostupnosti kritických systémů.

4. Implementace vybraných systémů aktualizací výrobců jednotlivých systémů.

5. Součástí dodávky bude i odzkoušení správnosti plánů postupů aktualizací a jejich průběžná aktualizace v rámci servisní podpory.

Požadavek P.111

Jako systém, který bude schopen identifikovat minimálně bezpečnostní aktualizace SW, a to napříč systémy (servery, DB, komunikační infrastruktura) a to minimálně pro základní systémy IS OŘ. Včetně evidence (inventarizaci) těchto zjištění bude využíván produkt, který již je uveden výše: „ Nessus Professional". Pro Windows servery a stanice IS OŘ předpokládáme doplnit identifikaci bezpečnostních aktualizací i pomocí stávajícího produktu FortiClient , který umožňuje na Windows stanicích a serverech, kde je nasazen, zjistit zranitelnosti a doporučit potřebné patche. Rovněž bude

možné využít navrhovaný produkt FortiManager, který umí provádět testy zranitelnosti, ohlásit problém a nalézt potřebné patche.

Požadavek P.112

V rámci dodávky bude také zpracován návrh procesů správy koncových a centrálních zařízení včetně implementace autentizace s využitím AD účtů.

Požadavek P.113

Jako systém pro audit pracovních stanic nabízíme nástroj MagikINFO – modul MagikAUDIT, který umožňuje následující:

1. Audit a evidence SW,
2. Evidence licencí,
3. Audit a evidence HW,
4. Evidence majetku včetně převodek a protokolů,
5. Vzdálené distribuce SW,
6. Vzdálená plocha a správa

Jedná se o licenci MagikINFO 18.5 Client a MagikINFO 18.5 Desktop, obě z modulu MagikAUDIT. Součástí dodávky je maintenance výrobce na 5 let.

Požadavek P.114

V rámci implementace jednotlivých komponent bude v případě možnosti exportu logů určených pro aktualizace jejich zasílání do centrálního systému logů včetně návrhu jejich zpracování, notifikací a reportů.

Požadavek P.115

V rámci servisní podpory bude realizována notifikace správcům o výskytu kritických zranitelností, které mají CVSS v3.x score větší než 7.0 a s tím související informace o dostupnosti relevantních kritických aktualizací pro prvky infrastruktury.

Požadavek P.116

V rámci implementace a licence monitorovacího systému WhatsUp Gold Premium bude sledováno využití / vytížení jednotlivých výpočetních prvků infrastruktury:

1. Všech serverů zabezpečovaných IS a dodávaných bezpečnostních technologií.
2. Koncových stanic IS ZOS.

Příloha č. 5: Nabídková cena – tabulka do ZD a nabídky

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	25.981.400,00 Kč	5.456.094,00 Kč	31.437.494,00 Kč
Celková nabídková cena za servisní služby dle vzorové Servisní smlouvy	9.921.600,00 Kč	2.083.536,00 Kč	12.005.136,00 Kč
Celková nabídková cena za plnění této VZ (dodávky i servisní služby)	**35.903.000,00 Kč**	**7.539.630,00 Kč**	**43.442.630,00 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 kalendářní čtvrtletí (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	Aplikační firewall pro IS ZOS	1 soubor	928.100,00 Kč	1.123.001,00 Kč			
2	Systémy pro monitoring systémů a komunikační infrastruktury	1 soubor	2.486.500,00 Kč	3.008.665,00 Kč			
3	Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí	1 soubor	5.959.700,00 Kč	7.211.237,00 Kč			
4	Analytické nástroje ZOS pro vytváření bezpečnostních analýz	1 soubor	1.350.000,00 Kč	1.633.500,00 Kč	575.100,00 Kč	9.201.600,00 Kč	11.133.936,00 Kč
5	Úpravy IS ZOS	1 soubor	1.230.000,00 Kč	1.488.300,00 Kč			
6	Dodávka a implementace technologií 802.1x pro zabezpečení přístupů do LAN sítě	1 soubor	3.796.600,00 Kč	4.593.886,00 Kč			
7	Zajištění šifrování v rámci komunikační sítě	1 soubor	3.645.900,00 Kč	4.411.539,00 Kč			
8	Infrastruktura (HW) pro běh dodávaného SW a technologií	1 soubor	1.801.400,00 Kč	2.179.694,00 Kč	---	---	---
9	Systémový SW pro běh dodávaného SW a technologií	1 soubor	1.545.600,00 Kč	1.870.176,00 Kč	---	---	---
10	Nástroje pro testování zranitelností a testování zranitelností	1 soubor	1.899.500,00 Kč	2.298.395,00 Kč	---	---	---
11	Řízení aktualizací a vzdálená správa zabezpečovaných IS, provozní infrastruktury a bezpečnostních technologií	1 soubor	830.000,00 Kč	1.004.300,00 Kč	---	---	---
Z	Rozšíření záruky u vybraných komponent nyd 36 měsíců (37 - 60 měsíc)	1 soubor	508.100,00 Kč	614.801,00 Kč	---	---	---
RP	Rozšířená podpora	30 hod / čtvrtletí	---	---	45.000,00 Kč	720.000,00 Kč	871.200,00 Kč
Celkem			**25.981.400,00 Kč**	**31.437.494,00 Kč**	**620.100,00 Kč**	**9.921.600,00 Kč**	**12.005.136,00 Kč**

Jednotková cena pro rozšířenou podporu (v Kč bez DPH): 1.500,00 Kč

Pokyny pro účastníka: Účastník vyplňuje jen zeleně zvýrazněné položky

Realizační tým

Role v realizačním týmu	**Vedoucí realizačního týmu**
Jméno, příjmení	[redacted]
Vztah k dodavateli (zaměstnanec / poddodavatel)	zaměstnanec
Role v realizačním týmu	**Technický specialista – zdravotnické operační středisko**
Jméno, příjmení	[redacted]
Vztah k dodavateli (zaměstnanec / poddodavatel)	poddodavatel
Role v realizačním týmu	**Technický specialista – analýza bezpečnostních logů IS ZOS**
Jméno, příjmení	[redacted]
Vztah k dodavateli (zaměstnanec / poddodavatel)	poddodavatel
Role v realizačním týmu	**Specialista řízení kybernetické bezpečnosti**
Jméno, příjmení	[redacted]
Vztah k dodavateli (zaměstnanec / poddodavatel)	zaměstnanec
Role v realizačním týmu	**Specialista řešení kybernetických bezpečnostních incidentů**
Jméno, příjmení	[redacted]
Vztah k dodavateli (zaměstnanec / poddodavatel)	poddodavatel
Role v realizačním týmu	**Specialista na penetrační testování**
Jméno, příjmení	[redacted]
Vztah k dodavateli (zaměstnanec / poddodavatel)	Poddodavatel [redacted]