Číslo Poskytovatele: S-JAKA-000237
Číslo Objednatele: ICT/2020/007

SMLOUVA NA SERVIS KOMUNIKAČNÍCH A INFORMAČNÍCH SYSTÉMŮ ZZS PAK

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

Smluvní strany:

Poskytovatel:

Název / jméno:	YOUR SYSTEM, spol. s r.o.
Sídlo:	Türkova 2319/5b, Praha 4, PSČ 149 00
Zastoupená:	RNDr. Martinem Nehasilem, jednatelem
IČ / DIČ:	00174939/CZ00174939
Plátce DPH:	Ano
Společnost zapsaná v:	OR vedeném Městským soudem v Praze, 18. července 1990, oddíl C, vložka č. 72
Bankovní spojení:	Uni Credit Bank Czech Republic, a.s.
Číslo účtu:	[redacted]
Kontaktní osoba:	[redacted]
Tel.:	[redacted]
Email:	[redacted]

dále jen „poskytovatel“

Objednatel:

Objednatel**:**	Zdravotnická záchranná služba Pardubického kraje
Sídlo:	Průmyslová 450, 530 03 Pardubice
Zastoupená:	MUDr. Igorem Paarem, ředitelem
IČ / DIČ:	69172196/ CZ69172196
Společnost zapsaná v:	OR u KS v Hradci Králové, pod sp. zn. Pr 715
Bankovní spojení:	ČSOB
Číslo účtu:	[redacted]
Kontaktní osoba ve věcech technických:	[redacted]
Kontaktní osoba ve věcech organizačních	[redacted]

dále jen „objednatel“

uzavírají níže uvedeného dne, měsíce a roku tuto

SMLOUVU:

I.
Úvodní ustanovení

1. Tato smlouva je uzavřena dle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „*občanský zákoník*“) za přiměřeného použití ustanovení upravujících smlouvu o dílo dle § 2586 a násl. občanského zákoníku a licenci dle § 2358 a násl. občanského zákoníku. Práva a povinnosti stran touto smlouvou neupravená se řídí příslušnými ustanoveními občanského zákoníku a 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 (dále jen „*autorský zákon*“).
2. Smluvní strany prohlašují, že údaje uvedené v záhlaví této smlouvy jsou v souladu s právním stavem platným v době uzavření smlouvy. Smluvní strany se zavazují, že změny údajů uvedených v záhlaví této smlouvy neprodleně písemně oznámí druhé smluvní straně. Smluvní strany prohlašují, že osoby podepisující tuto smlouvu jsou k tomuto úkonu oprávněny.
3. Poskytovatel podpisem smlouvy prohlašuje, že si prostudoval a detailně se seznámil se zadávací dokumentací veřejné zakázky s názvem: „**Kybernetická bezpečnost IS Zdravotnické záchranné služby Pardubického kraje“** ev. číslo P19V00000449 (dále jen „veřejná zakázka“) v rámci zadávacího řízení.
4. Tato smlouva navazuje na Smlouvu na dodávku komunikačních a informačních systémů ZZS ÚK (dále jen „smlouva na dodávku“) uzavřenou mezi smluvními stranami na základě veřejné zakázky. Tam, kde tato smlouva zmiňuje dílo, je míněn předmět plnění dle smlouvy na dodávku, tedy 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, ve znění pozdějších předpisů.
5. Poskytovatel potvrzuje, že se detailně seznámil s rozsahem a povahou servisu díla, že jsou mu známy veškeré technické, kvalitativní a jiné podmínky nezbytné k zajištění servisu díla a že disponuje takovou kapacitou a odbornými znalostmi, které jsou nezbytné pro zajištění servisu díla za dohodnutou maximální smluvní cenu uvedenou v článku IV. této smlouvy, a to rovněž ve vazbě na jím prokázanou kvalifikaci pro plnění veřejné zakázky.
6. Poskytovatel touto smlouvou garantuje objednateli splnění předmětu této smlouvy v souladu se zadáním veřejné zakázky a všech podmínek a povinností vyplývajících ze zadávací dokumentace zadávacího řízení veřejné zakázky. Tato garance plnění je nadřazena ostatním podmínkám plnění dle této smlouvy. Pro vyloučení veškerých pochybností smluvní strany prohlašují, že:
   a) v případě jakékoliv nejistoty ohledně výkladu ustanovení této smlouvy budou tato ustanovení vykládána tak, aby v co nejširší míře zohledňovala účel zadání veřejné zakázky dle příslušné zadávací dokumentace zadávacího řízení veřejné zakázky;
   b) v případě chybějícího smluvního ustanovení této smlouvy pro specifikaci, způsob, rozsah a charakter plnění budou adekvátně použita ustanovení dle příslušné zadávací dokumentace zadávacího řízení veřejné zakázky.

II.
Předmět smlouvy

1. Předmětem této smlouvy je závazek poskytovatele poskytovat servis díla zhotoveného a blíže specifikovaného na základě související a uzavřené Smlouvy na dodávku, a to nad rámec záruky, jak je definována ve smlouvě na dodávku a této smlouvě, a to v souladu se všemi závaznými právními předpisy, jakož i sjednanými podmínkami, a současně závazek objednatele hradit za poskytovaný servis díla cenu ve výši a za podmínek sjednaných touto smlouvou.

2. Poskytování servisu díla znamená zajištění technické a technologické podpory a nezbytných servisních služeb díla nad rámec záruk dle smlouvy na dodávku.
3. Servis díla zahrnuje zejména:
   - maintenance technologií a dodaného software, technickou a technologickou podporu,
   - nezbytné úpravy díla vyplývající ze změn legislativy, vyhlášek, případně dalších závazných dokumentů.
   - pozáruční servis HW a SW infrastruktury.
4. Podrobně je předmět smlouvy specifikován v příloze č. 1 smlouvy - Požadavky na servisní služby.

III.
Místo a doba plnění

1. Místy plnění jsou pracoviště objednatele, která jsou podrobně uvedena v příloze č. 1 smlouvy - Požadavky na servisní služby.
2. Servis díla bude poskytován od okamžiku předání a převzetí každé části díla dle smlouvy na dodávku.
3. Servis díla bude poskytován na dobu neurčitou od zahájení poskytování služeb dle této smlouvy.

IV.
Cena servisu

1. Cena za poskytování servisu díla je uvedena v příloze č. 3 smlouvy - Zpracování nabídkové ceny.
2. K ceně za provedení servisu díla bez DPH uvedené v příloze č. 3 smlouvy - Zpracování nabídkové ceny je poskytovatel oprávněn připočíst DPH dle aktuálně platné a účinné právní úpravy. Poskytovatel odpovídá za to, že jím účtovaná sazba daně z přidané hodnoty je stanovena v souladu s platnými a účinnými právními předpisy.
3. Součástí sjednané ceny za poskytování servisu díla je veškeré plnění, které se poskytovatel na základě této smlouvy zavázal poskytnout objednateli.

   Cena zahrnuje zejména, nikoliv však pouze:

   – veškeré náklady poskytovatele související s poskytováním servisu díla dle čl. II. smlouvy;
   – případné poplatky, jež bude muset poskytovatel při poskytování servisu díla dle čl. II. smlouvy uhradit;
   – zpracování veškerých nezbytných posudků, analýz a jiných odborných činností, které mohou být nezbytné pro řádné provedení servisu díla dle smlouvy;

   a dále vykonání všech ostatních činností tak, aby byl beze zbytku splněn předmět a účel smlouvy.
4. Součástí plnění předmětu této smlouvy jsou i práce v této smlouvě výslovně nespecifikované, které však jsou k řádnému plnění předmětu této smlouvy nezbytné a o kterých poskytovatel vzhledem ke své odbornosti a zkušenostem měl nebo mohl vědět a bez jejichž realizace se nedá zajistit servis díla, resp. jeho užívání objednatelem. Provedení takovýchto prací a dodávek se nepovažuje za vícepráce a nemá vliv na zvýšení ceny díla dle této smlouvy.
5. Rozsah servisu díla a cenu za poskytování servisu díla je možné měnit pouze písemným dodatkem k této smlouvě při respektování právní úpravy obsažené v zákoně č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“), případně jiném obecně závazném právním předpise upravujícím oblast veřejných zakázek.

V.
Platební podmínky

1. Zálohy na platby nejsou sjednány. Platby budou probíhat výhradně bezhotovostně v korunách

českých.

2. Podkladem pro úhradu ceny servisu díla, resp. jeho jednotlivých částí, jsou poskytovatelem vystavené daňové doklady (faktury), které musí mít veškeré náležitosti daňového dokladu dle zvláštních právních předpisů, zejména dle občanského zákoníku a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Faktura bude mít zejména tyto náležitosti:

   - označení daňového dokladu (faktury) a jeho číslo;
   - označení této smlouvy;
   - označení smluvních stran,
   - označení banky poskytovatele včetně identifikátoru a čísla účtu, na který má být úhrada provedena;
   - důvod fakturace, popis plnění;
   - den odeslání dokladu a lhůta splatnosti;
   - datum uskutečněného zdanitelného plnění;
   - částka k úhradě.

   Faktura dále musí obsahovat název projektu: „Kybernetická bezpečnost IS Zdravotnické záchranné služby Pardubického kraje“ a jeho registrační číslo: CZ.06.3.05/0.0/0.0/15_011/0006994.

3. Cena za poskytování servisu bude hrazena čtvrtletně – za období uplynulých tří měsíců (dále jen "zúčtovací období"). Faktury budou vystavovány vždy k poslednímu dni zúčtovacího období. Přílohou faktury proto vždy bude soupis plnění poskytnutého v zúčtovacím období.

4. Lhůta splatnosti jednotlivých faktur je 30 kalendářních dnů ode dne jejich doručení objednateli. Za den doručení faktury se považuje den uvedený na otisku razítka podatelny objednatele. Za okamžik úhrady faktury se považuje den, kdy byla předmětná částka odepsána z účtu objednatele.

5. V případě předložení vadné faktury, tj. faktury, která neobsahuje požadované údaje nebo obsahuje nesprávné údaje, není objednatel povinen takovou fakturu hradit. Objednatel je oprávněn vadnou fakturu před uplynutím lhůty splatnosti vrátit poskytovateli k provedení opravy. Ve vrácené faktuře objednatel vyznačí důvod vrácení. Poskytovatel provede opravu vystavením nové faktury. Nová 30denní lhůta splatnosti faktury začne běžet ode dne doručení nově vyhotovené faktury objednateli.

VI.
Způsob poskytování servisu díla

1. Poskytovatel se zavazuje poskytovat servis díla v souladu se všemi závaznými právními předpisy a podmínkami smlouvy.

2. Za účelem poskytování servisu díla je poskytovatel povinen opatřit si veškeré podklady, jež jsou nezbytné pro řádné poskytování servisu díla dle smlouvy. V souvislosti s povinností poskytovatele dle předchozí věty se objednatel zavazuje poskytnout poskytovateli nezbytnou součinnost, a to vyjma činností odborné povahy ve vztahu k předmětu této smlouvy.

3. Poskytovatel je povinen při poskytování servisu díla postupovat v souladu s podmínkami uvedenými v podkladech, jež mu byly zadavatelem předány.

4. Poskytovatel se zavazuje při plnění předmětu této Smlouvy spolupracovat a konzultovat průběh poskytování servisu díla či jeho částí dle této smlouvy s objednatelem, a to v rozsahu a způsobem dle požadavků objednatele, jinak v rozsahu a způsobem obvyklým pro plnění dle této smlouvy.

5. Poskytovatel je povinen upozornit objednatele bez zbytečného odkladu na nevhodnou povahu věcí převzatých od objednatele nebo požadavků, připomínek a pokynů daných mu objednatelem k plnění předmětu smlouvy, jestliže poskytovatel mohl tuto nevhodnost zjistit při vynaložení odborné péče.

6. Zjistí-li objednatel, že poskytovatel při provádění servisu díla dle smlouvy postupuje v rozporu se

svými povinnostmi, je oprávněn požadovat, aby poskytovatel bezodkladně odstranil vady vzniklé vadným poskytováním plnění dle smlouvy a aby při provádění servisu díla dle smlouvy postupoval řádně a v souladu se smlouvou. Neučiní-li tak poskytovatel ani v přiměřené lhůtě poskytnuté mu objednatelem, bude se tento stav považovat za podstatné porušení smlouvy ze strany poskytovatele.

7. Poskytovatel se zavazuje respektovat a dodržovat bezpečnostní politiku objednatele v rámci objednatelem nastaveného systému řízení bezpečnosti informací (dále jen „Systém řízení bezpečnosti informací“). Objednatel s tímto Systémem bezpečnosti informací seznámí poskytovatele před zahájením plnění dle této smlouvy a tento Systém bezpečnosti informací je pro poskytovatele závazný po celou dobu plnění předmětu této smlouvy.

VII.
Pojištění

1. Poskytovatel se zavazuje mít v průběhu trvání smlouvy uzavřenou pojistnou smlouvu mezi pojišťovnou a poskytovatelem v postavení pojištěného na pojištění rizik a odpovědnosti za škody způsobené při výkonu činnosti dle smlouvy s jednorázovým pojistným plněním minimálně ve výši 2 mil. Kč. Pojištění se poskytovatel zavazuje mít po celou dobu plnění smlouvy.
2. Náklady na pojištění nese poskytovatel a jsou zahrnuty v sjednaných cenách dle smlouvy.
3. Originál nebo ověřenou kopii dokladu o uzavření pojistné smlouvy předloží poskytovatel objednateli nejpozději do 10 dnů ode dne, kdy bude dle čl. III smlouvy zahájeno poskytování servisu díla. V případě změny pojištění předloží poskytovatel bezodkladně objednateli nový doklad prokazující uzavření příslušné pojistné smlouvy.
4. Poskytovatel se zavazuje uplatnit veškeré pojistné události související s poskytováním plnění dle smlouvy u pojišťovny bez zbytečného odkladu.

VIII.
Záruční podmínky a vady související s poskytováním servisu díla

1. Poskytování servisu díla má vady, jestliže neodpovídá požadavkům uvedeným ve smlouvě, požadavkům, připomínkám nebo pokynům uplatněným objednatelem v průběhu poskytování servisu díla, příslušným právním předpisům, technickým normám, smlouvě na dodávku komunikačních a informačních systémů ZZS PAK, nebo jiné dokumentaci vztahující se k servisu díla nebo pokud nesplňuje účel smlouvy.
2. Poskytovatel odpovídá za vady, jež má servis díla v době jeho provedení a za vady, které se projeví v záruční době, popřípadě v důsledku škody, za kterou odpovídá poskytovatel. Za vady servisu díla, které se projeví po záruční době, odpovídá poskytovatel jen tehdy, pokud jejich příčinou bylo prokazatelně porušení jeho povinností.
3. Poskytovatel poskytuje záruku na veškeré plnění servisu díla v délce 12 měsíců.
4. Záruční doba začíná běžet od okamžiku provedení opravy či úpravy nebo předání a převzetí technologie, na kterou se záruka vztahuje. Veškeré záruční opravy po dobu záruky budou poskytnuty bez dalších nákladů pro objednatele. Veškeré komponenty, náhradní díly a práce budou poskytnuty bezplatně v rámci záruky. Po dobu záruky musí poskytovatel nebo výrobce všech zařízení garantovat běžnou dostupnost náhradních komponentů a dostupnost servisu. Součástí záruky je i shoda dodávaných systémů s platnou legislativou.
5. Objednatel má právo uplatnit veškeré zákonné reklamační nároky. Volba reklamačního nároku je věcí objednatele.
6. Poskytovatel započne s odstraněním vady nejpozději do 7 dnů ode dne doručení oznámení o vadě, pokud se smluvní strany nedohodnou písemně jinak. Poskytovatel je povinen vadu odstranit nejpozději do 30 dnů ode dne doručení oznámení o vadě, pokud se smluvní strany nedohodnou písemně jinak.

7. Provedenou opravu vady poskytovatel objednateli předá písemně na základě příslušného předávacího protokolu. V předávacím protokolu o odstranění vady objednatel, resp. jím pověřená osoba, potvrdí odstranění vady nebo uvede důvody, pro které odmítá uznat vadu za odstraněnou. Pro provedenou opravu platí záruka za jakost ve stejné délce dle odstavce 3 tohoto článku smlouvy.

8. Neodstraní-li poskytovatel reklamované vady ve lhůtě 30 dní ode dne doručení oznámení o vadách, je objednatel oprávněn pověřit odstraněním reklamované vady jinou odborně způsobilou právnickou nebo fyzickou osobu. Veškeré takto vzniklé náklady uhradí poskytovatel do 14 dnů ode dne, kdy obdržel písemnou výzvu objednatele k uhrazení těchto nákladů. Uhrazením nákladů na odstranění vad jinou odborně způsobilou osobou podle tohoto odstavce není dotčeno právo objednatele požadovat na poskytovateli zaplacení sjednané smluvní pokuty a náhradu případné škody.

9. Záruční lhůta neběží po dobu, po kterou objednatel nemohl předmět díla byť jen z části užívat pro vady servisu díla, za které poskytovatel odpovídá. Uplatněním nároku z odpovědnosti za vady plnění není dotčen nárok objednatele na náhradu škody.

IX.
Poddodavatelský systém

1. Poskytovatel je oprávněn pověřit plněním částí předmětu této smlouvy třetí osobu, tj. poddodavatele. Poskytovatel odpovídá za činnost poddodavatele tak, jako by předmět této smlouvy plnil sám. Poskytovatel je povinen zabezpečit ve svých poddodavatelských smlouvách s poddodavateli splnění veškerých povinností poddodavatele tak, jak vyplývají poskytovatel z příslušných právních předpisů a dále z této smlouvy, a to přiměřeně k povaze a rozsahu poddodávky. Poskytovatel se zavazuje, že poddodavatel bude po celou dobu provádění poddodávky v rámci plnění předmětu této smlouvy splňovat požadavky stanovené zákonem. Poskytovatel je dále povinen zabezpečit, že poddodavatel bude seznámen se skutečností, že své činnosti a poskytování příslušných služeb musí provádět v souladu se zněním této smlouvy.

2. Poskytovatel je oprávněn v rámci plnění předmětu této smlouvy a v rámci jeho případného poddodavatelského systému pověřit plněním některých částí předmětu této smlouvy ty poddodavatele, jejichž prostřednictvím prokazoval v příslušném zadávacím řízení veřejné zakázky, na základě které byla uzavřena tato smlouva, kvalifikaci či které výslovně uvedl v rámci své nabídky v příslušném zadávacím řízení jako poddodavatele, kteří se budou podílet na plnění předmětu této smlouvy, tj. předmětu příslušné veřejné zakázky, nebude-li s objednatelem dohodnuto jinak. Poskytovatel 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 poskytovatele.

3. Poskytovatel není oprávněn v průběhu trvání této smlouvy pověřit plněním částí předmětu této smlouvy jiného dalšího poddodavatele (vyjma těch uvedených shora v odst. 2 tohoto článku této smlouvy) či změnit poddodavatele bez předchozího písemného souhlasu objednatele. Objednatel souhlas s pověřením či změnou poddodavatele dle tohoto článku poskytovateli nevydá, pokud:

   a) prostřednictvím původního poddodavatele zhotovitel v příslušném zadávacím řízení veřejné zakázky, na základě které byla uzavřena tato smlouva, prokazoval kvalifikaci a nový poddodavatel nebude mít odpovídající kvalifikaci či nebude naplňovat příslušná kvalifikační kritéria zadávacího řízení v rozsahu, v jakém tato kvalifikace byla poddodavatelsky prokázána, nebo

   b) nový poddodavatel nebude splňovat požadavky vyplývající z právních předpisů.

4. Poskytovatel 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 poskytovatel vstoupil s poddodavatelem ve smluvní vztah či ode dne, kdy nastala změna.

5. V případě realizace plnění dle této smlouvy prostřednictvím poddodavatele je poskytovatel povinen na žádost objednatele specifikovat části předmětu plnění, které plní pro poskytovatele jeho poddodavatelé, a to do 7 kalendářních dnů od doručení takové žádosti objednatele. Poskytovatel tak učiní písemně, kdy v takovém přípisu řádně a pravdivě uvede poddodavatelský systém společně s uvedením identifikačních údajů každého poddodavatele, rozsahu poddodávky, kterou bude tento poddodavatel provádět, a dále uvedením věcného a procentuálního podílu dodávky či služeb poddodavatele na realizaci předmětu plnění dle této smlouvy.

X.
Sankční ujednání

1. Pro případ prodlení objednatele se zaplacením ceny za poskytování servisu díla sjednávají smluvní strany zákonnou výši úroku z prodlení.
2. V případě prodlení poskytovatele se započetím s odstraněním vady anebo s odstraněním vady je poskytovatel povinen zaplatit objednateli následující smluvní pokuty dle kategorie vady, které jsou specifikovány v příloze č. 1 Smlouvy - požadavky na servisní služby:

Kategorie vady	Smluvní pokuta (v Kč)	Časový úsek
A	10 000	za každou započatou hodinu prodlení
B	5 000	za každý započatý den prodlení

3. V případě porušení povinnosti zhotovitele vyplývajících z ustanovení o Systému řízení bezpečnosti informací dle ustanovení čl VI. odst. 7 této smlouvy je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 50.000,- Kč za každý započatý den trvání takového porušení a každé jednotlivé porušení.
4. V případě porušení povinnosti zhotovitele vyplývajících z ustanovení o poddodavatelském systému plnění dle ustanovení čl IX. této smlouvy je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 20.000,- Kč za každý započatý den trvání takového porušení a každé jednotlivé porušení.
5. V případě porušení povinnosti zhotovitele vyplývajících z ustanovení o změně členů realizačního týmu dle ustanovení čl XIII. odst. 6 této smlouvy je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 20.000,- Kč za každé jednotlivé porušení.
6. V případě porušení povinnosti zhotovitele vyplývajících z ustanovení o tzv. exit strategii dle ustanovení čl XII. odst. 10 této smlouvy je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 30.000,- Kč za každý započatý den trvání takového porušení.
7. V případě porušení povinnosti zhotovitele vyplývajících z ustanovení o mlčenlivosti dle ustanovení čl XIII. odst. 3 této smlouvy je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 100.000,- Kč za každé jednotlivé porušení.
8. V případě porušení jiné povinnosti dle této smlouvy, za kterou není sjednána zvláštní smluvní pokuta dle ustanovení uvedených výše v tomto článku, má objednatel nárok na smluvní pokutu ve výši 5.000,- Kč za každý započatý den trvání takového porušení a každé jednotlivé porušení.
9. Zánik závazku pozdním splněním neznamená zánik nároku na smluvní pokutu za prodlení s plněním.
10. Sjednané smluvní pokuty zaplatí povinná strana nezávisle na zavinění a na tom, zda a v jaké výši vznikne druhé straně škoda.
11. Smluvní pokuty se nezapočítávají na náhradu případně vzniklé škody. Náhradu škody lze vymáhat samostatně vedle smluvní pokuty v plné výši (tj. nárok objednatele na náhradu škody není dotčen ujednáním o smluvní pokutě ani jejím zaplacením).

12. Smluvní pokuta je splatná ve lhůtě 15 dnů ode dne, kdy ji smluvní strana u druhé smluvní strany uplatnila. Objednatel je oprávněn smluvní pokuty započíst s jakoukoli pohledávkou poskytovatele vůči objednateli podle této smlouvy.

