Příloha č. 3: Technická specifikace dodávky

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

OBSAH

VYUŽITÉ ZDROJE

Nejsou

SEZNAM TABULEK

SEZNAM ZKRATEK A POJMŮ

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

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

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

Tabulka 1: Seznam zkratek a pojmů

1 PŘEDMĚT PLNĚNÍ

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

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

Konkrétně se jedná o zvýšení kybernetické bezpečnosti pro následující IS:

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

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

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

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

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

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

2 ČLENĚNÍ DOKUMENTU

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

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

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

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

3 POŽADAVKY NA DODÁVKY A SOUVISEJÍCÍ SLUŽBY

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

3.1 PŘEDMĚT A ROZSAH DODÁVKY

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

Cílem projektu je zvýšení kybernetické bezpečnosti pro následující IS:

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

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

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

b) nástroj pro ochranu integrity komunikačních sítí

c) nástroj pro ověřování identity uživatelů

h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

i) aplikační bezpečnost

Rozsah dodávky je uveden v následující kapitole.

3.1.1 Rozsah dodávky

Rozsah dodávky je následující:

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

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

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

Tabulka 2: Předmět a rozsah dodávky

3.1.2 Související služby a náležitosti dodávky

Součástí dodávky jsou dále následující služby a náležitosti:

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

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

Doplňující požadavky na implementaci:

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

3.1.3 Dodávkou nedotčené oblasti stávajícího řešení

Dodávkou nebudou dotčeny následující oblasti stávajícího řešení:

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

3.1.4 Vyloučení z dodávky

Předmětem dodávky není:

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

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

3.2 VÝCHODISKA A PŘIPRAVENOST

Pro řešení jsou stanovena následující východiska:

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

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

Tabulka 3: Východiska

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

3.3 ZÁKLADNÍ POŽADAVKY NA ZABEZPEČENÍ IS

Základní požadavky na požadované řešení jsou následující:

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

Detailní popis požadavků na dodávky je uveden v následující kapitole.

3.4 POŽADAVKY NA DODÁVKY

V této kapitole jsou uvedeny požadavky na dodávky.

3.4.1 Obecné a společné požadavky

V této kapitole jsou uvedeny obecné požadavky na požadované řešení:

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

Tabulka 4: Obecné požadavky

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

3.4.2 FireWall s IPS pro ZZOS

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

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

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

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

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

Tabulka 5: FireWall s IPS pro ZZOS

3.4.3 FireWall pro ochranu segmentu ZOS

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

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

Tabulka 6: FireWall pro ochranu segmentu ZOS

3.4.4 L3 switche pro ZZOS

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

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

Tabulka 7: L3 switche pro ZZOS

3.4.5 Aplikační firewall pro IS ZOS

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

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

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

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

Tabulka 8: Aplikační firewall pro IS ZOS

3.4.6 Systém analýzy bezpečnostních logů (SW)

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

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

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

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

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

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

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

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

Tabulka 9: Systém analýzy bezpečnostních logů (SW)

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

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

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

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

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

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

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

3.4.8 Úpravy IS ZOS

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

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

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

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

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

Tabulka 11: Úpravy IS ZOS

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

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

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

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

3.4.10 Dvoufaktorová autentizace administrátorských VPN přístupů

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

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

Tabulka 13: Dvoufaktorová autentizace administrátorských VPN přístupů

3.4.11 Nástroje pro bezpečnostní audit a penetrační testy

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

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

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

Tabulka 14: Nástroje pro bezpečnostní audit a penetrační testy

3.4.12 Bezpečnostní audit a penetrační testy

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

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

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

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

Tabulka 15: Bezpečnostní audit a penetrační testy

3.4.13 Bezpečnostní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

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

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

Tabulka 16: Bezpečnostní požadavky

3.4.14 Implementační a provozní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

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

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

Tabulka 17: Provozní požadavky

3.5 POŽADAVKY NA SLUŽBY

3.5.1 Realizace předmětu plnění

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

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

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

Popis bude obsahovat alespoň:

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

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

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

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

v) Detailní popis zajištění bezpečnosti systému a informací

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

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

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

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

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

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

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

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

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

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

a) Instalace, upgrade a zahoření HW na místě,

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

c) Nastavení HW a aplikací

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

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

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

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

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

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

Tabulka 18: Dokumentace – požadavky na zpracování

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

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

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

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

- Portable Document Format (formát .pdf).

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

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

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

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

3.5.2 Seznámení s funkcionalitami, obsluhou dodávaných technologií

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

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

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

3.6 ZÁRUKY

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

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

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

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

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

Poskytovatel zajistí HelpDesk pro hlášení vad.

4 HARMONOGRAM

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

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

Tabulka 19: Harmonogram

Doplňující informace:

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

5 MÍSTA PLNĚNÍ

Realizace předmětu plnění bude probíhat v následujících místech plnění:

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

Tabulka 20: Místa plnění

6 VÝCHOZÍ STAV

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

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

Kontext ZZS JMK v rámci řešení projektu je následující:

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

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

6.2 INFORMAČNÍ A KOMUNIKAČNÍ SYSTÉMY K ZABEZPEČENÍ

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

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

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

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

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

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

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

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

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

Tabulka 21: Výčet IS k zabezpečení

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

6.2.1 IS ZOS

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

6.2.1.1 Informační systémy a aplikační software ZOS

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

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

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

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

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

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

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

Tabulka 22: IS ZOS

6.2.1.2 Pracoviště ZOS

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

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

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

Tabulka 23: Pracoviště ZOS

6.2.2 Elektronická pošta

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

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

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

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

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

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

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

Elektronická pošta je provozována následujícím způsobem:

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

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

V následující tabulce jsou uvedena umístění IS ZOS:

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

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

Tabulka 24: Umístění

6.4 STAV OSTATNÍCH INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ

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

6.4.1 Datové centrum, HW infrastruktura, systémový SW

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

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

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

Tabulka 25: Datové centrum, HW infrastruktura, systémový SW

6.4.2 Datové sítě

V rámci projektu budou využity následující sítě:

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

Tabulka 26: Datové sítě

6.4.3 Síťová infrastruktura

V následující tabulce je uveden popis síťové infrastruktury:

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

Tabulka 27: Síťová infrastruktura

6.4.4 Provoz

Provoz stávajícího řešení je zajišťován s následujícími parametry:

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

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

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

KONEC ZÁKLADNÍ ČÁSTI DOKUMENTU