XI.
Licenční ujednání

1. Ochrana autorských práv se řídí autorským zákonem a veškerými mezinárodními dohodami o ochraně práv k duševnímu vlastnictví, které jsou součástí českého právního řádu.
2. Poskytovatel 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 poskytovatele dle této 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 této smlouvy.
3. Poskytovatel touto smlouvou poskytuje objednateli oprávnění užívat výsledky tvůrčí činnosti poskytovatele dle této smlouvy včetně jejich hmotného zachycení (dále jen „*licence*“) za podmínek sjednaných v této smlouvě. Právem užívat výsledky tvůrčí činnosti poskytovatele dle této smlouvy včetně jejich hmotného zachycení se ve smyslu této smlouvy rozumí nerušené využívání výsledků tvůrčí činnosti poskytovatele dle této smlouvy včetně jejich hmotného zachycení všemi známými způsoby v neomezeném rozsahu ve smyslu příslušných ustanovení občanského zákoníku a autorského zákona, včetně jejich dalšího zpracování, úpravy, rozmnožování, a to tak, aby byl naplněn účel této smlouvy.
4. Poskytovatel poskytuje licenci dle této smlouvy jako nevýhradní. Licence dle této smlouvy se poskytuje celosvětově na celou dobu trvání majetkových práv poskytovatele k autorskému dílu dle této smlouvy.
5. Objednatel je oprávněn práva tvořící součást licence dle této smlouvy poskytnout třetí osobě, a to ve stejném či menším rozsahu, v jakém je objednatel oprávněn užívat práv z licence sám, k čemuž se poskytovatel zavazuje udělit objednateli svůj souhlas.
6. Práva z licence poskytnuté touto smlouvou, přecházejí při zániku objednatele na jeho právního nástupce.
7. Nejpozději 12 měsíců před uplynutím doby plnění dle III. odst. 2 smlouvy je poskytovatel povinen poskytnout objednateli kompletní dokumentaci díla včetně zdrojových kódů veškerého software dodaného v rámci dodávky a servisu díla (dále jen „dokumentace díla“). Nejpozději 1 měsíc před uplynutím doby plnění dle III. odst. 2 smlouvy je poskytovatel povinen poskytnout objednateli aktuální verzi dokumentace díla.
8. V případě, že bude smlouva ukončena předčasně ve smyslu čl. XI. smlouvy, je poskytovatel povinen poskytnout objednateli dokumentaci díla nejpozději do 15 dnů od okamžiku, kdy se o ukončení smlouvy dozvěděl (uzavření dohody o ukončení smlouvy, doručení výpovědi smlouvy, doručení odstoupení od smlouvy).
9. Poskytovatel tímto výslovně souhlasí s tím, že objednatel je oprávněn dokumentaci díla využít k zajištění dalšího servisu a rozvoje díla a použít ji jako podklad v rámci zadávacího řízení na zajištění servisu díla.

XII.
Zánik smlouvy

1. Smlouvu lze ukončit buď dohodou smluvních stran, odstoupením od smlouvy kterékoliv ze smluvních stran, nebo výpovědí ze strany objednatele nebo poskytovatele.
2. Dohoda o ukončení smluvního vztahu musí být písemná, jinak je neplatná.
3. Objednatel je oprávněn smlouvu kdykoli v průběhu jejího trvání vypovědět i bez udání důvodu. Výpovědní doba činí tři měsíce a začíná běžet prvním dnem měsíce následujícího po měsíci, ve

kterém byla výpověď doručena poskytovateli.

4. Poskytovatel je oprávněn smlouvu vypovědět nejdříve po 5 letech trvání smlouvy a to i bez udání důvodu. Výpovědní doba činí šest měsíců a začíná běžet prvním dnem měsíce následujícího po měsíci, ve kterém byla výpověď doručena objednateli.

5. Objednatel i poskytovatel 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.

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

   a) prodlení poskytovatele se započetím s odstraněním vady anebo s odstraněním vady, dle kategorie vady, které jsou specifikovány v příloze č. 1 smlouvy - požadavky na servisní služby:

Kategorie vady	Prodlení
A	delší než 24 hodin
B	delší než 20 dnů

   b) postup při poskytování servisu díla způsobem, který zjevně neodpovídá dohodnutému rozsahu a způsobu poskytování,

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

7. 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.

8. V případě ukončení smluvního vztahu dohodou, odstoupením některé ze smluvních stran od smlouvy, nebo výpovědí objednatele jsou povinnosti obou stran následující:

   – poskytovatel provede soupis všech jím vykonaných činností a úkonů ke splnění jeho závazků dle této smlouvy za probíhající zúčtovací období do doby ukončení smlouvy;

   – objednatel uhradí poskytovateli cenu za poskytování servisu díla v alikvotní výši dané poměrem počtu dní probíhajícího zúčtovacího období, po které smlouva trvala, k celkovému počtu dní daného zúčtovacího období, přičemž platební podmínky se řídí čl. V této smlouvy.

9. Na poskytovatelem 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.

10. V případě předčasného ukončení této smlouvy (dále také „exit strategie“) má objednatel právo s pomocí poskytovatelem vypracované dokumentace pokračovat v plnění předmětu této smlouvy samostatně, nebo s jiným poskytovatelem. Poskytovatel se zavazuje v rámci exit strategie splnit tyto povinnosti:

   - vytvořit tzv. Exit plán, který bude přesně specifikovat postup pro přechodné období při případné předčasné ukončení smlouvy;
   - připravit podmínky novému poskytovateli nebo objednateli pro plnění předmětu této smlouvy na základě Exit plánu;
   - poskytnout požadovanou součinnost v souvislosti s předáním podpory a provozu systému novému poskytovateli;
   - řádně předat data zpracovávaná v systému (díle), včetně dat doplňkových či souvisejících;

- poskytnout informace nezbytné k převzetí systému (díla) novým poskytovatelem nebo objednatelem;
- poskytnout veškerou relevantní dokumentaci k podpoře provozu, k rozvoji systému (díla) a ke všem datovým strukturám (modelům, nastavením a dalším) v aktuálním stavu, které byly převzaty a vytvořeny v rámci plnění;
- předat objednateli prohlášení hlavních výrobců technologií s uvedením certifikovaných partnerů pro implementaci a následný support v České republice.

XIII.
Zvláštní ujednání

1. Poskytovatel je povinen chránit a zamezit přístupu k informacím, které objednatel označí za důvěrné. Závazky stanovené k ochraně informací objednatele, které jsou důvěrnými informacemi objednatele, platí i po zániku závazků ze smlouvy.
2. Poskytovatel je rovněž povinen poskytnout veškerou nezbytnou součinnost pro výkon finanční kontroly ve smyslu ust. § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, a to v souvislosti s prováděním díla dle smlouvy. Plnění smlouvy je financováno v rámci projektu „Kybernetická bezpečnost IS Zdravotnické záchranné služby Pardubického kraje“, registrační číslo CZ.06.3.05/0.0/0.0/15_011/0006994 (dále jen „Projekt“), který je realizován z výzvy č. 10 Integrovaného regionálního operačního programu (IROP) s názvem „KYBERNETICKÁ BEZPEČNOST“, prioritní osy PO 3: Dobrá správa území a zefektivnění veřejných institucí, specifického cíle SC 3.2: Zvyšování efektivity a transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality systémů IKT. Vzhledem k této skutečnosti je poskytovatel povinen mj. uchovávat veškerou dokumentaci nejméně po dobu 10 od finančního ukončení projektu, zároveň však alespoň do 31. 12. 2029. Poskytovatel je povinen minimálně do konce roku 2029 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 a poskytnout jim při provádění kontroly součinnost.
3. Poskytovatel má za 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 poskytovateli (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 poskytovatel má v souvislosti s ujednáním dle tohoto odstavce této smlouvy zejména povinnost zajistit:
   - mlčenlivosti vůči třetím osobám o veškerých skutečnostech, o nichž se dozvěděl v souvislosti s výkonem činnosti na základě této smlouvy;
   - 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;
   - 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;
   - povinnost mlčenlivosti osob, které pověří plněním této smlouvy, tj. zaměstnanců poskytovatele

a dalších osoby, které poskytovatel použije či pověří v souvislosti s poskytováním plnění dle této smlouvy (poddodavatelé);

- 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;
- 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.

4. Pokud je sdělení důvěrných informací třetí osobě nezbytné pro plnění závazků poskytovatele vyplývajících mu z této smlouvy, může poskytovatel 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 poskytovatel.
5. Tato smlouva bude zveřejněna v rozsahu údajů dle platných právních předpisů. Na takovéto zveřejnění se nevztahuje ustanovení bodů 2. a 3. tohoto článku.
6. Poskytovatel je povinen po celou dobu trvání smlouvy disponovat kvalifikací, kterou prokázal v rámci zadávacího řízení na veřejnou zakázku před uzavřením smlouvy. Poskytovatel se zavazuje, že veškeré osoby, které pověří plněním této smlouvy, tj. zaměstnance poskytovatele a další osoby, které poskytovatel použije či pověří v souvislosti s poskytováním plnění dle této smlouvy (poddodavatelé) (dále také „realizační tým“), budou po celou dobu trvání závazků z této smlouvy plynoucích splňovat příslušné kvalifikační předpoklady, jakož i dosahovat úrovně zkušeností deklarované v nabídce poskytovatele na veřejnou zakázku. Smluvní strany se také dohodly na minimálních požadavcích na složení realizačního týmu, kdy je změna členů realizačního týmu možná pouze za současného splnění následujících podmínek:

   a) poskytovatel objednateli předloží písemnou žádost o provedení změny člena realizačního týmu; s touto žádostí poskytovatel předloží rovněž doklady prokazující, že osoba, která se má stát novým členem realizačního týmu, splňuje kvalifikační předpoklady požadované objednatelem na člena realizačního týmu a

   b) objednatel schválí nového člena realizačního týmu; objednatel se k písemné žádosti vyjádří nejpozději do 5 pracovních dnů ode dne jejího doručení.

   Objednatel není povinen postupovat podle věty první písm. b) tohoto článku za předpokladu, že nový člen realizačního týmu nesplňuje příslušné kvalifikační předpoklady a nedosahuje úrovně zkušeností deklarovaných v nabídce poskytovatele na veřejnou zakázku.
7. Porušení povinnosti poskytovatele dle odstavce 6 tohoto článku se považuje za podstatné porušení povinností poskytovatele vyplývajících ze smlouvy a objednatel má právo na zaplacení smluvní pokuty ve výši dle čl. X. odst. 3 této smlouvy.

XIV.
Závěrečná ujednání

1. Smlouva nabývá platnosti dnem jejího podpisu smluvní stranou, která přijala nabídku – návrh na uzavření smlouvy. Smlouva nabývá účinnosti dnem předání a akceptace dodávky díla v souladu se Smlouvou na dodávku komunikačních a informačních systémů ZZS PAK ze dne 7.4.2020
2. Smluvní strany prohlašují, že mají plnou způsobilost k právnímu jednání, a smlouvu uzavírají svobodně a vážně, nikoliv v tísni za nápadně nevýhodných podmínek.
3. Smluvní strany prohlašují, že předmět plnění podle smlouvy není plněním nemožným a že smlouvu uzavírají po pečlivém zvážení všech možných důsledků. Poskytovatel prohlašuje, že se seznámil s předmětem smlouvy a že plnění může být poskytováno způsobem a v termínech stanoveným smlouvou.
4. Veškerá práva a povinnosti vyplývající ze smlouvy se řídí právním řádem České republiky.

5. 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.
6. Smlouva je vyhotovena v elektronickém originále a podepsána prostřednictvím uznávaného elektronického podpisu dle zákona č. 297/2016 Sb. o službách vytvářejících o důvěru pro el. transakce, ve znění pozdějších předpisů.
7. Poskytovatel esmí bez souhlasu objednatele postoupit svá práva a povinnosti plynoucí ze smlouvy třetí osobě.
8. Poskytovatel prohlašuje, že neporušuje etické principy, principy společenské odpovědnosti a základní lidská práva.
9. V případě plurality osob na straně poskytovatele se tyto osoby zavazují, že budou vůči objednateli a třetím osobám z jakýchkoliv právních vztahů vzniklých v souvislosti s plněním předmětu této smlouvy zavázáni společně anerozdílně, a to po celou dobu plnění smlouvy, i po dobu trvání jiných závazků vyplývajících ze smlouvy.
10. Vzhledem k veřejnoprávnímu charakteru objednatele se smluvní strany dohodly, že poskytovatel výslovně souhlasí se zveřejněním smluvních podmínek obsažených ve smlouvě v rozsahu a za podmínek vyplývajících z příslušných právních předpisů (zejména zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a zákona o registru smluv).
11. Smlouva podléhá povinnosti uveřejnění v registru smluv dle zákona o registru smluv. Smluvní strany se dohodly, že uveřejnění smlouvy v registru smluv zajistí objednatel.
12. Nedílnou součástí smlouvy je:
    Příloha č. 1: Požadavky na servisní služby
    Příloha č. 2: Popis navrhovaného řešení
    Příloha č. 3: Zpracování nabídkové ceny

Poskytovatel:	**Objednatel:**
V Praze, dne :	V Pardubicích dne:
……..	……..
RNDr. Martin Nehasil, jednatel YOUR SYSTEM, spol. s r.o.	Zdravotnická záchranná služba Pardubického kraje MUDr. Igor Paar, ředitel

PŘÍLOHA Č. 1 SERVISNÍ SMLOUVY: POŽADAVKY NA SERVISNÍ SLUŽBY

PŘÍLOHA Č. 2: SERVISNÍ SLUŽBY

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

OBSAH

SEZNAM PŘÍLOH

Nejsou.

VYUŽITÉ ZDROJE

[1] Technická specifikace

SEZNAM TABULEK

SEZNAM ZKRATEK A POJMŮ

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

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

Předmět plnění je tedy následující:

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

2 VÝCHOZÍ STAV

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

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

3 POŽADAVKY NA SERVISNÍ SLUŽBY

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

3.1 POSKYTOVANÉ SLUŽBY

Jsou požadovány následující služby:

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

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

3.2 PODMÍNKY POSKYTOVÁNÍ SLUŽEB

Druhy poruch:

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

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

Řešení poruch:

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

Způsob ohlašování poruch:

Poruchy Objednatel (oprávněné osoby Objednatele) hlásí na kontaktní místo Poskytovatele (Hot-line) prostřednictvím helpdesk, telefonicky a/nebo elektronickou poštou. Poruchy kategorie A objednatel vždy

hlásí telefonicky a doplňující informace poskytuje prostřednictvím helpdesk nebo elektronickou poštou. Kontaktní údaje a oprávněné osoby Objednatele jsou uvedeny v samostatné příloze smlouvy.

Reakce Poskytovatele:

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

Režimy

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

Lhůty

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

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

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

3.3 OSTATNÍ PODMÍNKY

Ostatní podmínky na poskytování základní podpory jsou:

1. Servisní výjezdy (práce a cestovní náklady) na území Pardubického kraje nebudou Poskytovatelem Objednateli účtovány (bezplatné plnění).
2. Legislativní úpravy systému v návaznosti na změny legislativy, vyhlášek a nařízení ČR a EU a zdravotních pojišťoven – v rámci paušální platby.
3. Poskytování součinnosti dalším poskytovatelům služeb zabezpečení provozu integrovaných systémů v rámci poskytování maintenance nebo základní podpory v rámci zabezpečení provozu.
4. V rámci provozu Systému bude v součinnosti Objednatele a Poskytovatele docházet k instalacím nových verzí SW, bezpečnostních a opravných balíčků systémového SW (OS, DB apod.) a obměna

HW a komunikační infrastruktury („modernizované provozní prostředí“). Služby budou na Systém poskytovány i na modernizované provozní prostředí, pokud bude zajištěno ve vzájemné součinnosti s Poskytovatelem nebo nebudou v rozporu se standartními požadavky na chod Systému.

4 ÚROVEŇ POŽADOVANÝCH SLUŽEB

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

#	Položka rozpočtu	Režim poskytování
1	FireWall(y) s IPS pro ZOS	24 x 7
2	Aplikační firewall pro IS ZOS	24 x 7
3	Systémy pro sběr dat (logů) o síťovém provozu	10 x 5
4	Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí	10 x 5
5	Analytické nástroje pro ZOS ZZS Pk	10 x 5
6	Pokročilé notifikační nástroje	10 x 5
7	Úpravy IS ZOS	24 x 7
8	Konfigurace systému elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů	10 x 5
9	Dvoufaktorová autentizace administrátorských VPN přístupů	24 x 7
10	Dodávka a implementace technologií 802.1x pro zabezpečení přístupů do LAN sítě	24 x 7
11	Zabezpečení systému elektronické pošty před škodlivým kódem	10 x 5
12	Kontrola přístupu do sítě Internet – webSecurity	10 x 5
13	Nástroje pro zajištění šifrování dat na PC/NB	10 x 5
14	Infrastruktura (HW) pro běh dodávaného SW	24 x 7
15	Systémový SW pro běh dodávaného SW	24 x 7

Tabulka 2: Úroveň požadovaných služeb

5 MÍSTA PLNĚNÍ

Realizace předmětu plnění bude probíhat v následujících místech plnění:

Místo	Adresa	Předmět realizace
Zdravotnická záchranná služba Pardubického kraje	**Průmyslová 450, Pardubice** PSČ: 530 03	Primární datové centrum ZZS PAK – návaznost na technologie umístěné v tomto DC a dodávka částí technologie. Poskytování servisních služeb pro dodané úpravy IS a technologie umístěné do této lokality.
Záložní zdravotnické operační středisko ZZS PAK a záložní datové centrum	Dr. Milady Horákové 1798/47, Chrudim	Záložní zdravotnické operační středisko ZZS PAK a záložní datové centrum pro toto ZZOS, kde bude umístěna dodaná technologie ZZOS a které bude propojeno s primárním datovým centrem ZZS PAK. Poskytování servisních služeb pro dodané úpravy IS a technologie umístěné do této lokality.

Tabulka 3: Místa plnění

6 OSTATNÍ PODMÍNKY

Kvalita a záruky:

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

Obnova dat, bezpečnost a pravidla pro update aplikace:

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

Servis vybavení prováděný pracovníky Objednatele:

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

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

KONEC ZÁKLADNÍ ČÁSTI DOKUMENTU

Příloha č. 2 Smlouvy o dílo a Smlouvy na servis: Popis navrhovaného řešení

Tato příloha je uvedena v nabídce Účastníka jako **Nabídka technického řešení** a je zpracována na základě požadavků Zadavatele uvedených v příloze č. 1 zadávací dokumentace (Technická specifikace).

1. OBSAH

2. 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
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

Zkratka/pojem	Význam
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
KB	Kybernetická bezpečnost
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
PAK	Pardubický kraj
PČR	Policie České republiky
PD	Projektová dokumentace
PNP	Přednemocniční neodkladná péče
RCT	Radiový komunikační terminál radiové sítě Pegas/Matra
SaP	Síly a prostředky
SLA	Úroveň a podmínky poskytování služeb technické a technologické podpory
SMS	Krátká textová zpráva
SNMP	Simple Network Monitoring Protocol
SQL	Strukturovaný dotazovací jazyk pro práci v relačních databázích

Zkratka/pojem	Význam
SW	Software
TS	Technická specifikace
VPN	Virtuální privátní síť
VŘ	Výběrové řízení
VZ	Veřejná zakázka
WAF	Webový aplikační firewall
WAN	Rozsáhlá počítačová síť
ZD	Zadávací dokumentace
ZKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
ZOS	Zdravotnické operační středisko
ZVZ	Zákon o zadávání veřejných zakázek
ZZOS	Záložní zdravotnické operační středisko
ZZS	Zdravotnická záchranná služba (ve všeobecném významu)
ZZS PAK	Zdravotnická záchranná služba Pardubického kraje

Tabulka 1: Seznam zkratek a pojmů

3. SHRNUTÍ PŘEDMĚTU A ROZSAHU DODÁVKY

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

Cílem projektu je zvýšení kybernetické bezpečnosti pro následující IS:

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

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

b) nástroj pro ochranu integrity komunikačních sítí

c) nástroj pro ověřování identity uživatelů

e) nástroj pro ochranu před škodlivým kódem

h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

j) kryptografické prostředky

i) aplikační bezpečnost

Rozsah dodávky a zároveň nabízeného plnění je následující:

#	Položka rozpočtu	Počet	Stručný popis položky
1	**FireWall(y) s IPS pro ZOS**	1 soubor	Dodávka Firewallu s IPS pro ochranu interní sítě ZZS, segmentů sítě ZZS a pro ochranu proti útokům z externích sítí v ZOS včetně zajištění vysoké dostupnosti. Součástí je dodávka, instalace, nastavení, propojení s dalšími síťovými prvky, implementace nastavení a pravidel a napojení na systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí a související služby.
2	**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.
3	**Systémy pro sběr dat (logů) o síťovém provozu**	1 soubor	Dodávka systémů pro sběr dat (logů) 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.
4	**Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí**	1 soubor	Dodávka systému analýzy bezpečnostních logů (OŘ/infrastruktura). Součástí je dodávka, instalace, nastavení, implementace nastavení a pravidel a související služby.
5	**Analytické nástroje pro ZOS ZZS PAK**	1 soubor	Dodávka analytického nástroje pro ZOS ZZS PAK pro vytváření bezpečnostních analýz. Součástí je dodávka, instalace, nastavení, implementace nastavení a pravidel a související služby.
6	**Pokročilé notifikační nástroje**	1 soubor	Dodávka pokročilého notifikačního nástroje nejenom pro bezpečností události ale i pro mimořádné události OŘ. Součástí je dodávka, instalace, nastavení, implementace nastavení a pravidel a související služby.
7	**Úpravy IS ZOS**	1 soubor	Úpravy IS ZOS v následujícím rozsahu: 1. pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů.

#	Položka rozpočtu	Počet	Stručný popis položky
			2. Autentizace uživatelů operačního řízení prostřednictví AD. 3. Integrace na personální systém. 4. Monitoring a reporting a přístupů. Součástí je dodávka úprav, implementace, nastavení a napojení na systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí a související služby.
8	**Konfigurace systému elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů**	1 soubor	Konfigurace systému elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů. Součástí je dodávka úprav nastavení, implementace, nastavení a napojení na systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí a související služby.
9	**Dvoufaktorová autentizace administrátorských VPN přístupů**	1 soubor	Dodávka a zavedení nástrojů pro dvoufaktorovou autentizaci administrátorských VPN přístupů Součástí je dodávka, implementace, nastavení a napojení na systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí a související služby.
10	**Dodávka a implementace technologií 802.1x pro zabezpečení přístupů do LAN sítě**	1 soubor	Implementace technologie 802.1x na přístupových switchích centrální lokality a výjezdových stanovišť. 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.
11	**Zabezpečení systému elektronické pošty před škodlivým kódem**	1 soubor	Dodávka technologií pro: 1. detekci spamů, nestandardní poštovní komunikace, definici politik pro antispam a filtrování komunikace. 2. ochranu proti webovým hrozbám Spyware/Adware/Phishing. 3. Možnost napojení na antivirové/antimalware programy. Součástí je dodávka, implementace, nastavení a napojení na systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí a související služby.

#	Položka rozpočtu	Počet	Stručný popis položky
12	**Kontrola přístupu do sítě Internet – webSecurity**	1 soubor	Ochrana před škodlivým kódem pro přístup do sítě internet musí disponovat následujícími vlastnostmi: 1. nasazení ochrany proti webovým hrozbám Spyware/Adware/Phishing včetně rychlé automatické aktualizace všech antimalware signatur. 2. podpora současného provozu více antimalware/antivir enginů. 3. URL filtrování dle kategorií (včetně možnosti uživatelského definování kategorií), dle web reputace, politik uživatelů, časového okna, dle objemových kvót apod. Součástí je dodávka, implementace, nastavení a napojení na systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí a související služby.
13	**Nástroje pro zajištění šifrování dat na PC/NB**	1 soubor	Dodávka nástrojů pro zajištění šifrování dat na PC/NB. Součástí je dodávka, implementace a související služby.
14	**Infrastruktura (HW) pro běh dodávaného SW**	1 soubor	Infrastruktura (HW) pro: 1. Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí 2. Nástroje pro ochranu před škodlivým kódem v rámci systému elektronické pošty Jedná se o datové úložiště, servery, implementaci a související služby.
15	**Systémový SW pro běh dodávaného SW**	1 soubor	Systémový SW pro: 1. Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí 2. Nástroje pro ochranu před škodlivým kódem v rámci systému elektronické pošty Jedná se o operační systémy, případně databázový SW, případně jiný SW nezbytný pro běh systému, implementaci a související služby.
16	**Nástroje pro bezpečnostní audit a penetrační testy**	1 soubor	Dodávka nástrojů pro bezpečnostní audit a testy zranitelnosti pro penetrační testy v souladu se standardy ZKB a závěrečných testů zranitelnosti z externí sítě na systémy IS ZOS a Elektronickou poštu a následné periodické testování bezpečnostních zranitelností systémů, které komunikují s externími subjekty.

#	Položka rozpočtu	Počet	Stručný popis položky
			Součástí je dodávka, instalace, nastavení, implementace a související služby.
17	**Bezpečnostní audit a penetrační testy**	1 soubor	Bezpečnostní audit a penetrační testy v souladu se standardy ZKB a závěrečných testů zranitelnosti z externí sítě na systémy IS ZOS a Elektronickou poštu.

Tabulka 2: Předmět a rozsah dodávky

4. PODROBNÝ POPIS NABÍZENÉHO PLNĚNÍ

V této kapitole je uveden podrobný popis navrhovaného a nabízeného řešení účastníka, členěný do kapitol po jednotlivých částech plnění.

Nabízená řešení jsou v souladu s požadavky na jednotlivé části plnění uvedené v Příloze č. 1 Technická specifikace uvedené v Zadávací dokumentaci.

4.1 FIREWALL(Y) S IPS PRO ZOS

Jako redundantní firewall s IPS pro řízení bezpečného přístupu mezi vnějšími sítěmi (internet, NIS IZS, PČR atd.) a vnitřní sítí ZZOS a ZOS nabízíme v souladu se ZD rozšíření stávajícího řešení Cisco Systems ASA 5516-X with FirePOWER services. Bude se tak jednat o dodávku jednoho HW FireWallu s požadovanými výkonnostními parametry, který rozšíří stávající řešení o další redundantní box a bude tak centrální FireWall konfigurován v HA režimu.

Tento FireWal bude doplněn licencí „Cisco ASA5516 FirePOWER IPS and AMP“ pro řešení požadavků ZD na Aplikační firewall a IPS senzor, která bud konfigurována ze vrámci stávajícího společného mamangementu.

Pro řešení VPN koncentrátoru bude nabízené řešení využívat stávající licenci „Cisco AnyConnect 25 User“, která zajišťuje požadované funkce pro celý redundantní FireWall.

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

Součástí implementace (montáž, instalace, konfigurace, zaškolení a seznámení s funkcionalitami a obsluhou, dokumentace) bude realizována konfigurace na základě požadavků ZZS s přihlédnutím ke konfiguraci stávajících oprávnění v rámci centrálního FireWallu v ZOS. Nastavení bude umožňovat bezproblémový chod IS OŘ (stávajících technologií) včetně využití připojení k externím sítím (Internet apod.). Pro konfiguraci přístupu vzdálených uživatelů v rámci VPN bude využito stejné konfigurace jako v stávající konfiguraci v době implementace FW (centrální RADIUS serverů).

Součástí implementace bude také:

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

Dále bude umožněna na dodávaném FireWallu možnost aktivace/deaktivace izolace systému IS ZOS od externích sítí nebo i od interních LAN/WAN segmentů ze systému IS OŘ (viz dále). V rámci řešení úpravy IS ZOS bude proveden detailní záznam událostí izolace systému IS ZOS včetně jejich časové souslednosti,

případně o uživatelích, kteří opatření realizovali, a to jak do logu IS OŘ, tak do systému analýzy bezpečnostních logů.

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.

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

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

Funkcionalita webového aplikačního firewallu (WAF) bude poskytovat ochranu webových aplikací před kybernetickými útoky s využitím pozitivní i negativní bezpečnostní logiky v bezpečnostních politikách (detekci a ochranu před známými útoky a povolení explicitního legitimního provozu s propustností 200Mbps. Nabízené řešení umožňuje bezpečnostních vlastností, jako je ochrana před útoky prolomením logovacích URL hrubou silou (Brute Force útoky) s možností eskalace a potlačení technologií CAPTCHA v případě podezření, že je aplikace pod útokem a technologie pro detekci a potlačení robotických (nelidských) uživatelů s možností výjimek (např. pro legitimní robotické klienty).

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

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

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

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

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

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

Součástí předávání logů do systému analýzy bezpečnostních logů:

- kritické bezpečnostní události související s chráněnými aplikacemi ZOS a případných útocích na ně vedených
- varování před nestandartními stavy jako jsou anomální nárůsty požadavků, pokusy o přístup do nepublikovaných částí aplikací apod.

logy o veškerých přístupech (úspěšné i neúspěšné) do managementu WAF a informace o změnách konfigurací WAF.

4.3 SYSTÉMY PRO SBĚR DAT (LOGŮ) O SÍŤOVÉM PROVOZU

Nabízené řešení bude v souladu s požadavky na 3 systémy pro sběr dat (logů) o síťovém provozu dle ZD.

Nabízená technologie je realizována na produktech firmy Flowmon Networks, a.s. Flowmon řešení nabízí požadované ucelené a škálovatelné řešení umožňující dlouhodobé i real-time monitorování sítě na bázi sledování toku založeného na technologii netflow složené z:

- Sondy síťového provozu (virtuální i fyzické)

- Kolektoru síťového provozu
- Modulu automatického vyhodnocování IP toků

4.3.1 Sonda pro virtualizační platformu

Jako sondu pro virtualizační platformu nabízíme produkt IFP-10000-VA (Flowmon Probe 10000 VA). Flowmon Probe 10000 VA disponuje jedním 10Gbps monitorovacím portem, je kompatibilní s virtualizačním prostředím ZZS (VMWare), virtualizačním prostředím dodávané infrastruktury a zcela splňuje požadavky ZD.

Flowmon sondy jsou výkonná autonomní zařízení, která monitorují provoz na počítačové síti, vytváří o něm statistiky v podobě IP toků a zasílají (exportují) je k uložení a další analýze na Flowmon kolektor či jinou kolektorovou aplikaci kompatibilní s NetFlow/IPFIX standardem. Tyto statistiky umožňují monitorování provozu na síti pro zajištění její bezpečnost a řešení provozních problémů.

Flowmon sondy ve formě virtuálních zařízení jsou určená pro instalaci do virtuálního prostředí (VMware, Hyper-V, KVM s OpenStack). Virtuální Flowmon sondy přináší stejnou funkcionalitu jako Flowmon sondy ve formě fyzických zařízení, ale díky instalaci do virtuálního prostředí umožňují navíc také monitorování síťového provozu v rámci virtuálního prostředí. Jednotlivé modely sond se liší v počtu a rychlosti monitorovacích portů. Všechny modely sond jsou kromě monitorovacích portů vybaveny dvěma administrativními (management) porty (sonda IFP-1000-VA je vybavena jedním). Na rozdíl od Flowmon sond ve formě fyzických zařízení virtuální Flowmon sondy neobsahují vestavěný kolektor, proto je pro sběr a analýzu NetFlow/IPFIX dat nutné použít samostatný Flowmon kolektor.

4.3.2 Fyzická sonda

Jako fyzickou sondu nabízíme produkt IFP-1000-CU (Flowmon Probe 1000 CU). Flowmon Probe 1000 CU disponuje jedním 1Gbps monitorovacím portem a zcela splňuje požadavky ZD.

Hardwarové Flowmon sondy jsou výkonná autonomní monitorovací zařízení pro všechny typy sítí od 10 Mb/s do 100 Gb/s. Sondy sledují komunikaci na počítačové síti a vytvářejí NetFlow/IPFIX statistiky. Sondy jsou nabízeny ve standardní a Pro verzi s různými počty a typy monitorovacích portů. Všechny modely hardwarových Flowmon sond obsahují vestavěný kolektor pro sběr, vizualizaci a analýzu NetFlow/IPFIX dat – Flowmon Monitorovací Centrum (FMC). Vestavěný kolektor umožňuje sběr NetFlow/IPFIX dat pouze z dané sondy, pro sběr NetFlow/IPFIX dat i z dalších zdrojů je nutné použít samostatný Flowmon kolektor. Všechny modely sond jsou kromě monitorovacích portů vybaveny dvěma metalickým 10/100/1000 Mb Ethernet administrativními (management) porty (sonda IFP-1000-CU je vybavena jedním), které se používají pro konfiguraci, správu a export flow dat.

4.3.3 Kolektor síťového provozu

Jako kolektor síťového provozu nabízíme produkt IFC-R5-1000 (Flowmon Collector R5-1000). Flowmon Collector R5-1000 disponuje datovým úložištěm 1TB (RAID5), je plně kompatibilní s nabízenými sondami a zcela splňuje požadavky ZD.

Flowmon kolektory jsou výkonná zařízení pro sběr, zobrazení, analýzu a dlouhodobé uložení síťových statistik (NetFlow v5/v9, IPFIX, sFlow, případně další kompatibilní s technologií NetFlow) ze zařízení podporující technologii flow (switche, routery), Flowmon sond či jiných zdrojů. Funkcionalitu kolektorů je dále možné rozšířit pomocí přídavných modulů.

Všechny kolektory jsou vybaveny Flowmon Monitorovacím Centrem (FMC) – aplikaci s pro detailní analýzu dat ve formě grafů, tabulek, výpisů komunikací, automatický reporting a mnoho dalšího. FMC poskytuje na dashboardu kompletní přehled o dění v síti včetně dlouhodobých grafů s různými perspektivami, top N statistik, uživatelsky nastavených profilů, možnosti zobrazení dat až na úroveň komunikací a další.

Jednotlivé modely se liší diskovou kapacitou, typem použitého RAIDu, výkonností a rozměrem serveru (1U/2U).

Všechny modely kolektorů jsou vybaveny dvěma metalickým 10/100/1000 Ethernet administrativními (management) porty, které se používají pro konfiguraci, správu a sběr flow dat.

4.3.4 Modul automatického vyhodnocování IP toků

Jako produkt pro automatické vyhodnocování IP toků nabízíme rozšíření nabízeného kolektoru IFC-R5-1000 o produkt FPC-ADS-S (Flowmon ADS Standard). Flowmon ADS Standard disponuje výkonem zpracování 1000 toků/s, je plně kompatibilní s nabízenými sondami, kolektorem a zcela splňuje požadavky ZD.

4.3.5 Instalace a záruka

Součástí dodávky je instalace a konfigurace dodávaného FlowMon řešení včetně součinnosti při konfiguraci síťových zařízení, poskytujících netflow informace o síťovém provozu.

Na nabízené řešení FlowMon je poskytována záruka 5 let, 5x8, garantovaná doba opravy do následujícího pracovního dne na místě včetně aktualizace SW.

4.4 Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí

V následující kapitole je popsáno nabízený systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí.

4.4.1 Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí

Nabízíme jako základní produkt SW nástroje pro sběr dat (logů, alertů a dalších vstupů) a vyhodnocení kybernetických bezpečnostních událostí ze zabezpečovaných informačních systémů, infrastruktury, HW, systémového SW a technologií včetně IS ZOS a systému elektronické pošty systém IBM QRADAR Software + 1x Event Capacity 100EPS (celková kapacita 200EPS s možností rozšíření na 5000EPS)

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

Nabízené řešení QRADAR plně splňuje požadavky uvedené v ZD P.40 a to jak výkonové, tak funkční.

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

Základní vlastnosti:

- Shromažďování logů o událostech ze zařízení a aplikací na síti
- Komplexní zpracování, korelace a vyhodnocení shromážděných logů a flows v reálném čase
- Monitorování chování v síti, tvorba přehledných reportů a přístup ke všem informacím z řešení webové konzole
- Identifikace a kategorizace zranitelností

- Informace o nalezené zranitelnosti, popis hrozby při jejím potenciálním zneužití a případné návrhy řešení, jak mezeru odstranit.
- Možnost filtrováni nalezených zranitelností a jejich priorizace.
- Možnost nad filtry zranitelností vytvářet pravidla pro korelaci
- Podpora operačních systémů Windows/Linux, mnoha síťových zařízení (routery, firewally), databází, webových serverů, mail serverů, DNS a mnoha dalších

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

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

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

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

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

4.4.2 Nástroj pro logování z IT infrastruktury

Pro analytickou práci s logy aplikací, bezpečnostních a síťových systémů využívaných v rámci ZZS nebo dodávaných v rámci dodávky nabízíme rozšíření systému analýzy bezpečnostních logů o nástroj pro logování z IT infrastruktury – SPLUNK Enteprise s licencí logovaných dat do 2 GB za den.

Nástrojem budou logovány minimálně:

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

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

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

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

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

Minimálně následující náhledy:

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

4.4.3 Jednotný bezpečnostní portál

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

Webové rozhraní:

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

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

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

4.5 Analytické nástroje pro ZOS ZZS PAK

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.

4.6 POKROČILÉ NOTIFIKAČNÍ NÁSTROJE

Nabízíme požadovaný pokročilý notifikační nástroj zcela v souladu se ZD.

Pokročilý notifikační nástroj bude propojen se systémem operačního řízení (IS OŘ) a napojen na stávající telefonní systém. S následujícími požadovanými funkcemi:

- Aplikační rozhraní pro uvedené funkce pro systém operačního řízení (IS OŘ), a pro monitorovací systém.
- Instalace ve virtualizovaném prostředí VMWare s možností migrace v rámci virtualizované platformy (nezávislost na HW).
- U všech hlasových úloh možnost programově nastavit číslo volajícího v rámci aplikačního rozhraní (v součinnosti s konfigurací stávající telefonní ústředny).
- Hlasové úlohy:
    - Prozvánění k výjezdu.
    - Přehrání hlasové zprávy pomocí převodu textu na hlasovou zprávu (text-to-speach) s podporou češtiny.
    - Přehrání zprávy s očekávanou návratovou hodnotou (v podobě tónové volby) – například Ano/Ne, přičemž dotaz a způsob odpovědí je zadáván konfiguračně v rámci systému operačního řízení (IS OŘ) a předáván aplikačním rozhraním.
    - Kapacita hlasového svolávání až 30 hlasových spojení v jednom okamžiku.
    - Úprava systému operačního řízení pro napojení na notifikační nástroj
- SMS úlohy
    - Odesílání SMS, a to prostřednictvím internet připojení – stávající „O2 Connector“ (zajistí Zadavatel) a pomocí GSM brány pro 4 SIM. Primárně přes „O2 Connector“, záložní způsob přes GSM bránu.
    - Dodávka GSM brány pro 4 SIM integrované s nabízeným svolávacím systémem. GSM brána připojena k infrastruktuře pomocí IP protokolu (ethernet port). Vlastní SIM karty zajistí Zadavatel.
    - Licence notifikačního nástroje pro využití min. 1x SMS connector a 4x SIM.
    - Odesílání definovaných, případně uživatelsky modifikovaných zpráv.
    - Odesílání zpráv s dotazem na uživatele a přijetím a předáním jeho odpovědi dále do operačního řízení.
- Mobilní aplikace
    - Odeslání zpráv na mobilní zařízení
    - Odesílání zpráv s dotazem na uživatele a přijetím a předáním jeho odpovědi dále do operačního řízení.

- Podpora mobilních platforem min. iOS a Android
- Integrační úlohy
  - Vyhodnocení odpovědí svolávaných skupin uživatelů a jejich přehledné zobrazení.
  - Plná aplikační integrace s IS OŘ (viz kap. 3.4.10).

Integrace notifikačního nástroje do IS OŘ umožní využití všech technologií nástroje pro doručení požadované zprávy a bude tak možné při výpadku jakékoliv technologie (Internet, telefonie, GSM SMS) doručit požadovanou zprávu ke koncovému uživateli jinou dostupnou technologií.

Vlastní inicializaci notifikace bude možné provádět jak z IS OŘ, tak z monitorovacích systémů (jako upozornění na aktuální problém).

Zadavatel zajistí SIM karty a konektor k mobilnímu operátorovi pro odesílání SMS a SIP trunk pro hlasové služby. Pro odesílání zpráv do mobilní aplikace bude využito stávajícího internet připojení.

Notifikační nástroj bude provozován ve virtuálním prostředí na dodávané infrastruktuře (HW a systémový SW).

4.7 Úpravy IS ZOS

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

4.7.1 Úprava systémů IS ZOS

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

Vlastní úpravy systémů IS ZOS budou provedeny dle požadavků ZD.

Jedná se o systémy:

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

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

IS OŘ

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

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

- Svolávací systém
- Záznamový systém (REDAT)

- Integrace telefonie a radiofonie

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

Pro kontrolu přístupu k systémových prostředků OS systémů:

- Telefonní ústředna – API serveru
- Integrace telefonie a radiofonie
- Aplikační SW na pracovištích ZOS/ZZOS
- Systém GIS
- Systém sledování vozů

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

IS OŘ - napojení na pokročilé notifikační nástroje

V rámci IS OŘ bude realizovaná požadovaná integrace pokročilého notifikačního nástroje (viz výše) minimálně s následujícími rozsahu:

- Možnost zadávat text zprávy pro notifikace a to jak technologií hlasového svolávání (text-to-speach), tak pro SMS a datový kanál (mobilní aplikace).
- Možnost definování textu otázky a odpovědí pro úlohy svolávání vyžadující odpověď koncového uživatele. Integrace s vyhodnocením odpovědí koncových uživatelů v závislosti na typu svolávání.
- Předávání zprávy k odeslání notifikačním nástrojům přes integrační rozhraní
- a rozšíření o volitelné texty a využití funkce text-to-speach v rámci systému operačního řízení (IS OŘ) a to jak běžných informací, tak i modulu hromadného neštěstí.

EKP/MZD a IS Pojišťovna

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

AVL/GIS

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

Záložní IS ZOS (ZZOS)

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

4.7.2 Napojení IS OŘ na FireWall ZZOS

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

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

4.7.3 Autentizace uživatelů operačního řízení prostřednictvím AD

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

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

- IS OŘ
- EKP/MZD

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

4.7.4 Integrace s personálním systémem

Stávající personální systém VEMA bude rozšířen o integraci s centrálním MS Active Directory ZZS s četností minimálně 1x za den (VEMA ADR).

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

4.7.5 Monitoring a reporting a přístupů

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

Součástí dodávky bude nástroj pro reportingu všech změn provedených jednotlivými uživateli/administrátory v rámci Microsoft Active directory (AD) ZZS (počet aktivních uživatelů 600), tak aby bylo možné kontrolovat změny oprávnění, které byly v rámci AD provedeny.

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

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

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

4.8 KONFIGURACE SYSTÉMU ELEKTRONICKÉ POŠTY PRO ZAZNAMENÁVÁNÍ ČINNOSTI (LOGŮ) DO SYSTÉMU ANALÝZY BEZPEČNOSTNÍCH LOGŮ

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

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

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

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

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

Minimálně:

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

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

Pro vytváření dynamických ACL bude možné systémově nastavovat následující parametry:

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

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

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

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

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

4.9 DVOUFAKTOROVÁ AUTENTIZACE ADMINISTRÁTORSKÝCH VPN PŘÍSTUPŮ

Pro řešení požadavků na dvoufaktorovou autentizaci nabízíme řešení firmy ESET: „ESET Secure Authentication“ licencováno pro 10 uživatelů s zárukou na funkčnost, podpora a aktualizace po dobu 5 let, které plně splňuje požadavky ZD.

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

- FireWall Cisco ASA
- Firemní VPN a OWA

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

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

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

ESET Secure Authentication

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

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

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

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

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

Podporované operační systémy Windows server 2008–2019.

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

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

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

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

Nabízené řešení bude v souladu s požadavky na implementaci technologií 802.1x pro zabezpečení přístupů do LAN sítě dle ZD.

Pro zabezpečení přístupu do LAN/WAN sítě ZZS bude implementovaná technologie 802.1x na přístupových switchích (umožňující konfiguraci 802,1x) centrální lokality a výjezdových stanovištích. Vlastní implementace bude využívat pro ověření zařízení a uživatelů autentizaci v rámci RADIUS serverů Microsoft

NPS s integrací do jednotného Active Directory. Pro neautorizované zařízení a uživatele bude vytvořena v rámci jednotlivých lokalit i GUEST VLAN s definovaně omezeným přístupem do sítě.

Požadavky implementace:

- Integrace s RADIUS servery Microsoft NPS v rámci AD ZZS
- Konfigurace všech stávajících LAN prvků umožňujících konfiguraci 802.1x v rámci WAN sítě ZZS
- Vytvoření GUEST VLAN ve všech lokalitách WAN ZZS a její zabezpečení v rámci dostupných technologií v dané lokalitě
- Vzorová konfigurace PC a NB pro 802.1x
- Konfigurace speciálních zařízení (Tiskárny apod.) bez podpory 802.1x
- Testovací provoz implementace bez reálného odepření přístupu včetně vyhodnocení provozu
- Přechod do provozního režimu včetně odepření přístupu neautorizovaným zařízením

Implementace zajistí možnost informování správce infrastruktury 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.

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. Bude realizována i integrace s používanými DHCP servery Microsoft. Reportovací sytém umožní získávat přehled i o připojených zařízeních do aktivních prvků, které nebudou podléhat autentizaci prostřednictvím 802.1x.

Součástí implementace je i dodávka 2ks přepínačů s podporou 802.1x. Nabízíme řešení na switchích Cisco Systems „Catalyst 9200L 24-port PoE+, 4 x 1G“ které plně splňují výkonnostní a funkční požadavky dle ZD.

4.11 Zabezpečení systému elektronické pošty před škodlivým kódem

Nabízené řešení bude v souladu s požadavky na zabezpečení systému elektronické pošty před škodlivým kódem dle ZD.

Nabízíme plně redundantní řešení pro kontrolu poštovního provozu (EmailSecurity) s veřejnou sítí Internet, včetně antispamové a antivirové ochrany řešené virtuálními appliance „Cisco Email Security Appliance (ESA) Essentials Bundle(AS+AV+OF)“.

Nabízené řešení splňuje veškeré výkonnostní a funkční požadavky dle ZD a je licencováno pro 150 chráněných stanic a záruku na funkčnost, podpora aktualizace všech signatur a dodaného řešení po dobu 5 let.

Nabízené řešení bude formou dvou virtuálních appliance v centrální lokalitě provozované na dodávané infrastruktuře s možností rozšíření počtu virtuálních strojů včetně případné realizace testovacího prostředí se samostatnou virtuální appliance.

Licence umožňuje instalaci další virtuální appliance i v záložní lokalitě. Tato možnost bude řešena v rámci prováděcího projektu.

Systém Cisco Email Security Appliance bude z hlediska příjmu zpráv ze sítě internet předřazen stávajícímu systému elektronické pošty – v režimu tzv. Mail relay gateway. Tím bude zajištěna vyšší bezpečnost interního mail serveru.

V rámci implementace budou realizována konfigurace na základě požadavků Zadavatele, a to hlavně pro nastavení anti-spam akce a anti spam karantény a dalších uživatelských nastavení pro optimalizaci fungování systému EmailSecurity. Součástí implementace bude i napojení a předávání alertů a logů do systému analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí (viz výše). Po

realizaci konfigurace proběhne seznámení Zadavatele s funkcionalitami a obsluhou implementovaného řešení.

Za 1 měsíc a za 3 měsíce bude provedeno vyhodnocení provozu a doladění pravidel/nastavení na základě získaných dat během provozu implementovaného systému a dle požadavků Zadavatele.

Vlastní nastavení se může v průběhu provozu měnit v závislosti požadavcích Zadavatele i v rámci standardní servisní podpory.

Součástí dodávky bude nejenom instalace a konfigurace řešení ale i součinnosti při konfiguraci návazných technologií – centrálního mail serveru apod.

4.12 KONTROLA PŘÍSTUPU DO SÍTĚ INTERNET – WEBSECURITY

Nabízené řešení bude v souladu s požadavky na kontrolu přístupu do sítě internet - websecurity dle ZD.

Nabízíme plně redundantní řešení WebSecurity pro kontrolovaný a zabezpečený přístup uživatelů do sítě Internet řešené virtuálními aliance „Cisco Web Security Appliance (WSA) Web Premium SW Bundle (WREP+WUC+AMAL)“.

Nabízené řešení splňuje veškeré výkonnostní a funkční požadavky dle ZD a je licencováno pro 150 chráněných stanic a záruku na funkčnost, podpora aktualizace všech signatur a dodaného řešení po dobu 5 let.

Nabízené řešení bude formou dvou virtuálních appliance v centrální lokalitě provozované na dodávané infrastruktuře s možností rozšíření počtu virtuálních strojů včetně případné realizace testovacího prostředí se samostatnou virtuální appliance. Licence umožňuje instalaci další virtuální appliance i v záložní lokalitě. Tato možnost bude řešena v rámci prováděcího projektu.

Nabízené řešení podporuje protokol VRRP který umožní vytvořit cluster virtuálních appliance na virtuální IP adrese včetně možnosti balancování. Druhou možností je využívání konfiguračního souboru PAC anebo WPAD. Tato technologie umožní možnost rozšíření redundance i s využitím záložní lokality ZZOS.

Navrhujeme s ohledem na možnost využití lokality ZZOS variantu PAC/WPAD souboru s možností využití instalace virtual appliance řešeení WSA i v lokalitě ZZOS

Systém Cisco Web Security Appliance bude z hlediska přístupu do sítě internet v režimu proxy a v rámci sítě bude nastaven přístup do sítě internet prostřednictvím WSA appliance. Tím bude zajištěna vyšší bezpečnost koncových stanic ZOS, které tak nabudou do sítě internet přistupovat přímo ale přes WSA

V rámci implementace budou realizována konfigurace na základě požadavků Zadavatele, a to hlavně pro nastavení pravidel přístupu a omezení do sítě internet a dalších uživatelských nastavení pro optimalizaci fungování systému WebSecurity. Součástí implementace bude i napojení a předávání alertů a logů do systému analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí (viz výše). Po realizaci konfigurace proběhne seznámení Zadavatele s funkcionalitami a obsluhou implementovaného řešení.

Za 1 měsíc a za 3 měsíce bude provedeno vyhodnocení provozu a doladění pravidel/nastavení na základě získaných dat během provozu implementovaného systému a dle požadavků Zadavatele.

Vlastní nastavení se může v průběhu provozu měnit v závislosti požadavcích Zadavatele i v rámci standardní servisní podpory.

Součástí dodávky bude nejenom instalace a konfigurace řešení ale i součinnosti při konfiguraci návazných technologií – centrálního mail serveru apod.

4.13 NÁSTROJE PRO ZAJIŠTĚNÍ ŠIFROVÁNÍ DAT NA PC/NB

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

Jako nástroj pro zajištění šifrování dat na PC/NB nabízíme produkt SODAT Encryption v rozsahu 20 licencí pro PC/NB, záruka na funkčnost a podpora aktualizace dodaného řešení po dobu min. 5 let, který plně splňuje ZD.

SODAT Encryption chrání data a informace uložené v počítačích, noteboocích a dalších zařízeních – ve firmě, na cestách i u zaměstnance doma. Zvolená data jsou bezpečně zašifrována s využitím standardizovaného algoritmu AES s délkou klíče minimálně 256 bitů a to technologií využívající „souborové“ šifrování a pro neoprávněnou osobu nečitelná, nezneužitelná.

SODAT Encryption zajišťuje ochranu proti připojování nepovolených externích USB zařízení. Přenosná datová zařízení používaná pro výměnu a sdílení dat zabezpečuje šifrováním. Identifikuje typ, výrobce a výrobní číslo zařízení, které lze implementovat do nastavených pravidel pro jednotlivce, skupiny nebo celou firemní doménovou síť a všechny její klienty.

Administrátorská konzole umožnuje provést instalaci i veškerá nastavení centrálně. Pravidla šifrování lze nastavit pro jednotlivce i skupiny uživatelů. Instalace a šifrování dat probíhá na pozadí. Klientská instalace komunikuje na pozadí s administrátorskou konzolí, posílá informace o ukončeném procesu šifrování a o dalších důležitých událostech. Klient nemůže svévolně nastavení měnit, dodržování bezpečnostních pravidel je snadno vynutitelné.

Administrátor může ihned změnit nastavení šifrovaných oblastí. Prostředí aplikace umožňuje také vidět stav šifrovaných i nešifrovaných souborů dle jejich užití a typu (dokumenty, media, výkresy, tabulky atd.).

4.14 INFRASTRUKTURA (HW) PRO BĚH DODÁVANÉHO SW

V této kapitole je popsána nabízená infrastruktura (HW) pro běh nabízeného SW.

4.14.1 Virtualizační servery

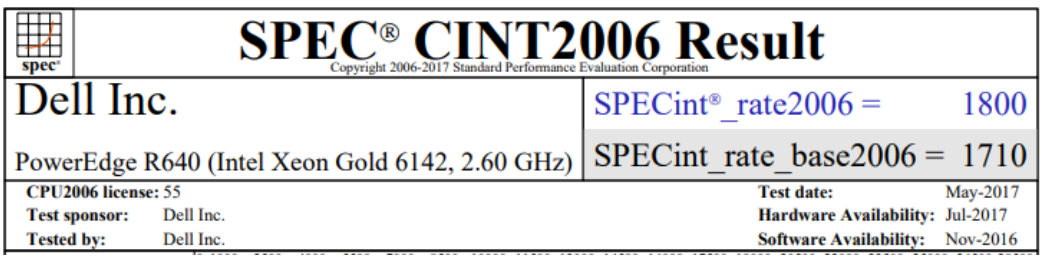
Virtualizační servery nabízíme servery firmy DELL PowerEdge R640 v konfiguraci plně splňující ZD.

Budou dodány celkem 3 kusy virtualizačních serverů ve stejné konfiguraci.

Servery jsou nabízeny s procesorem Intel Xeon Gold 6142 2.6G, 16C/32T, který splňuje požadavky ZD a je dostačující na požadovaný provoz dodávaného řešení

SPECint_rate2006 base min. 1700 bodů:

http://www.spec.org/cpu2006/results/res2017q3/cpu2006-20170807-48037.pdf



SPEC® CINT2006 Result

Copyright 2006-2017 Standard Performance Evaluation Corporation

Dell Inc.

PowerEdge R640 (Intel Xeon Gold 6142, 2.60 GHz)

SPECint®_rate2006 = 1800

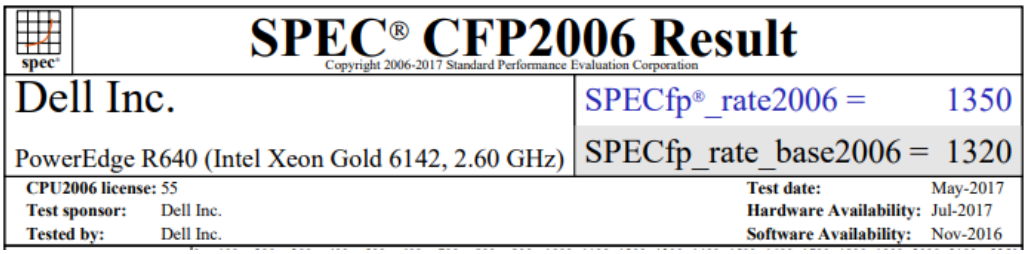
SPECint_rate_base2006 = 1710

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

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

SPECfp_rate2006 base min. 1300:

http://www.spec.org/cpu2006/results/res2017q3/cpu2006-20170807-48010.pdf



SPEC® CFP2006 Result

Dell Inc.

PowerEdge R640 (Intel Xeon Gold 6142, 2.60 GHz)

SPECfp®_rate2006 = 1350

SPECfp_rate_base2006 = 1320

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

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

Konfigurace Serveru PowerEdge R640 :

DELL PowerEdge R640
1 329-BDKC PowerEdge R640 Motherboard
1 338-BLMK Intel Xeon Gold 6142 2.6G, 16C/32T, 10.4GT/s 2UPI, 22M Cache, Turbo, HT (150W) DDR4-2666
1 379-BCSG iDRAC,Legacy Password
1 379-BCQV iDRAC Group Manager, Enabled
1 321-BCQJ 2.5 Chassis with up to 8 Hard Drives and 3PCIe slots
1 325-BCHG LCD Bezel
1 330-BBGY Riser Config 4, 2x16 LP
1 350-BBJS Dell EMC Luggage Tag
1 350-BBKB No Quick Sync
1 370-ADNM Blank for 1CPU Configuration
1 370-AAIP Performance Optimized
1 370-ADNU 2666MT/s RDIMMs
6 370-ADNF 32GB RDIMM 2666MT/s Dual Rank
1 385-BBCF Redundant SD Cards Enabled
2 385-BBKH 32GB microSDHC/SDXC Card
1 385-BBKT iDRAC9,Enterprise
1 385-BBLQ IDSDM and Combo Card Reader with 16GB VFlash SD
1 400-AZUT 480GB SSD SATA Mix Use 6Gbps 512 2.5in Hot-plug AG Drive, 3 DWPD, 2628 TBW
1 405-AANT PERC H730P RAID Controller, 2GB NV Cache, Mini card
1 412-AAIQ Standard 1U Heatsink
1 429-ABBF No Internal Optical Drive for x4 and x8 HDD Chassis
1 450-ADWS Dual, Hot-plug, Redundant Power Supply (1+1), 750W
2 450-AADY C13 to C14, PDU Style, 10 AMP, 6.5 Feet (2m), Power Cord
1 461-AAEM Trusted Platform Module 2.0
1 293-10049 Order Configuration Shipbox Label (Ship Date, Model, Processor Speed, HDD Size, RAM
1 389-DTIV PowerEdge R640 CE,CCC,BIS Marking
1 540-BBUL Broadcom 57412 2 Port 10Gb SFP+ + 5720 2 Port 1Gb Base-T, rNDC
1 540-BBVI Broadcom 57412 Dual Port 10Gb, SFP+, PCIe Adapter, Low Profile
1 750-AABF Power Saving Dell Active Power Controller
1 770-BBBL ReadyRails Sliding Rack Rails with Cable Management Arm
1 780-BCDS Unconfigured RAID
1 528-CHGB Windows Server 2019 Datacenter,No Media,WS2016 DC Downgrade DF Media, Multi Language,
1 528-CHGC Windows Server 2019 Datacenter,No Media,WS2012R2 DC Downgrade DF Media, Multi Language
1 384-BBPR 5 Standard Fans for R640
1 634-BLVV VMware ESXi 6.5 U3 Embedded Image on Flash Media (License Not Included)

1 634-BSFK Windows Server 2019 DataCenter,16CORE,Secondary OS,No MEDIA,Unlimited VMs
1 634-BSGO Windows Server 2019 Datacenter,No Media,WS2016 DC Downgrade Media, Multi Language
1 634-BSGJ Windows Server 2019 Datacenter,16CORE,Secondary OS,Media Kit, Multi Language
1 631-AACK No Systems Documentation, No OpenManage DVD Kit
1 528-BIYY OpenManage Enterprise Advanced
1 709-BBIM Basic Next Business Day 36 Months
1 865-BBMY ProSupport and Next Business Day Onsite Service Initial, 36 Month(s)
1 865-BBMZ ProSupport and Next Business Day Onsite Service Extension, 24 Month(s)

Tabulka 3: Konfigurace Serveru PowerEdge R640

Při realizaci bude odpovídat aktuální nabídce s tím, že splní veškeré podmínky ZD.

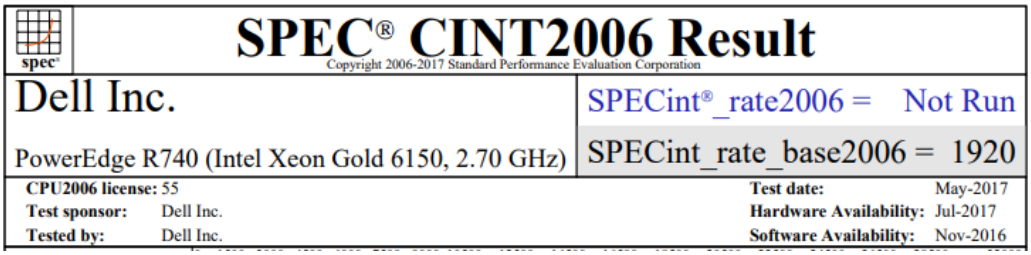
4.14.2 Logovací server

Logovací server nabízíme server firmy DELL PowerEdge R740 v konfiguraci plně splňující ZD.

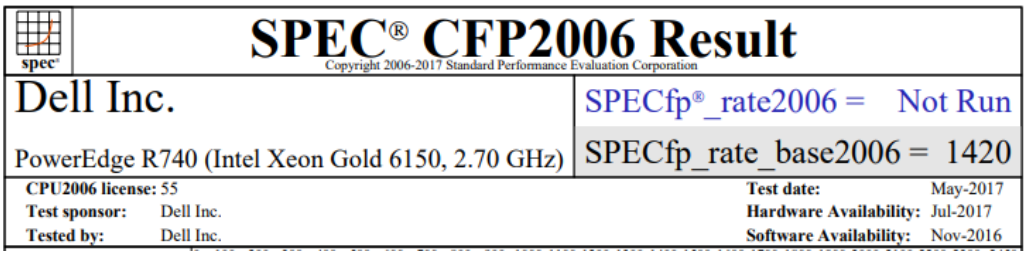
Server je nabízen s procesorem Intel Xeon Gold 6150 2.7G, 18C/36T, který splňuje požadavky ZD a je dostačující na požadovaný provoz dodávaného řešení

SPECint_rate2006 base min. 1700 bodů:

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


SPEC® CINT2006 Result
Copyright 2006-2017 Standard Performance Evaluation Corporation
Dell Inc.
PowerEdge R740 (Intel Xeon Gold 6150, 2.70 GHz)
SPECint®_rate2006 = Not Run
SPECint_rate_base2006 = 1920
CPU2006 license: 55
Test sponsor: Dell Inc.
Tested by: Dell Inc.
Test date: May-2017
Hardware Availability: Jul-2017
Software Availability: Nov-2016

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


SPEC® CFP2006 Result
Copyright 2006-2017 Standard Performance Evaluation Corporation
Dell Inc.
PowerEdge R740 (Intel Xeon Gold 6150, 2.70 GHz)
SPECfp®_rate2006 = Not Run
SPECfp_rate_base2006 = 1420
CPU2006 license: 55
Test sponsor: Dell Inc.
Tested by: Dell Inc.
Test date: May-2017
Hardware Availability: Jul-2017
Software Availability: Nov-2016

Konfigurace Serveru PowerEdge R740 :

DELL PowerEdge R740
1 329-BDKH PowerEdge R740/R740XD Motherboard
1 338-BLMO Intel Xeon Gold 6150 2.7G, 18C/36T, 10.4GT/s 2UPI, 25M Cache, Turbo, HT (165W) DDR4-2666
1 379-BCSG iDRAC,Legacy Password
1 379-BCQV iDRAC Group Manager, Enabled
1 321-BCSH Chassis with up to 8 x 3.5" SAS/SATA Hard Drives for 1CPU Configuration
1 325-BCHU PowerEdge 2U Standard Bezel
1 330-BBGZ Riser Config 1, 4 x8 slots
1 343-BBFG PowerEdge R740 Shipping Material

1 350-BBKG Dell EMC Luggage Tag
1 350-BBJV No Quick Sync
1 370-ADPF Blank for 1CPU Configuration
1 370-AAIP Performance Optimized
4 370-ADNI 8GB RDIMM, 2666MT/s, Single Rank
1 385-BBKT iDRAC9,Enterprise
1 385-BBLR VFlash Card Reader with 16GB Vflash SD card
3 400-AZVG 1.92TB SSD SATA Mix Use 6Gbps 512 2.5in Hot-plug AG Drive,3.5in HYB CARR, 3 DWPD, 10512 TBW
5 400-ASHY 4TB 7.2K RPM NLSAS 12Gbps 512n 3.5in Hot-plug Hard Drive
1 405-AAQU MOD,CRD,CTL,H730P,2GB,MCRD,14G
1 412-AAIR Standard 2U Heatsink
1 429-ABBJ No Internal Optical Drive
1 450-ADWS Dual, Hot-plug, Redundant Power Supply (1+1), 750W
2 450-AADY C13 to C14, PDU Style, 10 AMP, 6.5 Feet (2m), Power Cord
1 461-AAEM Trusted Platform Module 2.0
1 293-10049 Order Configuration Shipbox Label (Ship Date, Model, Processor Speed, HDD Size,RAM
1 540-BBBW Broadcom 5720 QP 1Gb Network Daughter Card
1 540-BBUH Broadcom 57412 Dual Port 10Gb, SFP+, PCIe Adapter, Full Height
1 750-AABF Power Saving Dell Active Power Controller
1 770-BBBR ReadyRails Sliding Rails With Cable Management Arm
1 780-BCDS Unconfigured RAID
1 384-BBPZ 6 Performance Fans forR740/740XD
1 619-ABVR No Operating System
1 631-AACK No Systems Documentation, No OpenManage DVD Kit
1 709-BBIM Basic Next Business Day 36 Months
1 865-BBMY ProSupport and Next Business Day Onsite Service Initial, 36 Month(s)
1 865-BBMZ ProSupport and Next Business Day Onsite Service Extension, 24 Month(s)

Tabulka 4: Konfigurace Serveru PowerEdge R640

4.14.3 Datové úložiště

Datové úložiště nabízíme server firmy DELL SCv3020 3Ux30 Drive Storage Array s dostačující kapacitou a v konfiguraci plně splňující ZD:

DELL SCv3020 3Ux30 Drive Storage Array
1 350-BBKJ SC Bezel
8 400-AEPR Hard Drive Filler 2.5in, single blank
15 400-AVKT SC, 1.8TB, SAS, 12Gb, 10K, 2.5", HDD
7 400-ASVG SC, 960GB, SAS, 12Gb 2.5" RI SSD
2 403-BBPD No Mezzanine Card
2 406-BBLZ IO, 10Gb iSCSI, 4 port, PCI-E, SFP+ w/o Optics, Full Height
2 407-BBPL IO,10Gb iSCSI,4x SFP+ Optical Adapter
1 450-AFMD Redundant Power Supply, 1485W, C14
2 450-AADY C13 to C14, PDU Style, 10 AMP, 6.5 Feet (2m), Power Cord
1 449-BBLE SCv30X0 Dual Controller Components
1 770-BBUJ Rack rail, 2Us, Static
1 634-BJUI Storage Center Core Software Bundle, Base License
1 634-BKCL SSN License
1 634-BKCF Data Progression, Software License
1 709-15120 3Yr Parts Only Warranty
1 723-40384 Channel 63M ProSupport and 4hr Mission Critical

1 821-18300 63M ProSupport for Software for Channel, Data Progression License (Non-Essential)

Tabulka 5: Konfigurace datového úložiště Cv3020 3Ux30 Drive Storage Array

Součástí dodávky datového úložiště je implementace a napojení do stávající infrastruktury iSCSI.

4.14.4 Systémový SW

Pro potřeby dodávaného řešení nabízíme následující systémový SW:

- Jako součást HW virtualizačního serveru (viz požadavek na dodávku jednoho virtualizačního serveru výše) licenci Windows Datacenter pro provoz jak nových, tak stávajících Windows Serverů na dodávaném HW. Pro Log server bude využito jako OS free LINUX.
- Virtualizační platforma pro virtualizační servery bude dodána licence 3x VMware vSphere 6 Standard for 1 processor. Licence odpovídá nabízenému počtu serverů a CPU virtualizačních serverů. Virtualizace je kompatibilní se stávající virtualizací a umožňuje zařadit servery do jedné konfigurační konzole.
- Pro zařazení virtualizačních serverů do systému zálohování bude dodána licence kompatibilního systému zálohování pro dodávané konfigurace virtualizačních serverů (případně doplněná o externí úložiště). Jedná se o 3x Veeam Backup & Replication pro VMware 1 CPU.
- Databáze pro dodávané servery jsou buď již součástí licencí stávajících systémů, u kterých dochází k rozšíření jejich funkčnosti nebo případně ve free nebo integrovanou verzi.

Nabízené řešení je plně kompatibilní se stávajícími technologiemi.

4.14.5 Služby

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

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

4.15 NÁSTROJE PRO BEZPEČNOSTNÍ AUDIT A PENETRAČNÍ TESTY

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

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

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

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

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

- Host Discovey,
- Basic Network Scan,
- Credentialed Patch Audit,
- Web Application Tests,

- Policy Compliance Auditing.

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

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

4.16 BEZPEČNOSTNÍ AUDIT A PENETRAČNÍ TESTY

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

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

4.16.1 Bezpečnostní audit / bezpečnostní analýza

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

Průběh analýzy:

1. Zahajuje se zaslání dokumentace ze strany Zadavate.

   Tzn. veškeré:

   - bezpečnostní a provozní politiky
   - definice aktiv
   - analýza rizik
   - zápisi z řídícího výboru KB
   - plány kontinuity
   - organizační struktura
   - topologie sítě
   - cmdb
   - atd.
2. Po nastudování dokumentace následuje úvodní workshop.

   Zde je předmětem:

   - Seznámení se s obecným fungováním organizace
   - Seznámení se s cíly a podstatou činnosti organizace.
   - Předání informací ohledně členění IT, topologií a zodpovědností.
   - Vydefinování majitelů a provozovatelů jednotlivých aktiv
   - Vydefinování specializovaných workshopů podle technologií, aplikací, lokalit apod.

- Zadavatel přiřadí zodpovědné osoby za jednotlivá aktiva z pohledu majitelů a provozovatelů

3. Po úvodním workshopu následují dílčí technické workshopy podle specializací.
   a) Pohovory s majiteli aktiv (většinou non-IT osoby). Upozorňujeme, že budeme potřebovat hovořit i s řadou osob, které se ZKB na první pohled nesouvisí. Tj. HR, finanční oddělení, top management … Seznam detailně určujeme podle dodané organizační struktury.
   b) Pohovory s provozovateli aktiv (obvykle s IT oddělením). Do této části patří i externí dodavatelé.
4. Na základě získaných informací dojde k sepsání auditní zprávu a hodnotící zprávy dle požadavků v zadávací dokumentaci.

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

<u>Součinnost:</u>

1. Zajištění součinnosti majitelů a provozovatelů aktiv a to včetně externích subjektů.
2. Aktivní účast na workshopech majitelů a provozovatelů aktiv a to včetně externích subjektů dle dohodnutého harmonogramu.
3. Poskytnutí vstupů pro technické hodnocení.
4. Dodání dokumentace
   a. kompletní ISMS dokumentaci
   b. kompletní dokumentaci k ZKB
   c. technickou a provozní dokumentaci k síťovým prvkům, serverům, aplikacím apod.
5. Zajištění všech požadovaných vstupních informací v úvodních týdnech od zahájení GAP analýzy. Pokud se to nepodaří, tak to znamená časový posun v termínu dokončení díla.

<u>Auditní zpráva</u>

- U každého opatření se vyhotoví popis aktuálního stavu.
- Bude provedeno hodnocení z pohledu požadavků aktuální prováděcí vyhlášky KB
- V případě, že to bude potřebné, tak dojde k hodnocení i z pohledu dobré praxe.
- Každé opatření bude popsáno minimálně v požadovaném rozsahu ½ A4
- Celková délka auditní zprávy je orientačně přes 50 stran A4. Finální rozsah je dán množstvím zkoumaných primárních a podpůrných aktiv, případně složitostí prostředí.

- Obsahem zprávy jsou veškeré paragrafy obsažené v prováděcí vyhlášce ZKB
- Organizace se zkoumá z pohledu:
    - organizačních opatření
    - technických opatření
    - fyzické bezpečnosti

Hodnocení stavu

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

Obecný návrh nápravných opatření

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

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

Součástí není:

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

4.16.2 Penetrační testování a testy zranitelností

Testy zranitelností

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 a SOSView. Cílem testů bude odhalení nedostatků, oproti požadavkům §25 vyhlášky 82/2018 Sb. Požadavky §25 budou vnímány v kontextu bezpečnostní strategie či dalších dokumentů Zadavatele.

Vlastnímu penetračnímu testu bude předcházet detekce zranitelností pomocí speciálního nástroje.

Metodické rámce

Penetrační testy budou provedeny:

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

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

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

Auditní zpráva

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

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

4.17 Bezpečnostní požadavky

Nabízené řešení bude splňovat uvedené bezpečnostní požadavky ZD.

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

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

Poptávané a nabízené systémy tak neobsahují osobní údaje o pacientech.

Nabízené systémy splňují požadavky:

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

4.18 Implementační a provozní požadavky

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

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

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

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

5. POŽADAVKY ZADAVATELE - POPIS POŽADOVANÝCH A NABÍZENÝCH FUNKČNÍCH VLASTNOSTÍ

V následujících kapitolách jsou uvedeny požadavky Zadavatele na rozsah dodávky a dále jeho funkční, bezpečnostní a implementační požadavky.

Účastník prohlašuje, že jím nabízené technické řešení veškeré požadavky Zadavatele, uvedené v této kapitole 5, splňuje.

Konkrétní popis nabízeného řešení k jednotlivým oblastem dodávky je uveden v kapitole 4 Podrobný popis nabízeného plnění.

5.1 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 PAK – jedná se o primární IS sloužící pro hlavní činnost ZZS PAK, tj. poskytování PNP na území Pardubického kraje.
    b. Elektronická pošta – jedná se o hlavní informační systém (IS) ZZS PAK zajišťující komunikaci mezi zaměstnanci ZZS PAK a podporu výkonu jejich činností.
2. Budou zajištěny všechny současné integrace uvedených IS a vazby na jiné IS a technologie nezbytné pro provoz ZZS PAK.
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.

5.2 POŽADAVKY NA DODÁVKY

V této kapitole jsou uvedeny požadavky na dodávky.

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

Tabulka 6: Obecné požadavky

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

5.2.2 FireWall(y) s IPS pro ZOS

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

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

#	Požadavek
P.12	Dodávka redundantního FireWallu pro primární ZOS: 1. Může se jednat jak o rozšíření stávajícího řešení (viz kapitola 7.4 – Stav ostatních informačních a komunikačních technologií, příloha č. 1 ZD (Technická specifikace)) nebo o jeho nahrazení. 2. FireWall bude oddělovat externí sítě připojené v rámci primární ZOS (internet apod.) 3. Stavový aplikační firewall jako samostatné HW zařízení, který musí nabízet a. Dynamický a statický NAT/PAT (překlad IP adres). b. Podporu dynamických směrovacích protokolů RIP, OSPF, BGP a Policy based Routing. c. Plnou podporou protokolu IPv6. d. Realizace redundance pro případ výpadku ve formě Active/Active failover, Active/Standby failover (redundance se stávajícím prvkem nebo jeho nahrazení a zajištění redundance nově dodanými prvky). e. Podpora zvyšování výkonu pomocí clusterování firewallů – sloučení firewallů do jednoho logického clusteru. f. Podpora filtrace Ipv4, Ipv6 a filtrace podle identity uživatele nebo jeho skupiny definované v AD. 4. Aplikační firewall a. Pokročilá hloubková analýza dat na aplikačních vrstvách ISO modelu b. Podpora pasivního monitorování (TAP režim) c. Rozeznávání a kategorizace aplikací, geografických lokalit, uživatelů d. Možnost rozšíření o identifikace a zamezení přístupu na nedůvěryhodné či škodlivé webové stránky – filtrace podle reputace serverů e. Security Inteligence database – známé adresy anonymních proxy, otevřených mail relay, uzly botnet sítí f. Možnost integrovat vlastní reputační databáze 5. IPS senzor, který musí nabízet a. Možnost definovat typ provozu předávaný k inspekci do IPS b. Možnost obejití IPS funkcí při zahlcení nebo nedostupnosti c. IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií d. Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací e. IPS musí umět detekovat a blokovat útoky průzkumných aktivit f. IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS g. IPS musí umět detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host“ jako je spyware, phishing nebo Botnet C&C h. aktuálních databázích AV dodavatelů i. Ochrana před malware typu „zero day attack“ které nelze detekovat tradičními antiviry j. Retrospektivní ochrana prostředí – pokud SW kód je později detekován jako malware, je na to IPS schopna reagovat

#	Požadavek
	k. Podpora databází reputací adres v internetu (Security Intelligence) 6. VPN koncentrátor a. Zakončení „full-tunnel“ IPSec nebo SSL VPN pro alespoň 300 současné připojených uživatelů – licence pro 25 uživatelů b. Možnost rozšíření (licence apod.) „odlehčené“ SSL VPN pro uživatele formou zabezpečeného přístupu na webový portál bez nutnosti tlustého klienta c. Zakončení alespoň 300 současně připojených site-to-site Ipsec tunelů d. Implementace Ipsec musí podporovat protokoly IKEv1 i IKEv2 a šifrovací standardy 3DES/AES a algoritmy nové generace popsané ve standardu NSA Suite-B 7. Výkonnostní parametry a provedení a. Minimální propustnost NGFW (hloubková inspekce) 850 Mbps b. Minimální propustnost NGFW (hloubková inspekce + IPS modulem) minimálně 450 Mbps. c. Minimální propustnost pro Ipsec VPN komunikaci (šifrování 3DES/AES) 250 Mbps d. Formát zařízení Appliance v provedení do racku max 2RU e. Samostatný port pro management f. Minimální 8 portů pro data 10/100/1000 BaseT Ethernet g. Podporovaný počet VLAN min. 100 Součástí dodávky je implementace (montáž, instalace, konfigurace, zaškolení a seznámení s funkcionalitami a obsluhou, dokumentace) Podpora na 5 let typu NBD pro celé dodané řešení této části, oprava v místě instalace zařízení včetně aktualizací všech signatur a SW komponent včetně jejich funkčnosti.
P.13	Umístění firewallu s IPS do DC v rámci primárního zdravotnického operačního střediska.
P.14	FireWall musí být v redundantním provedení (HW a SW).
P.15	Nastavení pravidel pro kontrolu přístupu do segmentů IS ZOS a ZZOS z externích sítí před případnými externími i interními útoky. Konfigurace FireWallu bude realizována na základě požadavků ZZS s přihlédnutím ke konfiguraci stávajících oprávnění v rámci centrálního FireWallu v ZOS. Nastavení bude umožňovat bezproblémový chod IS OŘ ze ZOS (stávajících technologií) včetně využití připojení k externím sítím v ZOS (internet apod.). Pro konfiguraci přístupu vzdálených uživatelů v rámci VPN bude využito stejné konfigurace jako v době implementace FW (centrální RADIUS serverů), tak aby byla umožněna jednotná konfigurace těchto přístupů bez ohledu na lokalitu přístupu. *Konfigurace stávajících firewallů a nastavení sítě budou poskytnuty v rámci implementační analýzy.*
P.16	Výchozí nastavení pravidel pro alertování upozorňující na bezpečnostní události detekované na tomto bezpečnostním prvku. *Bezpečnostní alerty v rámci IS ZOS budou definovány a konfigurovány na základě požadavků ZZS v rámci implementační analýzy.*

#	Požadavek
P.17	Napojení a předávání alertů a logů do systému analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí (viz kap. 4.4.5, příloha č. 1 ZD (Technická specifikace)). Včetně specifikace korelace kritických bezpečnostních alertů z tohoto bezpečnostního prvku týkajících se IS ZOS.
P.18	Dodávka FireWallu jako kompaktního zařízení, tj. HW včetně vnitřního SW zajišťujícího všechny požadované funkcionality. Pro případný podpůrný SW sloužící pro instalaci, konfiguraci a aktualizace FW ZZS umožní využití stávající virtualizační infrastruktury ZZS za předpokladu, že nepřesáhne požadavek na jeden server (4 vCPU, 8 GB RAM a 500 MB vHD, OS MS Windows Server 2016 Standard nebo Linux). V případě vyšších požadavků na server dodavatel dodá i nezbytný HW a systémový SW včetně licencí pro běh podpůrného SW (HW ve verzi rack mount).
P.19	Možnost aktivace/deaktivace izolace systému IS ZOS od externích sítí nebo i od interních LAN/WAN segmentů ze systému IS OŘ (viz kap. 4.4.8 – Úpravy IS ZOS příloha č. 1 ZD (Technická specifikace)). Vlastní izolace bude provedena na firewallech v rámci ZOS (součástí dodávky) a ZZOS (součinnost poskytne ZZS).
P.20	Bude proveden detailní záznam událostí izolace systému IS ZOS včetně jejich časové souslednosti, případně o uživatelích, kteří opatření realizovali, a to jak do logu IS OŘ, tak do systému analýzy bezpečnostních logů (viz kap. 4.4.5 příloha č. 1 ZD (Technická specifikace)).

Tabulka 7: FireWall(y) s IPS pro ZOS

5.2.3 Aplikační firewall pro IS ZOS

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

#	Požadavek
P.21	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 Jedná se o služby IS ZOS dostupné z externích sítí.
P.22	Funkcionalita webového aplikačního firewallu (WAF) bude poskytovat ochranu webových aplikací před kybernetickými útoky s využitím pozitivní i negativní bezpečnostní logiky v bezpečnostních politikách (detekci a ochranu před známými útoky a povolení explicitního legitimního provozu s minimální propustností 200Mbps. K těmto základním bezpečnostním politikám požadujeme implementaci dalších dodatečných bezpečnostních vlastností, jako je ochrana před útoky prolomením logovacích URL hrubou silou (Brute Force útoky) s možností eskalace a potlačení technologií CAPTCHA v případě podezření, že je aplikace pod útokem.
P.23	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.

#	Požadavek
P.24	Aplikační firewall musí plnit následující min. parametry: 1. Ochrana proti aplikačním DoS a DDoS útokům (SlowLoris, R.U.D.Y, ApacheKiller, SSL útoky, SYN flood, HTTP flood aj.) 2. Ochrana proti "forcefull browsing", XSS, SQL-INJ, CSRF, remote command execution a ostatním útokům podle OWASP Top 10 3. Ochrana proti manipulaci s cookies 4. Ochrana parametrů webové aplikace 5. Session Management – ochrana proti únosům relací 6. Brute Force Ochrana – ochrana před prolomení hrubou silou 7. Detekce a potlačení robotických uživatelů aplikace 8. Ochrana AJAX a JSON aplikací, zabezpečení XML komunikace 9. Možnost rozšíření o detekci a ochranu před robotickými klienty pro nativní mobilní aplikace IOS a Android 10. Blokování požadavků z podezřelých prohlížečů (proaktivní ochrana proti botnetům) 11. Automatická instalace a aktualizace databáze pro detekci útoků, botnetů nebo kampaní kybernetických útoků 12. Blokování útočníků na základě geolokace 13. Podpora různých typů reportů – PCI, geolokační reporty, OWASP Top 10 14. Identifikace zařízení a potlačení škodlivých zařízení v bezpečnostní politice (fingerprinting) 15. Podpora rozkládání zátěže na více než 3 servery a podpora různých typů mechanismů rozkladu zátěže, minimálně kruhová metoda (round-robin), vážená kruhová metoda s (weighted round-robin) podle počtu spojení 16. Podpora zajištění konektivity uživatelů k serveru (persistence) na základě IP adresy, HTTP cookie 17. Podpora REST API pro správu a monitoring zařízení 18. Možnost doprogramovat filtrovací pravidla pro aplikace 19. Ochrana proti L7 DDoS útokům, web scrapingu a útokům pomocí hrubé síly (brute force), mitigace DDoS útoků založená na behaviorální analýze 20. Podpora SSL (šifrování a dešifrování) 21. Povoleni jednotlivých HTTP metod pro jednotlivá URL 22. Detekce anomálií a podezřelých operacích na aplikační vrstvě 23. implementace (instalace, konfigurace, seznámení s funkcionalitami a obsluhou, dokumentace) 24. záruka a aktualizace SW apod. na 5 let.
P.25	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.26	Pro chod aplikačního FW je možné využít jak HW, který bude součástí dodávky řešení (viz kap. 4.4.8 přílohy č. 1 ZD (Technická specifikace)) nebo i stávající virtualizační infrastruktury ZZS za předpokladu, že nepřesáhne požadavek na jeden server (4v CPU, 8 GB RAM a 100 GB HD, OS MS Windows Server 2016 Standard nebo Linux). V případě vyšších požadavků na server dodavatel dodá i nezbytný HW a systémový SW včetně licencí pro běh FW (HW ve verzi rack mount).

#	Požadavek
P.27	Umístění aplikačního firewallu do DC v rámci primárního zdravotnického operačního střediska. S možností migrace do ZZOS v případě plné aktivace ZZOS (s možností využití stávající virtualizační platformy ZZOS).
P.28	Napojení a předávání alertů a logů do systému analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí (viz kap. 4.4.5 přílohy č. 1 ZD (Technická specifikace)). WAF musí podporovat logování ve formátu minimálně Syslog, a případně s navrženým logovacím systémem (viz kap. 4.4.5 přílohy č. 1 ZD (Technická specifikace)). 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 8: Aplikační firewall pro IS ZOS

5.2.4 Systémy pro sběr dat (logů) o síťovém provozu

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

#	Požadavek
P.29	Je požadováno ucelené škálovatelné řešení umožňující dlouhodobé i real – time monitorování sítě na bázi technologie NetFlow složené z: 1. Sondy síťového provozu (virtuální i fyzické) 2. Kolektoru síťového provozu 3. Modul automatického vyhodnocování IP toků
P.30	Minimální požadovaná funkční specifikace sondy 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 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.31	Minimální požadovaná funkční specifikace fyzické sondy:

#	Požadavek
	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
P.32	Minimální požadovaná funkční specifikace kolektoru síťového provozu: Specializované zařízení (kolektor) určené pro uložení, vizualizaci a vyhodnocení síťových statistik exportovaných NetFlow/IPFIX dat. 1. Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite. 2. 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. 3. Rack mount zařízení, snadná instalace do stávající síťové infrastruktury. 4. Datové úložiště minimálně o velikosti 1TB, použití RAID5. 5. Dva plnohodnotné management (administrativní) porty 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat. 6. Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS. 7. Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. Separace dat s omezením přístupu pro jednotlivé role/uživatele. 8. Podpora autentizace vůči LDAP (Active Directory). 9. Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména. 10. Podpora pro Cisco NEL, Cisco NSEL, Cisco NBAR2, IPFIX položek proměnlivé délky. 11. Schopnost sbírat a ukládat dlouhodobě data z tisíců zdrojů flow dat. 12. 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. 13. Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard s podporou více záložek (konfigurace per uživatel). 14. 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. 15. Generování statistik a podrobných výpisů nad volitelnými časovými intervaly s volitelnými filtry. Různé formáty výstupů, minimálně PDF, CSV. 16. 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. 17. Časová synchronizace zařízení proti centrálnímu zdroji času na síti. 18. Možnost přístupu a konfigurace zařízení prostřednictvím sériové linky (RS-232). 19. Podpora autentizace vůči LDAP (Active Directory). 20. Řízení uživatelského přístupu.
P.33	Minimální požadovaná funkční specifikace automatického vyhodnocování IP toků:

#	Požadavek
	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.). 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.34	Instalace a konfigurace dodávaných komponent a celkového řešení.
P.35	Záruka 5 let, režim 5x8, garantovaná doba opravy do následujícího pracovního dne na místě včetně aktualizace SW.

Tabulka 9: Systémy pro sběr dat (logů) o síťovém provozu

5.2.5 Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí

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

#	Požadavek
P.36	Dodávka SW nástroje pro sběr dat (logů, alertů a dalších vstupů) a vyhodnocení kybernetických bezpečnostních událostí ze zabezpečovaných informačních systémů, infrastruktury, HW, systémového SW a technologií včetně IS ZOS a systému elektronické pošty. Systém bude sdružovat záznamy o událostech z jednotlivých aplikačních modulů IS ZOS, elektronické pošty a z okolí uvedených systémů (to je ze všech důležitých zařízení, systémů, sítě LAN/WAN a navazujících aplikací). Tyto záznamy bude ukládat a bude tyto záznamy dávat do souvislostí – korelovat a zajistí tak okamžitou detekci nebezpečného, případně nestandardního chování právě v IS ZOS, systému elektronické pošty nebo jejich infrastruktury.
P.37	Pro sběr dat z OS a DB serverů IS ZOS a elektronické pošty požadujeme minimálně následující události: 1. Přihlášení 2. Odhlášení 3. Neúspěšné pokusy o přihlášení Ukládání sesbíraných dat do úložiště nástroje pro následnou analýzu.
P.38	Zpracování (korelace) záznamů s cílem detekce nebezpečného, případně nestandardního chování v zabezpečovaných IS infrastruktury, infrastruktury, HW, systémového SW a technologií.
P.39	Zpracování bezpečnostních logů z IS ZOS a jeho komunikačních modulů/aplikací a elektronické pošty tak, aby bylo možné jej využít k identifikaci a korelaci bezpečnostních incidentů, a to nejenom na úrovni přístupů, včetně možnosti zablokování, ale i chování uživatele v rámci aplikace,
P.40	Minimální požadavky na systém analýzy bezpečnostních logů: 1. podporované protokoly: Syslog, Windows Events Collection (WinRM/RPC), FTP, S/TP/SCP, SNMP, ODBC/JDBC, CP-LEA, SDEE, 2. bezagentový sběr logů (sběr bez nutnosti instalovat agenta na cílový systém), 3. licence pro zpracování 200 EPS (událostí za sekundu) s možností rozšíření až na 5000 EPS, 4. možnost řešení jak prostřednictvím VirtualAppliance nebo samostatným HW, 5. počet zdrojů pro sběr logů minimálně 150, 6. možnost sběru logů samostatným lokálním kolektorem s přeposíláním do centrálního systému, 7. možnost záložního uložení logů (rozšiřitelné úložiště neodpovídá tomuto požadavku), 8. centrální management všech komponent a administrativních funkcí ve webovém uživatelském rozhraní, 9. možnost definovat uživatelům systému přístup k jednotlivým zařízením, jejich skupinám či síťovým segmentům, 10. automatická identifikace systémů – zdrojů logů, 11. podpora šifrované komunikace mezi zdroji logů a systémem analýzy bezpečnostních logů,

#	Požadavek
	12. integrace s adresářovým systémem (LDAP, Active Directory) pro potřeby autentifikace uživatelů, 13. minimální administrace /výběr zařízení ze seznamu od výrobce/pro připojení dalších zdrojů událostí (servery Windows, Unix/Linux, přepínače, routry, FW apod.), 14. Log Management s minimální postimplementační administrací. /agregace událostí dle typů, analýza, vyhodnocování/ pro případy, jako je zavedení nového zdroje událostí, nastavení pravidel pro sběr dat a archiv událostí, 15. definice základních korelačních pravidel v návaznosti na IS ZOS s důrazem na jeho bezpečnost a případné pokusy o zneužití, a to vše s korelací získávaných informací z okolí systému (provoz, aktivní prvky, OS atd.), 16. podpora sběru síťových toků (NetFlow, JFLow, Sflow) z navržených infrastrukturních prvků (switche, routery, NetFlow sondy), 17. řešení musí umožňovat automatické aktualizace, 18. webové uživatelské rozhraní pro management, analýzu a reporting, 19. poskytování automatického backup/recovery procesu, 20. poskytovat interní kontroly stavu zařízení (healthcheck) a upozornění uživatele v případě problému, 21. možnost integrovaného managementu rizik na základě síťových toků a konfigurace aktivních prvků do GUI, 22. poskytování analytických a korelačních funkcí bez dalších zásahů a činností (out-of-the-box), 23. řešení musí být dodáno jako all-in-one appliance (vAppliance), 24. sběr logů z dalších bezpečnostních a síťových systémů (např. FlowMon, AFW f5, FW Cisco, AV Symantec, IronPort Cisco) a prvků navržených v rámci tohoto projektu, 25. výkonová rozšiřitelnost – přidání nových zařízení, lokací, aplikací, 26. možnost rozšíření výběrů o uživatelské položky z obsahu logů, 27. zajištění integrity nasbíraných dat, 28. umožnění nárůstu zdrojů událostí bez nutnosti pořizování dalšího hardware (v případě fyzického HW), 29. Near-real-time analýza událostí, 30. analýza dlouhodobých trendů událostí, 31. řešení musí být hodnocené v segmentu „leaders“ v GartnerMagicQuadrantu za minulé dva roky, 32. pokročilé "drill-down" dohledávání v případě potřeby, 33. možnost agregace události z logů i podle položek které nejsou standardně zahrnuty v řešení, 34. podpora a normalizace časových značek z různých časových zón, 35. sběr textových logů ze souborů, 36. sběr logů z databází pomocí JDBC/ODBC, 37. sběr log záznamů z prostředí Windows a Linux/Unix/AIX. Sběr Windows EVT záznamů i z Windows Server, a navržených OS v rámci SOBD, 38. rozčlenění vyhledaných dat (Drilldown): Vyhledávací rozhraní systému správy logů musí nabízet možnost rozčlenění vyhledaných dat až na detailní úroveň, IP adresa, typ události, protokol, port atd.,

#	Požadavek
	39. způsob zadávání vyhledávání: vyhledávací rozhraní systému správy logů musí poskytovat podporu jak pro zadání dotazu s použitím Booleovy logiky, tak pro regulární výrazy, 40. poskytování alertů na detekované anomálie, změny chování sítě a změny v generování logů a událostí, a to i v návaznosti na aplikaci operačního řízení, 41. kombinované hledání v indexovaných i neindexovaných datech v systému správy logů s použitím regulárních výrazů a fulltextového vyhledávání v nestrukturovaném textu současně, 42. korelační modul musí poskytovat již po instalaci (out-of-the-box) metody korelačních pravidel, která automatizují zjišťování incidentů a související workflow procesy, 43. korelace mezi zařízeními již po instalaci (out-of-the-box). Zjišťování chyb autentizace, chování perimetru a výskytu infiltrací (červů apod.) bez potřeby specifikovat typy sledovaných zařízení, 44. řešení musí poskytnout alerting vycházející z detekovaných bezpečnostních hrozeb od monitorovaných zařízení a aplikace operačního řízení, 45. alerting založený na vypozorovaných anomáliích a změnách chování sítě (analýza síťových toků). Řešení musí poskytovat NBAD (Network Behavior Anomaly Detection) funkcionalitu, 46. řešení musí poskytnout alerting porušení bezpečnostních pravidel, založený na stanovené bezpečnostní politice (např. IM provoz je zakázán), 47. vykonávání akcí v závislosti na přijatém logu jako např. zaslat email, 48. schopnost pracovat s IP geolokacemi (botnet kanály atp.), 49. generování alertu při výpadku logů z konkrétního zařízení, 50. vestavěný mechanismus na klasifikaci systémů podle typu (např. mail server vs. databázový server), 51. vyhodnocení chybějících sekvencí (např. služba přestala běžet), 52. schopnost monitorovat historii útoků (typů událostí) na kritické komponenty a historii útoků jednotlivých uživatelů, 53. schopnost korelovat události DHCP, VPN a Active Directory a sledovat průběh uživatelské relace (session) v rámci celé instituce (přesná identifikace uživatele), 54. schopnost korelovat data o událostech se statickými a dynamickými seznamy označujícími položky, které mají či nemají být v síti povoleny (tj. seznam nezabezpečených protokolů), 55. poskytování rozhraní pro reporting, pomocí kterého lze vytvářet nové sestavy bez nutnosti sestavovat SQL dotazy, 56. nezměněná funkcionalita reportingu i při změně nebo náhradě některé technologie jako např. firewallu nebo IDS, 57. přístup k datům skrze otevřené REST API pro integraci s dalšími systémy, 58. postupné doplňování funkcionalit pro log management a security intelligence (rozšíření o další analytické moduly by mělo mít minimální dopad přidávání komponent třetích stran a mělo by být primárně umožněno jen licenčním klíčem), 59. řešení musí být schopno pracovat s interními překrývajícími se rozsahy adres, 60. řešení si musí pasivně budovat tabulku zařízení v síti z informací obsažených v již příchozích zdrojích (flows), 61. schopnost agregovat záznamy o síťovém provozu z obou stran datového toku do jedno záznamu,

#	Požadavek
	62. provádění deduplikace záznamů o síťovém provozu v případě identických záznamů z různých zařízení, 63. podpora korelace dat proti výsledkům scanům zranitelností třetích stran, 64. uchovávání logů i flows jak v normalizovaném formátu, tak i „raw“ formátu, 65. řešení nebude licenčně omezeno počtem používaných korelačních pravidel a nebude licenčně omezeno počtem generovaných reportů, 66. možnost nasazení High Availability režimu v jakékoliv fázi životního cyklu řešení bez nutnosti reinstalace řešení.
P.41	Záruka 5 let, 5x8, garantovaná doba opravy do následujícího pracovního dne na místě včetně update SW a všech modulů.
P.42	Součástí dodávky musí být instalace a konfigurace řešení, včetně součinnosti při konfiguraci jednotlivých zařízení a aplikací a nastavení notifikací, a to včetně seznámení s funkcionalitami a obsluhou.
P.43	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.44	Implementace notifikací s využitím jak stávajících notifikačních nástrojů ZZS, tak s využitím pokročilého notifikačního nástroje, který je součástí dodávky tohoto projektu (viz kap. 4.4.7 přílohy č. 1 ZD (Technická specifikace)). Notifikace budou prováděny následujícími nástroji: 1. Email 2. SMS 3. Hlasová zpráva (text-to-Speech) 4. Push aplikace na mobilní zařízení 5. Využití záložního svolávacího systému (jiná ZZS) *Pro notifikaci emailem bude využíván protokol SMTP.*
P.45	Pro analytickou práci s logy aplikací, bezpečnostních a síťových systémů využívaných v rámci ZZS nebo dodávaných v rámci dodávky je požadována dodávka nástroje pro logování z IT infrastruktury: 1. Aktivní prvky (sítě) 2. Informační systémy – IS ZOS/ZZOS a systém elektronické pošty 3. Databáze (ORACLE, MS SQL) 4. Operační systémy (MS Windows, Linux) – servery, pracoviště ZOS/ZZOS V případě, že se bude jednat o jeden nástroj zajišťující všechny uvedené služby, musí nástroj umožnit samostatný přístup k různým službám pro různé osoby na základě oprávnění definovaného správcem a možnost instalace na oddělený samostatný server (log server v kap. 4.4.15 – Infrastruktura (HW) a systémový SW pro běh dodávaného SW).
P.46	Dodávka a implementace nástroje na logování z IT infrastruktury, IS ZOS a elektronické pošty, tzn. aktivní prvky, aplikace, operační systémy apod. ve kterém bude možnost plošně prohledávat sesbíraná data a mít k dispozici statistiku a analytické funkce – přičemž zdrojem dat může být stávající syslog systém ZZOS a bude rozšířen o následující funkce: 1. Schopnosti provádět korelace přes více datových zdrojů a hledání specifických vzorů

#	Požadavek
	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. Není třeba vytvářet datové schéma nebo připravit vyhledávací dotazy ještě před indexováním 6. Možnost využití nestrukturovaných souborů a datového skladu bez pevného schématu (bez relační databáze s pevným schématem) 7. Schopnost indexovat a připravit pro vyhledávání všechna originální data bez jakékoliv modifikace (bez normalizace/redukce dat) 8. Automatická komprese indexovaných dat pro redukci nároků na úložný prostor 9. Flexibilní nastavení uchování dat s možností odstupňování řízení toho, co se stane s postupně stárnoucími daty. Neaktuální data mohou být přesunuta na externí (levnější) datové úložiště k archivaci a (nebo) smazána. 10. Flexibilní kontrola přístupu na základě rolí pro řízení přístupu uživatelů a přístupů přes API. 11. Integrace autentizace a autorizace s Microsoft Active Directory, případně samostatný oddělený systém pro auditní účely (mimo stávající systém AD). 12. Generování hashe pro každou událost v době indexování tak aby umožnilo při vyhledávání zjistit, zda s daty nebylo manipulováno 13. Monitoring své vlastní konfigurace a využití s cílem udržet si kompletní, digitálně podepsané auditní záznamy o tom, kdo přistupuje k systému, jaké dotazy spouští, na jaké reporty se dívá, jaké konfigurační změny provádí a další. 14. Řešení by mělo umožnit snadné vytváření široké palety vizualizací (nejen pevně dané, předpřipravené reporty) 15. Dostupné vizualizace by měly zahrnovat: čárový graf, časový graf, plošný graf, sloupcový graf vertikální, sloupcový graf horizontální, jediná hodnota s trendem (růst, pokles), koláčový graf, bodový graf, bublinový graf, ciferníkový (budíkový) ukazatel, graf typu teploměr (zobrazení hodnoty ve vztahu k rozsahu), geolokační mapa, graf zobrazující rozložení hodnot v geografických regionech, kruhový graf, výplňový graf, tabulky (vč. doplňkových funkcí jako jsou automatické sumy, procentuálních vyjádření, číslování řádků, atd.)
P.47	Implementace nástroje na logování bude obsahovat nejenom zprovoznění a základní nastavení systému ale vytvoření i reportů a dashboardů (náhledů) na jednotlivé komponenty IT infrastruktury a IS ZOS. Minimálně následující náhledy: 1. Aktivní prvky (LAN/WAN/FW) – přihlášení, změny konfigurací, chyby atd. 2. FW/VPN – přístupy (oprávněné a neoprávněné) včetně geolokace (zobrazení na mapě a v tabulce) 3. Operační systémy a databáze IS ZOS – přihlášení, chyby atd. 4. Emailová komunikace – přístupy (oprávněné a neoprávněné) včetně geolokace, chyby systému atd.

#	Požadavek
P.48	Je požadována realizace jednotného bezpečnostního portálu pro správce a management ZZS, který bude zahrnovat dodané technologie v rámci projektu. Minimální požadavky na přehledový bezpečnostní portál: 1. Webové rozhraní 2. Autentizace/autorizace uživatelů proti Microsoft Active Directory 3. Zobrazení posledních incidentů na základě analýzy bezpečnostních logů 4. Zobrazení VPN připojení (úspěšné i neúspěšné) 5. Zobrazení přihlášení do aplikací IS ZOS (úspěšné i neúspěšné) 6. Zobrazení přehledu emailové komunikace ZZS (chyby, vytížení apod.) 7. Možnost dalšího rozvoje dle požadavků ZZS – otevřený systém
P.49	Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí bude provozován na infrastruktuře (HW a systémový SW) požadovaný a dodávaný dle kap. 4.4.15 – Infrastruktura (HW) a systémový SW pro běh dodávaného SW..

Tabulka 10: Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí

5.2.6 Analytické nástroje pro ZOS ZZS PAK

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

#	Požadavek
P.50	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. Vytvoření vzorových analýz 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.
P.51	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.52	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 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.
P.53	Požadované řešení má umožnit analýzy bezpečnostních logů i na základě anomálií v časovém sledu. Například zaměstnancovo (uživatelovo) nezvyklé navýšení počtu prohlížených a/nebo

#	Požadavek
	modifikovaných záznamů v určitém měsíci / týdnu / dni oproti ostatním měsícům / týdnům / dnům může naznačovat bezpečnostní incident.
P.54	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.55	Možnost dohledání detailů všech přístupů k datům na základě znalosti konkrétní události, resp. existujícího bezpečnostního incidentu / nahlášeného úniku dat.
P.56	Analytické nástroje pro ZOS ZZS PAK budou provozovány nově dodávané infrastruktuře (HW a systémový SW) v kap. 4.4.15 – Infrastruktura (HW) a systémový SW pro běh dodávaného SW). Dodavatel musí provozní požadavky dodávané technologie zohlednit v rámci navrhovaného HW a SW.
P.57	Není požadováno navýšení ani změna stávajících licencí. Součástí dodávky je systémová podpora na 5 let.

Tabulka 11: Analytické nástroje pro ZOS ZZS PAK

5.2.7 Pokročilé notifikační nástroje

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

#	Požadavek
P.58	Je požadována dodávka a realizace pokročilého notifikačního nástroje vč. instalace a propojení se systémem operačního řízení (IS OŘ), propojený se stávajícím svolávacím systémem implementovaným v rámci ZZOS ZZS PaK, napojení na stávající telefonní systém, s následujícími požadovanými funkcemi: 1. Aplikační rozhraní pro uvedené funkce pro systém operačního řízení (IS OŘ), a pro monitorovací systém. 2. Instalace ve virtualizovaném prostředí VMWare s možností migrace v rámci virtualizované platformy (nezávislost na HW). 3. U všech hlasových úloh možnost programově nastavit číslo volajícího v rámci aplikačního rozhraní (v součinnosti s konfigurací stávající telefonní ústředny). 4. Hlasové úlohy: a. Prozvánění k výjezdu. b. Přehrání hlasové zprávy pomocí převodu textu na hlasovou zprávu (text-to-speach) s podporou češtiny. c. Přehrání zprávy s očekávanou návratovou hodnotou (v podobě tónové volby) – například Ano/Ne, přičemž dotaz a způsob odpovědí je zadáván konfiguračně v rámci systému operačního řízení (IS OŘ) a předáván aplikačním rozhraním. d. Kapacita hlasového svolávání až 30 hlasových spojení v jednom okamžiku. e. Úprava systému operačního řízení pro napojení na notifikační nástroj (detailní požadavky jsou uvedeny v kap. 4.4.8). Pokročilý notifikační nástroj musí umožnit všechny scénáře uvedené v kap. 4.4.8. 5. SMS úlohy a. Odesílání SMS, a to prostřednictvím internet připojení – stávající „O2 Connector“ (zajistí Zadavatel) a pomocí GSM brány pro 4 SIM. Primárně přes „O2 Connector“, záložní způsob přes GSM bránu.

#	Požadavek
	b. Dodávka GSM brány pro 4 SIM integrované s nabízeným svolávacím systémem. GSM brána připojena k infrastruktuře pomocí IP protokolu (ethernet port). Vlastní SIM karty zajistí Zadavatel. c. Licence notifikačního nástroje pro využití min. 1x SMS connector a 4x SIM. d. Odesílání definovaných, případně uživatelsky modifikovaných zpráv. e. Odesílání zpráv s dotazem na uživatele a přijetím a předáním jeho odpovědi dále do operačního řízení. 6. Mobilní aplikace a. Odeslání zpráv na mobilní zařízení b. Odesílání zpráv s dotazem na uživatele a přijetím a předáním jeho odpovědi dále do operačního řízení. c. Podpora mobilních platforem min. iOS a Android 7. Integrační úlohy a. Vyhodnocení odpovědí svolávaných skupin uživatelů a jejich přehledné zobrazení. b. Plná aplikační integrace s IS OŘ (viz kap. 4.4.8 přílohy č. 1 ZD (Technická specifikace)).
P.59	Integrace notifikačního nástroje musí umožnit využití všech technologií nástroje pro doručení požadované zprávy. Pokročilý notifikační nástroj musí být schopen při výpadku jakékoliv technologie (Internet, telefonie, GSM SMS) doručit požadovanou zprávu ke koncovému uživateli jinou dostupnou technologií.
P.60	Vlastní inicializaci notifikace bude možné provádět jak z IS OŘ, tak z monitorovacích systémů (jako upozornění na aktuální problém).
P.61	Zadavatel zajistí SIM karty a konektor k mobilnímu operátorovi pro odesílání SMS a SIP trunk pro hlasové služby. Pro odesílání zpráv do mobilní aplikace bude využito stávajícího internet připojení.
P.62	Notifikační nástroj pro ZOS ZZS PAK bude provozován na infrastruktuře (HW a systémový SW) požadovaný a dodávaný dle kap. 4.4.15 – Infrastruktura (HW) a systémový SW pro běh dodávaného SW.

Tabulka 12: Pokročilé notifikační nástroje

5.2.8 Úpravy IS ZOS

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

#	Požadavek
Napojení na Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí (viz kap. 4.4.5 přílohy č. 1 ZD (Technická specifikace))	
P.63	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. 4.4.5 přílohy č. 1 ZD (Technická specifikace)).
P.64	**IS OŘ:** Předávání logů z IS OŘ do systému analýzy bezpečnostních logů v následujícím rozsahu: 1. Přihlášení a odhlášení do systémů a modulů

#	Požadavek
	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.65	**IS OŘ:** Napojení na pokročilé notifikační nástroje (viz kap. 4.4.7) – je požadována úprava IS OŘ tak aby, byl schopen využívat jak pokročilý notifikační nástroj (viz kap. 4.4.7 přílohy č. 1 ZD (Technická specifikace)) implementovaný v ZOS, tak stávající svolávací systém provozovaný v rámci ZZOS, dle dostupnosti požadovaných technologií a to minimálně s následujícími požadavky: 1. Možnost zadávat text zprávy pro notifikace a to jak technologií hlasového svolávání (text-to-speach), tak pro SMS a datový kanál (mobilní aplikace). 2. Možnost definování textu otázky a odpovědí pro úlohy svolávání vyžadující odpověď koncového uživatele. Integrace s vyhodnocením odpovědí koncových uživatelů v závislosti na typu svolávání. 3. Předávání zprávy k odeslání notifikačním nástrojům přes integrační rozhraní 4. a rozšíření o volitelné texty a využití funkce text-to-speach v rámci systému operačního řízení (IS OŘ) a to jak běžných informací, tak i modulu hromadného neštěstí. 5. Jednoduchý proces přepínání využívaného rozhraní mezi pokročilým notifikačním nástrojem v ZOS a svolávacím systémem ZZOS.
P.66	**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.67	**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.68	**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.69	**Systém sledování vozidel (AVL):** Předávání logů z AVL do systému analýzy bezpečnostních logů v následujícím rozsahu: 1. Přihlášení a odhlášení do systému

#	Požadavek
	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.70	**Svolávací systém** využívá data IS OŘ a jeho volání je realizován z IS OŘ, tj. data budou sbírána cestou IS OŘ.
P.71	**Telefonní ústředna** je integrována s IS ZOS prostřednictvím JTAPI a 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.
P.72	**Záznamový systém (REDAT)** je uzavřené řešení pro nahrávání hovorů. Dispečeři ZOS mají přístup k nahrávkám prostřednictvím systému IS OŘ, který loguje přístupy k aplikačnímu serveru systému REDAT v rámci IS OŘ. Tyto informace jsou tak předávány v rámci přeposílání logů IS OŘ. Součástí dodávky je parsování logů záznamového systému přes IS OŘ, jejich analýza a ukládání do Systému analýzy bezpečnostních logů.
P.73	**Integrace telefonie a radiofonie** je vázaná na dané dispečerské pracoviště a informace o přihlášení a přístupu uživatele budou brány z IS OŘ dle toho, který dispečer na daném pracovišti pracoval (vlastní integrace nevyužívá speciální přístupy a ovládá komunikační prostředky na daném pracovišti). Vlastní přístup na server určený pro integraci je logován v rámci systémových prostředků OS. Data jsou tedy sbírána na systémové úrovni. Součástí dodávky parsování logů z IS OŘ je jejich analýza a ukládání do Systému analýzy bezpečnostních logů.
P.74	**Záložní IS ZOS (ZZOS):** ZZOS využívá v současné době repliku některých systémů IS ZOS (IS OŘ, AVL/GIS, MZD/EKP). Je požadováno, aby pro tyto systémy byla sbíraná data stejná v primární i záložní lokalitě.
P.75	Aplikační SW na pracovištích ZOS/ZZOS: Vlastní přístup do OS na pracovištích ZOS a ZZOS bude logován v rámci systémových prostředků operačního systému. *Sbíraná data z operačních systémů a dalších technologie na pracovištích ZOS/ZZOS budou sbírána na systémové úrovni.*
Napojení IS OŘ na FireWall(y) s IPS pro ZOS (viz kap. 4.4.2 přílohy č. 1 ZD (Technická specifikace))	
P.76	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

#	Požadavek
	bude předávat do IS OŘ – dispečerského pracoviště. Tak bude aktivně informován provoz centrálního dispečinku ZOS o vážných bezpečnostních událostech.
P.77	Oprávněné osoby centrálního dispečinku budou mít možnost pomocí rozhraní v IS ZOS (IS OŘ) na základě vzniklých bezpečnostních událostí a jejich průběhu rozhodnout o možnosti aktivace (a následné deaktivace) izolace systému IS ZOS od externích sítí nebo i od interních LAN/WAN segmentů. Vlastní izolace bude realizována na uvedených bezpečnostních prvcích (ZOS/ZZOS). Oprávněný uživatel bude před vlastní aktivací daného typu izolace informován o rozsahu izolace a z toho plynoucích omezení centrálního dispečinku a IS ZOS. O těchto událostech bude proveden detailní záznam událostí včetně jejich časové souslednosti a uživatelích, kteří taková opatření realizovali a neprodleně automaticky informováni definovaní pracovníci ZZS v rámci stávajícího svolávacího systému ZZS.
Autentizace uživatelů operačního řízení prostřednictvím AD	
P.78	V rámci sjednocení ověřování identity uživatelů v rámci IT a operačního řízení je požadováno využití stávající domény v rámci Microsoft Active Directory. Pro tyto účely požadováno rozšíření stávajícího IS ZOS o možnost autentizace a autorizace v rámci struktury MS Active Directory.
P.79	**IS OŘ:** Správce IS OŘ bude pak schopen zvolit způsob autentizace jednotlivých uživatelů dle potřeb ZZS a typu modulů/subsystémů. Je požadováno, aby bylo možné plně využít pro autentizaci a autorizaci uživatelů IS OŘ jednotných účtů v rámci MS Active Directory. Autorizace uživatelů pro jejich oprávnění pak bude spočívat v příslušnosti k dané skupině uživatelů.
P.80	**EKP/MZD:** EKP/MZD musí umožňovat autentizaci a autorizaci uživatelů jak interní (stávající stav) nebo v rámci MS Active Directory. Správce IS v návaznosti na okolní systémy bude schopen zvolit způsob autentizace EKP/MZD dle požadavku ZZS. Autorizace uživatelů pro jejich oprávnění pak bude spočívat v příslušnosti k dané skupině uživatelů.
Integrace s personálním systémem	
P.81	Je požadováno rozšíření stávajícího personálního systému o integraci s centrálním Active Directory ZZS s četností aktualizace dat minimálně 1x za den.
P.82	IS OŘ a EKP/MZD pak musí umožnit využití integrace s personálním systémem, a to jak při zakládaní uživatele a případně jejich základní role v rámci personálního systému (která se promítne do AD) využití zneplatnění účtů uživatelů, u kterých bude ukončen pracovní poměr (zneplatnění/vymazání účtu v AD). Tím bude zajištěna maximální aktuálnost uživatelských účtů zaměstnanců ZZS.
Monitoring a reporting a přístupů	
P.83	Pro správu a reporting oprávnění bude dodán i samostatný portál pro správu uživatelů IS OŘ a přiřazování jejich rolí. Tento portál bude sloužit pro vedoucí pracovníky OŘ, kteří budou tato oprávnění spravovat a kontrolovat a monitorovat.
P.84	Součástí dodávky bude nástroj pro reportingu všech změn provedených jednotlivými uživateli/administrátory v rámci Microsoft Active directory (AD) ZZS (počet zaměstnanců –

#	Požadavek
	potenciálních uživatelů 600), tak aby bylo možné kontrolovat změny oprávnění, které byly v rámci AD provedeny. Je požadováno reportovat minimálně: 1. Vytvoření nového uživatele nebo skupiny 2. Vymazání uživatele nebo skupiny 3. Zneplatnění (disable) uživatele 4. Přidání člena skupiny 5. Vymazání člena skupiny
Infrastruktura (HW) a systémový SW pro úpravy IS ZOS	
P.85	Stávající infrastruktura (HW) a systémový SW pro běh IS ZOS po realizaci úprav zůstane beze změny, tj. nedojde ke změně konfigurace, parametrů, licencí systémového SW využívaných pro běh IS ZOS.

Tabulka 13: Úpravy IS ZOS

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

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

#	Požadavek
P.86	Napojení na Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí a předávání následujících dat ze systému elektronické pošty: 1. Úspěšná a neúspěšná připojení k systému dostupnými protokoly 2. Využívání systému elektronické pošty jednotlivými uživateli 3. Dostupné bezpečnostní logy používaného systému 4. Dostupné chybové a provozní logy používaného systému Předávání veškerých logů systému do nástroje/rozhraní pro logování.
P.87	Toto nastavení realizovat pro všechny komponenty systému elektronické pošty.
P.88	Předávání logů systému online prostřednictvím syslog služby.
P.89	Součinnost při konfiguraci FireWallu ZOS a konfigurace FireWallu ZZOS pro získávání informací o bezpečnostních událostech na prvcích FireWall, týkajících se systému elektronické pošty. Minimálně: 1. Odepření přístupu z dané IP adresy na systém (reputace dynamický ACL apod.) 2. IPS a AntiMalware události 3. Identifikace chyb v protokolu
P.90	Systém dynamických ACL na základě parametrického vyhodnocení bezpečnostních logů systému. Dynamický ACL bude vytvářen prostřednictví analýzy logů na základě neoprávněného přístupu k systému. Pro vytváření dynamických ACL bude možné systémově nastavovat následující parametry: 1. Počet špatných přihlášení k danému protokolu 2. Minimální čas od posledního výskytu špatného přihlášení

#	Požadavek
	Publikace dynamického ACL pro systém elektronické pošty bude pro účely aktualizace pravidel FireWallu realizována web serverem jako standardní textový soubor s výčtem (list) IP adres (jedna IP na jednom řádku).
P.91	Nástroj/rozhraní pro logování bude zpracovávat i uvedený dynamický ACL pro systém elektronické pošty a zobrazovat časový průběh počtu IP adres obsažených v listu a upozorňovat na enormní nárůst.
P.92	Provedení konfigurace FireWallu ZOS (kap. 4.4.2) a součinnost pro konfiguraci FireWallu ZZOS pro implementaci dynamického ACL – aktualizace listu IP adres
P.93	Stávající infrastruktura (HW) a systémový SW pro běh elektronické pošty po realizaci úprav zůstane beze změny, tj. nedojde ke změně konfigurace, parametrů, licencí systémového SW využívaných pro běh elektronické pošty.

Tabulka 14: Konfigurace systému elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů

5.2.10 Dvoufaktorová autentizace administrátorských VPN přístupů

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

#	Požadavek
P.94	Pro autentizaci administrátorských VPN přístupů je požadován systém dvoufaktorové autentizace. Minimální požadavky: 1. Integrace s FireWallem ZOS (součást dodávky), stávajícím FireWallem ZZOS (viz výchozí stav) a autentizačním serverem (viz výchozí stav) 2. Správa pomocí webové konzole nebo Microsoft Management Console (MMC) 3. Bez potřeby dalšího zařízení nebo tokenu 4. Kompatibilní se všemi telefony, které umožňují přijímat SMS 5. Jednorázové heslo nejen přes mobilní aplikaci, push notifikaci, hardwarové tokeny a SMS, ale i vlastní cestou (např. e-mailem). 6. Push autentifikace – možnost autentifikace potvrzením v aplikaci na mobilním telefonu, bez nutnosti přepisovat jednorázové heslo (podpora iOS, Android i Windows Mobile). 7. Podpora Virtual Private Networks (VPN) – Cisco ASA, Remote Desktop Protocol (RDP) a RADIUS.
P.95	Licence pro 10 min. uživatelů.
P.96	Je požadována záruka na funkčnost, podpora a aktualizace po dobu min. 5 let.

Tabulka 15: Dvoufaktorová autentizace administrátorských VPN přístupů

5.2.11 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.97	Pro zabezpečení přístupu do LAN/WAN sítě ZZS požadujeme implementaci technologie 802.1x na přístupových switchích centrální lokality a výjezdových stanovišť. Vlastní implementace

#	Požadavek
	bude využívat pro ověření zařízení a uživatelů autentizaci v rámci RADIUS serverů Microsoft NPS s integrací do jednotného Active Directory. Pro neautorizované 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.98	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.99	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.100	Pro některé lokality bude třeba realizovat i dodávku 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,

#	Požadavek
	12. implementace (montáž, instalace, konfigurace, seznámení s funkcionalitami a obsluhou, dokumentace) 13. veškerý potřebný drobný materiál (kabely apod.) 14. Záruka min. na 5 let.

Tabulka 16: Dodávka a implementace technologií 802.1x pro zabezpečení přístupů do LAN sítě

5.2.12 Zabezpečení systému elektronické pošty před škodlivým kódem

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

#	Požadavek
P.101	Je požadováno plně redundantní řešení pro kontrolu poštovního provozu (EmailSecurity) s veřejnou sítí Internet, včetně antispamové a antivirové ochrany. Řešení může být formou virtuálního appliance do Vmware – rozšíření počtu virtuálních strojů musí být bezplatné (neomezený počet virtuálních strojů v rámci jedné sítě), případně dedikovaným HW (primární a sekundární) nebo kombinací těchto variant. Požaduje se dodávka licencí i pro testovací prostředí na samostatné virtuální appliance. Dodané licence musí umožnit převedení licencí mezi uvedenými variantami (HW/virtual). Licence musí umožnit instalaci další virtuální appliance i v záložní lokalitě. V nabídce bude uveden způsob řešení a způsob redundance.
P.102	Minimální požadavky na EmailSecurity řešení: 1. Řešení musí být výkonově dimenzováno minimálně na 1000 uživatelů a licencováno na 1500 chráněných stanic (využíváno celkem 600 uživateli) 2. nabízené zařízení je možné provozovat v clusteru v režimu loadbalancing, 3. Reputační filtrování na základě zdrojových IP adres odesílatele a reputační způsob blokování spamu na úrovni TCP spojení 4. Možnost nastavení anti-spam akce pro pozitivní nebo podezřelý spam: Doručit, zahodit, karanténa, doručit jako přílohu, přesměrovat 5. Per-user anti-spam karanténa s ověřováním pomocí LDAP 6. Definice whitelist a blacklist pro každého uživatele v karanténě 7. Periodické zasílání notifikací o novém spamu v karanténě pro každého uživatele 8. Možnosti uživatele pro práci se spamem v karanténě: Smazat, doručit, přidat do whitelistu 9. Možnost označit/klasifikovat email jako spam přímo z emailového klienta 10. Detekce a klasifikace marketingových emailů, které nejsou spam 11. Podpora pro současné kontroly více antivirovými engines přímo na zařízení včetně detekce viru uvnitř víceúrovňového archivu 12. Možnost opravy zavirovaných příloh nebo jejich zahození 13. Automatická aktualizace všech antimalware signatur v intervalu 5 minut či méně 14. Per-user nebo per-group nastavení pro Anti-spam a Anti-virus akce pro příjemce či odesílatele 15. Možnost vytváření sofistikovaných filtrů na emailovou komunikaci s možností filtrace na obsah hlaviček, těla i příloh emailu 16. kontrola příchozí i odchozí poštovní komunikace na jednom zařízení zároveň, 17. Filtrování obsahu a ochrana proti úniku dat a. Podpora váhových slovníků

#	Požadavek
	b. Podpora pro mezinárodní a multibyte umístění (nejlépe podpora UTF8) c. "Pattern matching" uvnitř vícevrstvých archivů d. Plná podpora regulárních výrazů pro "pattern matching" e. Plnohodnotný a pravdivý filetype matching (ne na základě MIME type / filename) f. Detekce chráněných archivů g. Možnost omezit maximální velikost přílohy nebo celého emailu h. Filtrování na základě výsledku DKIM/SPF ověření i. LDAP integrace pro filtrování obsahu j. Per-user a per-group nastavení pro podmiňovací a nápravné akce pro příjemce či odesílatele k. Možnost nápravné akce: Karanténa, upozornění, zahodit email, zahodit přílohu, nahradit přílohu, přesměrovat, kopírovat 18. Modifikace obsahu a zabezpečení dat a. Per-user a per-group nastavení pro modifikaci obsahu a dat pro příjemce či odesílatele b. Podmíněné přidání hlavičky do emailu, možnost přidat tzv. "footer" c. Možnost odstranění hyperlinku URL z textu emailu 19. Funkce SMTP – omezení protokolu např. na a. Omezení maximálního počtu současných spojení per odesílatele b. Omezení maximálního počtu zpráv per spojení c. Omezení maximálního počtu příjemců v emailu d. Omezení maximálního počtu příjemců za hodinu 20. Administrace a management a. HTTPS Management console b. Ověřování a autorizace administrátorů pomocí lokálních účtů a pomocí RADIUS c. Napojení do centrálního dohledu pomocí SNMP d. Podpora centrálního logování pomocí SYSLOG
P.103	Řešení email security pro ZOS ZZS PAK bude provozováno na infrastruktuře (HW a systémový SW) požadovaného a dodávaného dle kap. 4.4.15 – Infrastruktura (HW) a systémový SW pro běh dodávaného SW.
P.104	Součástí dodávky musí být instalace a konfigurace řešení včetně součinnosti při konfiguraci jednotlivých zařízení a aplikací a nastavení notifikací, a to včetně seznámení s funkcionalitami a obsluhou.
P.105	Je požadováno za 1 měsíc a za 3 měsíce vyhodnocení provozu a doladění pravidel/nastavení na základě získaných dat během provozu implementovaného systému a dle požadavků Zadavatele.
P.106	Napojení a předávání alertů a logů do systému analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí (viz kap. 4.4.5 přílohy č. 1 ZD (Technická specifikace)).
P.107	Je požadována dodávka nezbytných licencí, záruka na funkčnost, podpora aktualizace všech signatur a dodaného řešení po dobu 5 let.

Tabulka 17: Zabezpečení systému elektronické pošty před škodlivým kódem

5.2.13 Kontrola přístupu do sítě Internet – webSecurity

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

#	Požadavek
P.108	Je požadováno plně redundantní řešení WebSecurity systému pro kontrolovaný a zabezpečený přístup uživatelů do sítě Internet. Řešení může být formou virtuálního appliance do Vmware – rozšíření počtu virtuálních strojů musí být bezplatné (neomezený počet virtuálních strojů v rámci jedné sítě) případně dedikovaným HW (primární a sekundární) nebo kombinací těchto variant. Požaduje se dodávka licencí i pro testovací prostředí a speciální segmenty (typu GUEST) na samostatných virtuálních appliance (instalace těchto appliance není součástí dodávky). Dodané licence musí umožnit převedení licencí mezi uvedenými variantami (HW/virtual). Řešení musí podporovat VRRP, nebo jinou podobnou metodu, která umožní vytvořit cluster na virtuální IP adrese a musí podporovat balancování. V nabídce bude uveden způsob řešení a způsob redundance.
P.109	Minimální požadavky na websecurity řešení: 1. Řešení musí být výkonově dimenzováno minimálně na 1000 uživatelů a licencováno na 150 chráněných stanic (využíváno celkem 600 uživateli) 2. Jedno virtuální zařízení musí být schopné zpracovat minimálně 240 požadavků za sekundu při zapnutých všech bezpečnostních funkcích (NTLM ověřování uživatelů, HTTPS dešifrování, antivirus, antimalware, filtrování URL, proxy cache) 3. Rozšiřitelnost o centralizovanou konfiguraci pomocí dedikované management appliance 4. Podpora balancování 5. Jednoduše škálovatelné řešení pro případ rozšíření 6. Malware kontrola a filtrování 7. Spyware/Adware/komplexní ochrana proti webovým hrozbám, antivirová ochrana, automatická aktualizace všech antimalware signatur po 5 minutách nebo častěji 8. Podpora současného provozu více antimalware engines přímo na appliance (ne na dalším serveru) 9. Antivirové engines 10. Ochrana proti phishing útokům, automatická aktualizace pravidel na ochranu proti phishing útokům 11. Podpora filtrování URL, minimálně 60 URL kategorií, používané databáze pro URL/web filtrování 12. Vytváření politik per identita/zákazník, definice politik dle: a. časového okna b. dle URL kategorie c. pro cílové URL d. pro cílovou IP adresu e. možnost definice časových a objemových kvót pro uživatele 13. Možnost blokování, možnost pouze monitorovat, možnost zobrazit notifikační stránku při přístupu s možností potvrzení sdělení a vytvoření záznamu v logu 14. Možnost vytvoření vlastních URL kategorií, kategorizace URL (domén) i vyšších řádů (subdomén) 15. Možnost filtrovat přístup na Webmail, web chat aplikace

#	Požadavek
	16. Dynamická kategorizace nekategorizovaných URL přímo na zařízení nebo v cloud výrobce 17. Filtrování na základě web reputace a nastavitelné reputační filtrování na základě hodnoty reputace pro blokování/povolení/skenování obsahu 18. Blokování metody HTTP POST a FTP PUT pomocí metadata (file type, file name, file size) 19. Plnohodnotné a pravdivé skenování obsahu pro detekci typu souboru 20. Skenování na vrstvě TCP pro detekci nakažených stanic s aplikacemi, které komunikují po nestandardních portech 21. Monitorování a blokování malware spojení na všech 65535 portech a v příchozím i odchozím směru 22. Řešení musí být rozšiřitelné (např. licencí) o pokročilé funkce proti malware hrozbám o sandboxing pro neznámé typy souborů 23. Proxy cache a výkon a. Maximální velikost cacheovaného objektu minimálně 1 GB b. Technologie proxy cache c. Implementace v transparentním módu pomocí WCCPv2 nebo pomocí policy routingu nebo L4 přepínače d. Implementace jako explicitní proxy pomocí PAC souboru anebo WPAD e. Možnost hostování PAC souborů přímo na řešení f. Podpora více upstream proxy s podmíněným směrováním HTTP provozu g. Více datových portů pro skenování web provozu h. Možnost současného provozu řešení v explicitním i transparentním módu i. Možnost plné modifikace chybových hlášení pro koncové uživatele uvnitř zařízení 24. Kontrola protokolů pro kontrolu a. HTTP, HTTPS (dešifrování provozu) s možností selektivního výběru stránek pro dešifrování b. FTP (native) a FTP over HTTP c. Filtrování dílčích elementů web stránek d. Filtrování konkrétních typů prohlížečů a jejich verzí e. Blokování Java, ActiveX f. Detekované typy archivů včetně detekce vnořených archivů g. Blokování konkrétních typů souborů h. Detekce a blokování šifrovaných souborů i. Blokování souborů nad definovanou maximální velikost j. Monitorování a blokování aplikací P2P, IM, Youtube, Facebook, Flash video na aplikační úrovni (AVC) k. Možnost omezení šířky pásma pro media streaming provoz (youtube, atd.) l. Omezování šířky pásma pro video přenosy m. Ověřování důvěryhodných vydavatelských certifikátů pro HTTPS komunikaci n. Granulární rozpoznávání obsahu stránek facebook (tzn. Povolení přístupu na facebook, ale blokování facebook chat, facebook video či facebook games) 25. Ověřování uživatelů a. Autorizace uživatele na základě IP adresy a subnetu b. Ověření uživatele oproti LDAP (LDAPS)

#	Požadavek
	c. Active directory ověření uživatele pomocí NTLMSSP (integrované ověřování Windows) - NTLMv1, NTLMv2 d. Podpora LDAP/Active directory skupin pro přiřazení politik e. Pro NTLM podpora Windows serverů 2008 a vyšší f. Podpora multidomain v prostředí Windows bez externích agentů g. Možnost integrace s MS AD pomocí externího agenta i bez něj 26. Administrace a management a. HTTPS Management console b. Ověřování a autorizace administrátorů pomocí lokálních účtů a pomocí RADIUS c. Napojení do centrálního dohledu pomocí SNMP d. Podpora centrálního logování pomocí SYSLOG e. Podpora centrálního logování pomocí kopírování logů skrze FTP a SCP f. Upgradu firmware bez výpadku plné funkčnosti zařízení (s vyjímkou případného krátkého restartu OS nebo služeb) 27. Reporting a. GUI rozhraní pro účely administrace a prohlížení reportů b. Možnost vlastního nastavení reportu c. Možnost detailního prohlížení reportů pro každého uživatele a jeho aktivit pro účely analýzy d. Export reportů a plánování jejich pravidelného zasílání e. Zobrazení podezřelých aktivit pro každého uživatele f. Top-N reporty pro: Top uživatele, top URL, top URL kategorie, top malware, používání web aplikací g. Možnost ukládání reportu v PDF a CSV formátu
P.110	Řešení websecurity pro ZOS ZZS PAK bude provozováno na infrastruktuře (HW a systémový SW) požadované a dodávané dle kap. 4.4.15 – Infrastruktura (HW) a systémový SW pro běh dodávaného SW.
P.111	Součástí dodávky musí být instalace a konfigurace řešení včetně součinnosti při konfiguraci jednotlivých zařízení a aplikací a nastavení notifikací, a to včetně seznámení s funkcionalitami a obsluhou.
P.112	Je požadováno za 1 měsíc a za 3 měsíce vyhodnocení provozu a doladění pravidel/nastavení na základě získaných dat během provozu implementovaného systému a dle požadavků Zadavatele.
P.113	Je požadována dodávka nezbytných licencí, záruka na funkčnost, podpora aktualizace všech signatur a dodaného řešení po dobu 5 let.
P.114	Napojení a předávání alertů a logů do systému analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí (viz kap. 4.4.5 přílohy č. 1 ZD (Technická specifikace)).

Tabulka 18: Kontrola přístupu do sítě Internet – webSecurity

5.2.14 Nástroje pro zajištění šifrování dat na PC/NB

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

#	Požadavek
P.115	Požadujeme dodávku software řešení, pro on-line symetrické šifrování dat PC/NB s využitím standardizovaného algoritmu AES s délkou klíče minimálně 256 bitů a to technologií využívající „souborové“ šifrování, nikoli celodiskovou nebo kontejnerovou technologii.
P.116	Minimální požadavky na systém: 1. systém musí být dodán jako standardní komerční verze, ne jako speciální verze nebo kompilát 2. systém musí být plně lokalizován do českého jazyka včetně jeho technické podpory a veškeré dokumentace 3. systém musí zabezpečit ochranu dat uložených na koncových stanicích šifrováním profilů uživatelů, jednotlivých adresářů a souborů či dalších logických disků pomocí on-line souborového šifrování prostřednictvím standardního algoritmu AES 256 4. systém musí zajistit šifrování dat uložených na běžných přenosných paměťových médiích a to soukromým klíčem uživatele, sdíleným klíčem nebo jednorázovým klíčem 5. systém musí zajistit šifrování celého uživatelského profilu 6. systém musí umožnit práci více uživatelů na sdílených stanicích, kdy každý uživatel má šifrovaný svůj uživatelský profil svým soukromým klíčem a uživatelé mohou mít v rámci stanice sdílené zašifrované adresáře, které jsou šifrovány sdíleným klíčem 7. systém musí zajistit snadné sdílení zašifrovaných informací mezi jednotlivými oprávněnými uživateli i v rámci sdílených síťových adresářů nebo sdílených složek na lokálních discích 8. systém nesmí měnit uživatelské prostředí a procesy, to znamená, že uživatel pracuje ve standardním (jemu známém) prostředí, jeho styl práce se po implementaci šifrování nemění, veškeré disky, adresáře a soubory se mu jeví standardně, nejsou znatelné žádné rozdíly mezi šifrovanými a nešifrovanými informacemi při práci s nimi (vytváření, editování, mazání, kopírování, přesouvání) 9. systém musí zajistit správu přístupového hesla nebo šifrovacího klíče pouze oprávněným uživatelům s možností obnovení šifrovacího klíče z depozitáře šifrovacích klíčů s prokazatelným, autenticitním a nepopiratelným zaznamenáním použití této možnosti 10. Systém musí umožnit běžný servis koncové pracovní stanice a poskytování technické podpory ze strany administrátorů, aniž by jím šifrovaná data byla k dispozici v čitelné podobě, administrátor nepotřebuje mít k dispozici šifrovací klíče k tomu, aby mohl provádět instalace a nastavení programů či jiné administrátorské úkony na koncové stanici; koncové stanice musí pracovat i v režimu off-line
P.117	Je požadována dodávka minimálně 20 licencí pro PC/NB, záruka na funkčnost a podpora aktualizace dodaného řešení po dobu min. 5 let.

Tabulka 19: Nástroje pro zajištění šifrování dat na PC/NB

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

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

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.118	Dodávka infrastruktury a běhového prostředí pro následující části dodávky: 1. Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí (kap. 4.4.5) 2. Pokročilé notifikační nástroje (kap. 4.4.7) 3. Zabezpečení systému elektronické pošty před škodlivým kódem (kap. 4.4.12) 4. Kontrola přístupu do sítě Internet – webSecurity (kap. 4.4.13) 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.119	Dodávka min. 3 ks virtualizačního serveru s min. konfigurací: 1. provedení rack mount pro až 8 2,5“ pozic, maximální velikost 1U, pro přístup ke všem komponentám serveru bez použití nářadí 2. interaktivní LCD display či obdobný systém indikující základní informace o systému (min. IP adresa, stav serveru a výpis chybových stavů), možnost nastavení IP konfigurace OOB managementu na čelním panelu 3. minimálně jeden šestnáctijádrový 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) 4. min. 192 GB RAM (min. 32GB moduly 2666MHz) s možností rozšíření na 24 DIMM pozic 5. min. 2x 32 GB (flash či netočící médium) v raid 1 pro hypervizor 6. min. 1x 400 GB SSD s minimální hodnotou denního přepisu 3 7. hw řadič s min. 2GB cache a podporou raid 0, 1, 5, 6 8. min. 2x 1Gbase-T ethernet síťové porty typu LOM s podporou IPv4, IPv6 9. min. 4x 10GbE SFP+ porty 10. 2 redundantní síťové napájecí zdroje min. 750 W 11. rackové lyžiny a rameno na kabeláž na zadní straně serveru 12. management serveru nezávislý na operačním systému s dedikovaným USB či SD úložištěm dostupným i v případě výpadku interních disků, poskytující management funkce a vlastnosti: webové rozhraní a dedikovaná IP adresa, sledování hardwarových senzorů (teplota, napětí, stav, chybové senzory); podpora virtuální mechaniky 13. vyžadována je schopnost monitorovat a spravovat server out-of-band bez nutnosti instalace agenta do operačního systému 14. management musí podporovat dvoufaktorovou autentikaci, filtrování přístupu na základě IP adres (IP blocking) a AD/LDAP

#	Požadavek
	15. požadujeme vestavěné GUI s podporou HTML5 a možnost komunikace pomocí: HTTPS, CLI, IPMI, WSMAN, REDFISH 16. certifikace pro aktuální verze VMware ESX, vSphere, Windows Server 2016, Red Hat Enterprise Linux a SUSE 17. licence Microsoft Windows Server 2016 Datacenter pro požadovaný případně dodaný počet jader (vyšší hodnota) pro provoz jak nových, tak stávajících Windows Serverů na dodávaném HW. 18. podpora na 5 let typu NBD, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení 19. je vyžadována kompatibilita se stávajícím prostředím – server bude zařazen do stávající infrastruktury a virtualizačního prostředí
P.120	Dodávka min. 1 ks samostatného log 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 2. minimálně jeden šestnáctijádrový procesor s hodnotou dle SPECint_rate2006 base min. 1700 bodů a dle SPECfp_rate2006 base min. 1300 pro 2 CPU konfiguraci (údaje musí být k dispozici na www.spec.org) 3. min. 32 GB RAM (min. 8 GB moduly 2666MHz typu DDR4) 4. min. 5x 4 TB disk min 7200 otáček a min 3x 1,92 TB SSD s min DPWD 3 5. min. 4x 1Gbase-T ethernet síťové porty s podporou IPv4, IPv6 6. 2 redundantní síťové napájecí zdroje min. 750W 7. Interface: 4 x USB (1 vpředu, 2 vzadu, jeden uvnitř) a sériový port 8. hw řadič s min. 2GB cache a podporou raid 0, 1, 5, 6, 50, podpora SED disků a SSD disků, podpora globálního i dedikovaného hot-spare 9. certifikace pro aktuální verze VMware ESX, vSphere, Windows Server 2016, Red Hat Enterprise Linux a SUSE 10. 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) 11. vyžadována je schopnost monitorovat a spravovat server out-of-band bez nutnosti instalace agenta do operačního systému 12. management musí podporovat dvou faktorovou autentifikaci, filtrování přístupu na základě IP adres (IP blocking) a AD/LDAP 13. požadujeme vestavěné GUI s podporou HTML5 a možnost komunikace pomocí: HTTPS, CLI, IPMI, WSMAN, REDFISH 14. podpora na 5 let typu NBD, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení 15. operační systém dle požadavků navrženého nástroje na logování z IT infrastruktury je vyžadována kompatibilita se stávajícím prostředím – server bude zařazen do stávající infrastruktury

#	Požadavek
P.121	Datové úložiště s následujícími min. parametry: 1. diskové pole typu iSCSI SAN s interní virtualizací disků 2. velikost maximálně 3U s min. 30 pozicemi na disky 3. pole musí podporovat blokový přístup protokolem 10GbE iSCSI s možností rozšíření o protokol 12Gb SAS 4. základní konektivita: min. 2 Storage procesory, minimálně čtyři 10Gb/s iSCSI SFP+ porty na každý storage procesor – dodání včetně min. 8 potřebných SFP+ transceiverů s konektory LC a 4ks odpovídajících propojovacích kabelů LC-LC pro připojení do stávající infrastruktury. 5. diskové řadiče musí pracovat v režimu Active-Active (nikoliv ALUA) 6. každý řadič musí obsahovat min. 2 nezávislé back-end smyčky 12Gb SAS (2 porty na řadič) 7. min. 16GB cache na každý storage procesor, zálohovaná baterií (řešení s SSD cache není přípustné) 8. kapacita pro ukládání dat min.: 7x 960GB SAS SSD 12Gb 9. možnost rozšíření kapacity o min. 220 HDD/SSD a to pouze přidáním polic a disků, bez nutnosti dokupovat storage procesory a licenční funkce na další prostor (disky) 10. možnost použití SED disků. 11. licence pro plně automatický sub-LUN tiering dat s 3 tier architekturou a granularitou přesouvaných oblastí max. 10 MB 12. licence tiering musí umožnovat kvalifikaci a přesun mezi různými typy disků oběma směry (SSD, SAS 10K, NL-SAS 7,2K) 13. licence tiering musí umožnovat kvalifikaci a přesun mezi různými typy Raid (Raid 5, Raid 6 a Raid 10) 14. podpora thin-provisioning s eliminací zápisu nulových bloků 15. redundantní zdroje 16. webový management musí být možný z prostředí OS UNIX / Linux a MS Windows 17. monitoring musí umožnovat sledovat min. IOPS, MB/s pro front-end a back-end, vytížení CPU a cache 18. součástí licence či plug-in pro management z prostředí vSphere (VMware vSphere vCenter server) 19. podpora standardu pro záznam SYSLOG zpráv a protokolu SNMP 20. diskové pole musí být možné rozšířit o licence pro synchronní a asynchronní replikace mezi dvěma diskovými poli včetně licence pro metro-cluster řešení (pro VMware) 21. certifikace pro MS Windows 2016 a 2012, Hyper-V, VMware ESX, Redhat Enterprise Linux, XEN, HP-UX, AIX 22. přímá podpora VAAI, VASA, QoS, VVOLs 23. podpora na 5 let typu 24x7x365 s reakční dobou 4 hodiny, oprava v místě instalace zařízení, servis je poskytován výrobcem zařízení 24. je vyžadována kompatibilita se stávajícím prostředím – datové úložiště bude zařazeno do stávající infrastruktury (napojení na stávající 10g switche – ISCSI a připojení k virtualizačnímu prostředí) a.

#	Požadavek
P.122	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 přílohy č. 1 ZD (Technická specifikace)), 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 příloze č. 1 ZD (Technická specifikace). V případě, že nabízené řešení vyžaduje další nespecifikovaný systémový SW tak musí být součástí nabídky.
P.123	Součástí dodávky je integrace dodávaných technologií do stávajícího monitorovacího nástroje (WhatsUp firmy Ipswitch), který není součástí dodávky tohoto projektu. Monitoring musí jednoznačně identifikovat chod jednotlivých komponent.
P.124	Součástí dodávky je zařazení dodávané infrastruktury do stávající infrastruktury (napojení na stávající 10g switche – ISCSI a připojení k virtualizačnímu prostředí) včetně dodávky potřebných kabelů. Návrh propojení do stávající infrastruktury bude součástí implementační analýzy a návrhu řešení a bude podléhat schválení zadavatelem.
P.125	Součástí dodávky není strukturovaná kabeláž.
P.126	Dodávka, zapojení, instalace technologií, instalace a zprovoznění dodávaných technologií a prvků na dodaných technologiích.

Tabulka 20: Infrastruktura (HW) a systémový SW pro běh dodávaného SW

5.2.16 Nástroje pro bezpečnostní audit a penetrační testy

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

#	Požadavek
P.127	Je požadována dodávka nástroje/nástrojů pro periodické testování bezpečnostních zranitelností interních systémů i systémů, které komunikují s externími subjekty i jako součást penetračních testů (nástroj/nástroje budou využity v rámci kap. 4.4.17 – Bezpečnostní audit a penetrační testy.
P.128	Minimální rozsah: externí testy, interní testy a testy zranitelností operačních systémů, databází a informačních systémů (aplikací).

#	Požadavek
	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.129	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.130	Předmětem dodávky není periodické provádění testů zranitelností (nad rámec testů v rámci vedlejších aktivit), ale zajištění nástrojů pro provádění a vyhodnocování uvedených testů.
P.131	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.132	Instalaci skeneru musí být možné realizovat na prvky s operačními systémy Microsoft Windows 7 a vyšší, Microsoft Windows Server 2008 a vyšší, macOS i Linux. Součástí dodávky nebude HW, OS ani další aplikační vybavení nutné pro provoz nástroje. Předpokládá se instalaci na prostředky Zadavatele (virtuální server nebo testovací PC/notebook).
P.133	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.134	Řešení musí být schopné identifikovat chybějící záplaty/zranitelné služby a aplikace běžící na skenovaných systémech.
P.135	Součástí dodávky bude licence relevantního nástroje s podporou a funkčností po dobu 5 let, instalace a aktivace jednoho skeneru v prostředí Zadavatele a úvodní zaškolení administrátorů a uživatelů.

Tabulka 21: Nástroje pro bezpečnostní audit a penetrační testy

5.2.17 Bezpečnostní audit a penetrační testy

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

#	Požadavek
P.136	Bezpečnostní analýza stávajícího prostředí z pohledu souladu se zákonem 181/2014 Sb., ve znění pozdější novelizace a s vyhláškou 82/2018 Sb.
P.137	Hodnocení stávajícího rozsahu řízení bezpečnosti informací: 1. Politiky 2. Metodiky a. Metodika identifikace a hodnocení aktiv b. Metodika analýzy rizik

#	Požadavek
	3. Proces a výstupy hodnocení aktiv 4. Proces a výstupy hodnocení rizik 5. Revize primárních a podpůrných aktiv, jejich vzájemné vazby, určení jejich hodnoty a hodnocení jejich správy garanty 6. Plán zvládání rizik 7. Prohlášení o aplikovatelnosti bezpečnostních opatření 8. Zajištění zpětné vazby 9. Plán rozvoje bezpečnostního povědomí 10. Strategie řízení kontinuity 11. Pravidla řešení kybernetických bezpečnostních incidentů 12. Pravidla řízení provozu ICT 13. Hodnocení definice kontextu organizace, hodnocení jeho rozdělení na vnitřní a vnější kontext a hodnocení SLA mezi těmito 2 kontexty
P.138	Přezkoumání implementace technických opatření do praxe. Technické ověření souladu implementace primárních a podpůrných aktiv dle požadavků ZKB: 1. Aplikace 2. Operační systémy 3. Síťové prvky 4. Bezpečnostní prvky 5. Fyzická bezpečnost 6. Zálohování 7. Apod.
P.139	Výsledkem auditu bude: 1. Zpráva z přezkoumání stávajícího prostředí Zadavatele s následujícím obsahem: a. Pro každé opatření bude uveden popis aktuálního stavu b. Zhodnocení z pohledu požadavků prováděcí vyhlášky KB (ZKB) c. Případné zhodnocení z pohledu „best practice“, pokud bude takovéto doporučení žádoucí. d. Každé opatření bude popsáno minimálně v rozsahu ½ A4. e. Obsahem zprávy jsou veškeré paragrafy obsažené v prováděcí vyhlášce ZKB, tzn. že se organizace zkoumá z pohledu organizační opatření, technických opatření i fyzické bezpečnosti. 2. Hodnocení stavu a. Přehledový dokument s výpočetní logikou, který bude hodnotit výsledek pro ▪ Technické role ▪ Odděleně a s menší mírou detailu pro manažerské role b. Hodnocení bude provedeno jednotlivě pro každý požadavek paragrafů ZKB 3. Obecný návrh nápravných opatření a. Cílem není hodnotit veškeré možné technické varianty nápravných opatření, ale určit orientační výši nákladů pro zajištění souladu se ZKB a určit druh technologie. 4. Prezentace výsledků projektu pro projektový tým a. PT prezentace a diskuze s týmem 5. Prezentace výsledků projektu pro vrcholový management

#	Požadavek
P.140	Provedení penetračních testů a testů zranitelnosti: 1. Provedení penetračních testů a testů zranitelnosti pro IS ZOS, IS ZZOS a systému elektronické pošty (informační systémy a technologie jsou popsány v kap. 7.2 – Informační systémy k zabezpečení). 2. Pro systémy IS ZOS, IS ZZOS a Elektronickou poštu budou provedeny závěrečné testy zranitelnosti z externí sítě. V zájmu ověření korektního fungování webového aplikačního firewallu (WAF) a zajištění vysoké úrovně bezpečnosti provozovaných webových aplikací je požadováno provedení jednorázových penetračních testů.
P.141	Závěrečné testy zranitelnosti budou provedeny z externí sítě na IS ZOS, IS ZZOS a Elektronickou poštu. Jedná se tedy o testy zranitelnosti realizované přes bezpečnostní prvky – perimetry (FireWall) implementované v ZOS a ZZOS. Tyto testy musí obsahovat min.: 1. Host Discovery – vyhledávání aktivních strojů; 2. Port Scanning – skenování portů; 3. Service Discovery – vyhledání běžící služby; 4. Brute Force – testování Brute Force Attack; 5. Web Applications – skenování webových aplikací; Účelem těchto testů je ověření konfigurace perimetrů a nalezení zranitelností publikovaných služeb/systémů.
P.142	Součástí bezpečnostního auditu budou i penetrační testy, které musí splňovat minimálně: 1. Penetrační testy se budou týkat uvedených aplikací provozovaných zadavatelem a jejich účelem bude identifikovat případné nedostatky v nastavení nasazeného WAF a odhalit případné zranitelnosti ve výše uvedených aplikacích, které jsou jím chráněny, a zajistit tak jejich bezpečnost v rámci plnění požadavků §25 vyhlášky 82/2018 Sb. v souladu s bezpečnostní strategií a dalšími dokumenty zadavatele. 2. Součástí testů nebude vyhledávání zranitelností v síťové ani jiné infrastruktuře, virtualizačních platformách ani dalším SW vybavení serverů provozujících uvedené aplikace, které s provozem daných aplikací přímo nesouvisí. Před vlastními penetračními testy bude proveden test zranitelnosti nástrojem uvedeným v kapitole 3.4.11. přílohy č. 1 ZD (Technická specifikace) viz předcházející požadavek. 3. Testy budou realizovány dle aktuální verze OWASP Testing Guide (OTG) a v souladu s metodikou OSSTMM a budou primárně zaměřeny na odhalování zranitelností dle platné verze OWASP Top 10. Využito při tom bude automatizovaných nástrojů i manuálního testování.
P.143	Výstupem testů zranitelnosti a penetračních testů musí být: 1. Závěrečná zpráva, která bude obsahovat soupis provedených testů a jejich výsledků, detailní popis odhalených zranitelností, ohodnocení jejich nebezpečnosti včetně konkrétního postupu umožňujícího jejich odstranění. 2. Doporučení řešení odhalených zranitelností – konkrétní postupy umožňující jejich odstranění u oblastí/technologií, které nejsou součástí dodávky. 3. Realizace opatření k odstranění odhalených zranitelností ve formě nastavení a implementace u oblastí, které jsou součástí dodávky.

Tabulka 22: Bezpečnostní audit a penetrační testy

5.2.18 Bezpečnostní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.144	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.145	Vybavení musí plnit podmínky zákona č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
P.146	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.147	Zabránění vstupu neautorizovaného subjektu do systému – zamezení možnosti přístupu neoprávněného subjektu.
P.148	Zajištění šifrované komunikace mezi všemi součástmi systému a pracovišti uživatelů, případně zajištění komunikace v odděleném síťovém prostředí.
P.149	Evidence přístupů všech uživatelů do systémů a technologií (logování) včetně časových údajů.
P.150	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.151	Veškeré logy budou dostupné pro externí Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí.

Tabulka 23: Bezpečnostní požadavky

5.2.19 Implementační a provozní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.152	Všechny komponenty musí být připraven na provoz 24x7x365 (non-stop).
P.153	Počet uživatelů informačních systémů se nezmění.
P.154	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.155	Instalace do prostředí objednatele uvedeného v kap. 7.4 – Stav ostatních informačních a komunikačních technologií a kap. 7.2 – Informační systémy k zabezpečení.

#	Požadavek
P.156	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.157	Dodávka OS na servery, včetně instalace do prostředí objednatele, vč. potřebných licencí, pokud se jedná o licencovaný OS.
P.158	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.159	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.160	Zajištění administrátorských aplikací, konzolí pro všechny součástí systému (OS, DB, IS, …) pro zajištění konfiguračního managementu systému anebo jeho součástí.
P.161	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.162	Architektura řešení celého systému musí korespondovat s požadavky na jeho dostupnost, uvedenými v servisní smlouvě.
P.163	Synchronizace času všech zařízení s time serverem nebo zprostředkovaně přes centrální systém.

Tabulka 24: Provozní požadavky

5.3 POŽADAVKY NA SLUŽBY

5.3.1 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 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 25: Dokumentace – požadavky na zpracování

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

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

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

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

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

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

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

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

5.3.2 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.

5.4 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.

Detailnější popis záručních služeb zpracovaný účastníkem tvoří přílohu č. 4 Smlouvy o dílo.

6. 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.	160	Dodávka a implementace HW, SW a síťové infrastruktury.
4	Vývoj a implementace úprav SW, dodávka dokumentace k SW.	160	Vlastní vývoj a implementace úprav IS dle analýzy a návrhu řešení.
5	Ověření funkčnosti dodaných technologií a systémů.	170	Otestování funkčnosti technologií a systémů a ověření jejich plné funkčnosti.
6	Seznámení s funkcionalitami, obsluhou dodávaných technologií	170	Seznámení s funkcionalitami, obsluhou dodávaných technologií
7	Dodávka dokumentace dodaného systému a jeho částí.	170	Min. uživatelská dokumentace, dokumentace skutečného provedení, systémová dokumentace, projektová dokumentace.

#	Fáze	Doba trvání od zahájení	Doplňující informace
8	Převedení do zkušebního provozu.	170	Převedení do zkušebního provozu, odstranění všech vad a nedodělků, dokončení realizace a převedení do ostrého provozu.
9	Bezpečnostní audit a penetrační testy	180	Zpracování a předání bezpečnostního auditu a penetračních testů. *Pozn.: zpracování bezpečnostního auditu bude zahájeno při zahájení realizace. Jedná se o termín předání a akceptace výstupů.*
10	Ukončení realizace dodávky.	180	Součástí je zahájení doby provozu dodaného systému a poskytování servisních služeb.

Tabulka 26: 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.

7. MÍSTA PLNĚNÍ

Realizace předmětu plnění bude probíhat v následujících místech plnění:

Místo	Adresa	Předmět realizace
Zdravotnická záchranná služba Pardubického kraje	Průmyslová 450, Pardubice PSČ: 530 03	Primární datové centrum ZZS PAK – dodávky v návaznosti na technologie umístěné v tomto DC a dodávka částí technologie. Primární lokalita, kde je provozován IS ZOS a kde je primární ZOS. Současně se jedná o primární lokalitu IS elektronická pošta. Sídlo ZZS PAK – místo předání výstupů projektu.
Záložní zdravotnické operační středisko ZZS PAK a záložní datové centrum	Dr. Milady Horákové 1798/47, Chrudim	Záložní datové centrum je umístěno v objektu ZZS – VZ Chrudim, kde je umístěno jak DC, tak Záložní zdravotnické operační středisko (ZZOS) ZZS PAK. V této lokalitě je umístěna dodaná technologie ZZOS, DC je propojeno s primárním datovým centrem ZZS PAK. Dodávky v návaznosti na technologie umístěné v tomto DC a dodávka částí technologie.

Tabulka 27: Místa plnění

8. POŽADAVKY NA SOUČINNOST

Předpokladem úspěšné realizace dodávek je zajištění těchto základních součinností ze strany Zadavatele:

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

#	Požadovaná součinnost	Poznámky
8	Zajištění prostor pro jednání projektových týmů – zajištění prostor pro jednání týmů na všech úrovních projektového řízení. Včetně WC a napájení 230V.	Organizační komplikace, možnost vzniku vícenákladů na projekt. Při zahájení projektu.
9	Zajistit akceptační proceduru na straně Objednatele/Zadavatele pro zajištění akceptace poskytovaných služeb/jednotlivých dílčích plnění převzetí jednotlivých dodávek.	Zpoždění v projektu, nemožnost zahájit případné návazné etapy projektu. Při zahájení projektu.
10	Součinnost při školení – pro zdárný průběh školení poskytnout potřebnou infrastrukturu: zajištění školící místnosti, počítačového vybavení a projektoru po celou dobu školení. Delegovat osobu zodpovědnou za organizaci školení na straně Objednatele/Zadavatele. Delegovat pracovníky na školení a zajistit jejich rozdělení do skupin.	Neproškolení uživatelů, nemožnost používat systém autorizovanými pracovníky. 1 týden před započetím školení.
11	Součinnost v rámci Zkušebního a testovacího provozu – delegovat osoby Objednatele (testery) a zajistit organizaci zkušebního provozu (kdo, kdy bude prověřovat výstupy projektu) / Zkušební, jaká funkcionalita a jak dlouhou dobu bude prověřována)	Riziko na straně Objednatele/Zadavatele – aplikace není ověřena v živém provozu. 1 měsíc před předáním do zkušebního provozu) / V příslušné etapě.
12	Plnění operativních úkolů – realizovat a zabezpečovat operativní úkoly stanovené na jednotlivých úrovních řízení (na základě zápisů z jednání, rozhodnutí Řídícího výboru a vyplývající z ostatní projektové dokumentace). Zajištění reakční doby v souladu s úkoly zadanými v rámci projektových činností	Nedodržení harmonogramu, zpoždění v projektu. V rámci realizace projektu průběžně.
13	Zadavatel zajistí po celou dobu instalace a zprovozňování systému přístup pro pracovníky uchazeče do prostor budování KB pro ZZS PAK (dispečerský sál, technologická místnost a přilehlé prostory) a dále zajistí uzamykatelný prostor za účelem uložení montážního a instalačního materiálu a dočasné šatny pracovníků. Zajištění přístupových cest pro vozidla s dodávkou technologie, volné stěhovací trasy do místa určení, výtah. Zajištění možnosti provádět implementační práce v době od 8:00-18:00.	Organizační problémy při zahájení instalace, ztížené podmínky. V rámci realizace projektu průběžně.
14	Zajištění dostatečného prostoru (RACK), napojení na infrastrukturu a zálohovaného napájení pro instalace dodávaných technologií	Nelze efektivně realizovat projekt.

#	Požadovaná součinnost	Poznámky
15	Zajištění konfigurací, součinnosti a přístupů k navazujícím technologiím.	Nemožnost realizace projektu
16	Pro zrychlení řešení případných problémů uživatelů s klientskou částí systému a pro zvýšení efektivity při poskytování telefonických konzultací navrhujeme umožnit vzdálený přístup pracovníků podpory na plochu koncové stanice operátora; přístup bude umožněn pouze na vyžádání ze strany uživatele. - Vzdálený přístup ke klientským pracovištím a serverům pro IT dodavatele - Zajistit vzdálený přístup pro instalační práce - Zajištění přístupových účtů a oprávnění k provádění záručního servisu - Vzdálený přístup pro realizaci zásahů v rámci záruky	Zpomalení řešení případných problémů se systémem na koncových stanicích operátorů, nemožnost podpořit telefonické konzultace sdílením obrazovky. Před termínem s požadovaným přístupem uživatele.

Tabulka 28: Požadavky na součinnost

Nabídka servisních podmínek

V této je popsán návrh servisních služeb, které jsou v souladu s přílohou č. 2 zadávací dokumentace.

1. Předmět poskytování servisních služeb

Předmětem poskytování servisních služeb budou tyto činnosti:

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

Budou poskytovány následující služby:

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

2. Podmínky poskytování služeb

Níže jsou shrnuty podmínky poskytování servisních služeb.

2.1 Druhy poruch

Při kategorizaci rozlišujeme dvě závažnosti poruch.

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

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

2.2 Řešení poruch

1. V případě, že se jedná o poruchu na Systému dle této Smlouvy, vztahují se na ni SLA dle této Smlouvy.

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

2.3 Způsob ohlašování poruch

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

2.4 Reakce Poskytovatele

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

2.5 Režimy

Servisní služby budou poskytovány v těchto režimech, respektive v režimech provozu jednotlivých oblastí systému.

- 24 x 7 – poskytování služeb non-stop, tj. 24 hodin denně, 7 dní v týdnu, 365 dní v roce.
- 5 x 10 – poskytování služeb v pracovní dny, v pracovní době

Pracovní dny: pondělí – pátek; vyjma státních svátků, pracovní doba v pracovních dnech od 7:00 do 17:00 hodin.

2.6 Lhůty pro jednotlivé režimy

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

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

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

2.7 Ostatní podmínky

Ostatní podmínky na poskytování základní podpory jsou:

1. Servisní výjezdy (práce a cestovní náklady) na území Pardubického kraje nebudou Poskytovatelem Objednateli účtovány (bezplatné plnění).
2. Legislativní úpravy systému v návaznosti na změny legislativy, vyhlášek a nařízení ČR a EU a zdravotních pojišťoven – v rámci paušální platby.
3. Poskytování součinnosti dalším poskytovatelům služeb zabezpečení provozu integrovaných systémů v rámci poskytování maintenance nebo základní podpory v rámci zabezpečení provozu.
4. V rámci provozu Systému bude v součinnosti Objednatele a Poskytovatele docházet k instalacím nových verzí SW, bezpečnostních a opravných balíčků systémového SW (OS, DB apod.) a obměna HW a komunikační infrastruktury („modernizované provozní prostředí“). Služby budou na Systém poskytovány i na modernizované provozní prostředí, pokud bude zajištěno ve vzájemné součinnosti s Poskytovatelem nebo nebudou v rozporu se standartními požadavky na chod Systému.

3. Úroveň poskytovaných služeb

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

#	Položka rozpočtu	Režim poskytování
1	FireWall(y) s IPS pro ZOS	24 x 7
2	Aplikační firewall pro IS ZOS	24 x 7
3	Systémy pro sběr dat (logů) o síťovém provozu	10 x 5
4	Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí	10 x 5
5	Analytické nástroje pro ZOS ZZS PAK	10 x 5
6	Pokročilé notifikační nástroje	10 x 5
7	Úpravy IS ZOS	24 x 7
8	Konfigurace systému elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů	10 x 5
9	Dvoufaktorová autentizace administrátorských VPN přístupů	24 x 7
10	Dodávka a implementace technologií 802.1x pro zabezpečení přístupů do LAN sítě	24 x 7
11	Zabezpečení systému elektronické pošty před škodlivým kódem	10 x 5
12	Kontrola přístupu do sítě Internet – webSecurity	10 x 5
13	Nástroje pro zajištění šifrování dat na PC/NB	10 x 5
14	Infrastruktura (HW) pro běh dodávaného SW	24 x 7

#	Položka rozpočtu	Režim poskytování
15	Systémový SW pro běh dodávaného SW	24 x 7

Tabulka 29: Úroveň požadovaných služeb

4. OSTATNÍ PODMÍNKY

Kvalita a záruky:

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

Obnova dat, bezpečnost a pravidla pro update aplikace:

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

Servis vybavení prováděný pracovníky Objednatele:

1. Pracovníkům Objednatele bude umožněno provádět drobné opravy závad vybavení vlastními silami při dodržení všech závazných podmínek a ustanovení jakož i veškerých pracovních postupů a doporučení stanovených Poskytovatelem.
2. Pracovník Objednatele bude povinen vyžádat si souhlas Poskytovatele v každém případě, kdy nebude zcela jisté, zda bude oprávněn provést danou opravu vlastními silami a současně si vyžádat doporučení vhodného postupu provedení opravy. Souhlas Poskytovatele i jím doporučený pracovní postup musí být zaevidován v helpdesku, provozovaném Poskytovatelem.

3. Stejně tak veškeré informace o zjištěných závadách a provedených opravách (vč. sériových čísel měněných komponent) bude Objednatel povinen řádně evidovat prostřednictvím helpdesku, provozovaného Poskytovatelem.
4. Za opravy provedené pracovníky Objednatele neponese Poskytovatel žádnou zodpovědnost a na tyto opravy nebude poskytovat žádné záruky. Poskytovatel dále neponese žádnou zodpovědnost za jakékoli závady nebo škody, způsobené pracovníky Objednatele při provádění oprav vybavení. Tyto závady nebude možné považovat za chyby informačního systému a případné odstranění těchto závad Poskytovatelem bude placenou službou.

5. POPIS SLUŽBY HELPDESK

Pro hlášení vad díla a chyb v systému Objednatelem zajistí Poskytovatel HelpDesk.

HelpDesk bude zajištěn takto:

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

        - V případě chybějících údajů, neprodleně kontaktuje oprávněnou osobu, která požadavek zaregistrovala, pro jejich doplnění
    - Operátor YS Helpdesk
        - YS Helpdesk zajistí získaní všech potřebných a dostupných údajů pro co nejrychlejší a nejefektivnější řešení
        - Helpdesk provede vyhodnocení relevantnosti požadavku, následně provede jeho klasifikaci a kategorizaci a požadavek zaregistruje
- Po zaregistrování platného požadavku je oprávněné osobě, případně dalším zainteresovaným osobám, automaticky vygenerována e-mailová notifikace s potvrzením přijetí požadavku
- Helpdesk předá požadavek kompetentnímu pracovníkovi technické podpory
- Po přidělení je pracovníkovi TP vygenerována automatická e-mailová notifikace o přiděleném případu k řešení. V případě požadavků/závad s vysokou prioritou jsou tyto potvrzeny pracovníkovi technické podpory zároveň telefonicky
- Helpdesk průběžně monitoruje stav řešení a na vyžádání o něm informuje oprávněné osoby
- Helpdesk hierarchicky nebo funkčně eskaluje požadavky, které nejsou řešeny v dohodnutých termínech nebo kde se blíží konec dohodnutého termínu
- Je-li požadavek ze strany oprávněné osoby, která požadavek nahlásila, urgován nebo doplněn o nové skutečnosti, Helpdesk provede aktualizaci požadavku, o čemž je oprávněná osoba, další zainteresované osoby a příslušný pracovník technické podpory informován formou e-mailové notifikace.

Aktualizace, urgence, případně storno požadavku je možné provést pomocí veškerých smluvních komunikačních kanálů.

- Po vyřešení požadavku Helpdesk informuje osobu, která požadavek nahlásila, o jeho vyřešení.
    - Telefonicky
        - Po ověření a odsouhlasení řešení je případ uzavřen a automaticky vygenerována e-mailová notifikace o uzavření požadavku
        - Při neakceptování je požadavek vrácen zpět k řešení kompetentnímu pracovníkovi technické podpory
    - Automaticky generovanou e-mailovou notifikací o vyřešení požadavku
        - Při akceptování řešení (libovolným smluvním komunikačním kanálem) Helpdesk požadavek uzavře.
        - Při neakceptování řešení (libovolným smluvním komunikačním kanálem) je požadavek vrácen zpět k řešení kompetentnímu pracovníkovi technické podpory
        - Neobdrží-li Helpdesk do 5 pracovních dnů reakci na vyřešení požadavku, je řešení požadavku automaticky považováno za odsouhlasené a je požadavek je uzavřen.
        - Při uzavření požadavku je automaticky vygenerována e-mailová notifikace o uzavření požadavku

Komunikační kanály

- Placená telefonní linka 277 775 555
- Placená faxová linka 277 775 501
- Záložní mobilní spojení 737 203 233

- Elektronická pošta helpdesk@ys.cz
- Webové rozhraní https://yourdesk.ys.cz

6. MÍSTA PLNĚNÍ

Servisní služby budou poskytovány na těchto místech plnění:

Místo	Adresa	Předmět realizace
Zdravotnická záchranná služba Pardubického kraje	Průmyslová 450, Pardubice PSČ: 530 03	Primární datové centrum ZZS PAK – návaznost na technologie umístěné v tomto DC a dodávka částí technologie. Poskytování servisních služeb pro dodané úpravy IS a technologie umístěné do této lokality.
Záložní zdravotnické operační středisko ZZS PAK a záložní datové centrum	Dr. Milady Horákové 1798/47, Chrudim	Záložní zdravotnické operační středisko ZZS PAK a záložní datové centrum pro toto ZZOS, kde bude umístěna dodaná technologie ZZOS a které bude propojeno s primárním datovým centrem ZZS PAK. Poskytování servisních služeb pro dodané úpravy IS a technologie umístěné do této lokality.

Tabulka 30: Místa plnění

Příloha č. 3 Zpracování nabídkové ceny

Položka ceny	**Cena v Kč s DPH**
Celková nabídková cena za servisní služby dle vzorové Servisní smlouvy	4 317 280,00 Kč

Ozn.	**Položka rozpočtu**	**Počet jednotek**	**Cena za servisní služby / 1 rok (v Kč bez DPH)**	**Cena za servisní služby / 4 roky (v Kč bez DPH)**	**Cena za servisní služby / 4 roky (v Kč s DPH)**
1	FireWall(y) s IPS pro ZOS	1 soubor	892 000,00 Kč	3 568 000,00 Kč	4 317 280,00 Kč
2	Aplikační firewall pro IS ZOS	1 ks			
3	Systémy pro sběr dat (logů) o síťovém provozu	1 soubor			
4	Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí	1 soubor			
5	Analytické nástroje pro ZOS ZZS PAK	1 soubor			
6	Pokročilé notifikační nástroje	1 soubor			
7	Úpravy IS ZOS	1 soubor			
8	Konfigurace systému elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů	1 soubor			
9	Dvoufaktorová autentizace administrátorských VPN přístupů	1 soubor			
10	Dodávka a implementace technologií 802.1x pro zabezpečení přístupů do LAN sítě	1 soubor			
11	Zabezpečení systému elektronické pošty před škodlivým kódem	1 soubor			
12	Kontrola přístupu do sítě Internet – webSecurity	1 soubor			
13	Nástroje pro zajištění šifrování dat na PC/NB	1 soubor			
14	Infrastruktura (HW) pro běh dodávaného SW	1 soubor			
15	Systémový SW pro běh dodávaného SW	1 soubor			
16	Nástroje pro bezpečnostní audit a penetrační testy	1 soubor	---	---	---
17	Bezpečnostní audit a penetrační testy	1 soubor	---	---	---
Celkem			**892 000,00 Kč**	**3 568 000,00 Kč**	**4 317 280,00 Kč**